Incident Management for Industrial Control Systems

Safeguard industrial control systems by mastering critical infrastructure cybersecurity

DURGESH KALYA

Foreword by Marco (Marc) Ayala, ISA Fellow National Sector Chief – Energy, InfraGard National President, InfraGard Houston

packt

Incident Management for Industrial Control Systems

Safeguard industrial control systems by mastering critical infrastructure cybersecurity

Durgesh Kalya

‹packt›

Incident Management for Industrial Control Systems

Portfolio Director: Vijin Boricha
Relationship Lead: Niranjan Naikwadi
Project Manager: Gandhali Raut
Content Engineer: Shubhra Mayuri
Technical Editor: Nithik Cheruvakodan
Copy Editor: Safis Editing
Indexer: Rekha Nair
Production Designer: Alishon Falcon
Growth Lead: Ankita Thakur

First published: January 2026

Production reference: 1230126

Published by Packt Publishing Ltd.
Grosvenor House
11 St Paul's Square
Birmingham
B3 1RB, UK.

ISBN 978-1-83546-971-2
www.packtpub.com

To my wife, Swati, for her patience, strength, and unwavering support throughout this journey.

To our parents, for their blessings, sacrifices, and the values that shaped who we are today.

To my children, Siddhant and Sachi, for their understanding, resilience, and grace during the late nights, weekends, and stolen hours it took to write this book.

- Durgesh Kalya

Foreword

It is a profound honor to pen this foreword for Durgesh Kalya's insightful book, *Incident Management for Industrial Control Systems*. I've known Durgesh for well over a decade, ever since our paths crossed at Nippon Chemicals in Texas, where he was already making waves in the world of IT by supporting the site and the folks in operations. From those early days, I've watched him evolve into a true leader in control systems security, particularly through his dedicated involvement with the International Society of Automation. It's been a privilege to play a small role in his journey, offering guidance and sharing experiences as he honed his expertise in OT and incident management. Durgesh isn't just a colleague; he's a steadfast friend whose passion for safeguarding critical infrastructure has inspired many, including myself.

In this book, you will find wisdom put into a practical roadmap for navigating the complex terrain of cyber and safety incidents in industrial environments. What strikes me most is how he shifts the conversation beyond mere technical fixes. Too often, incidents are viewed through a narrow cybersecurity lens, but Durgesh reminds us that true resilience comes from integrating people, processes, and technology. His four-pillar model serves as a sturdy foundation for organizations operating in high-stakes settings. It's a unified approach that ensures IT, OT, operations, safety, and emergency teams work in harmony, rather than in silos.

Drawing from public frameworks, industry standards, and real-world lessons, the book adapts proven emergency management principles to the unique demands of industrial control systems. This book focuses on timeless elements: clear roles, effective communication, and sound decision-making under duress. The inclusion of practical tools—such as worksheets, exercise injects, and planning templates—makes this more than a theoretical read; it's a hands-on guide that invites readers to roll up their sleeves and apply what they've learned.

Reflecting on my own career, I can't help but think of the times when many of us in this field learned the hard way—thrown into active responses without the benefit of structured preparation. Those experiences were invaluable, but they came at a cost. Durgesh's work offers a better path: one of foresight through planning and exercises. By emphasizing cross-functional coordination, he equips professionals to anticipate challenges, interact seamlessly with operations and safety teams, and emerge stronger from incidents. This is especially crucial for manufacturing facilities, where the stakes are sky-high, and a single misstep can cascade into catastrophe.

Whether you're a cybersecurity officer, an OT engineer, an incident responder, or a leader overseeing critical infrastructure, this book is an essential companion. It empowers you to transition from reactive firefighting to a disciplined, resilient stance. Durgesh has crafted a resource that not only educates but also motivates, drawing from the grit of industrial experience to foster better practices across the board.

In closing, I commend Durgesh for this timely contribution. As our world grows more interconnected and vulnerable, books like this light the way forward. May it serve as a beacon for industry professionals everywhere, helping to build safer, more secure systems for generations to come.

Marco (Marc) Ayala, ISA Fellow

National Sector Chief – Energy, InfraGard National

President, InfraGard Houston

Contributors

About the author

Durgesh Kalya is an industrial cybersecurity and incident management practitioner with over 20 years of experience across manufacturing, engineering, and information technology. A network security and OT specialist, his work focuses on protecting critical infrastructure by aligning operational technology, industrial control systems, cybersecurity, safety, and emergency response in real-world industrial environments.

He is an active contributor, speaker, and mentor within the industrial cybersecurity community, with a strong focus on practical and repeatable incident management and cybersecurity mentorship, particularly supporting young professionals entering the field. Outside of work, Durgesh is a black belt in Taekwondo, practices yoga, and enjoys spending time with his children on creative endeavors, including storytelling and filmmaking.

This book is the result of years of hands-on work, late-night reflection, and learning from people who generously shared their time, experience, and trust. I am deeply grateful to the mentors, colleagues, and communities who shaped my understanding of industrial systems, cybersecurity, and incident management.

I would like to acknowledge Mike Richard (Triad Engineering, Houston, retired Senior Project Engineer), who taught me the importance of preparation and discipline early in my career and set expectations that continue to guide my approach to safety and operational readiness. Webster Draughon (retired VP of Operations, Nisseki Chemical Texas Inc.) gave me my first opportunity to work at the intersection of industrial control systems and network security, trusting me to redesign networks and gain early exposure to ICS cybersecurity. That opportunity fundamentally shaped my career path.

I am especially thankful to Richard Modisette (I&E / DCS Engineer, JX Nippon Chemical Texas Inc.), who guided me as an I&E designer and helped me understand the practical realities of fiber optic networks, safety PLCs, and industrial automation systems. His mentorship extended beyond formal responsibilities, encouraging curiosity, experimentation, and continuous learning. Tony Aguilar (Safety Officer, JX Nippon Chemical Texas Inc.) introduced me to emergency response teams and root cause analysis, where I worked closely as an IT liaison and ICS specialist, gaining a deeper appreciation for how safety, operations, and response intersect during real incidents. I am also grateful to David Burch (retired VP of Operations, JX Nippon Chemical Texas Inc.), whose encouragement and confidence provided the motivation to continue writing, refining, and completing this book.

I would also like to recognize colleagues and coworkers who supported me as mentors and trusted peers along the way. Mike Banda, Luis Rubio, and Madhu Maganti consistently offered guidance, perspective, and encouragement, helping me navigate both technical challenges and professional growth within the industrial cybersecurity and operations space.

I would like to thank Marco Ayala (National Sector Chief, InfraGard), who instilled in me a sense of urgency around industrial automation and control systems and their critical role in national security. His guidance reinforced the importance of disciplined incident management and cross-sector collaboration in protecting critical infrastructure.

Much of the content in this book draws from publicly available frameworks and guidance. I extend my sincere appreciation to the individuals, volunteers, and organizations—including USCG, NIST, FEMA, and DHS—whose work has fundamentally shaped the practices discussed in these pages. I am also thankful to the technical reviewers and the editorial team at Packt Publishing for their guidance, diligence, and support throughout this process.

About the reviewer

With over 40 years of experience in the construction and manufacturing industries, **Richard Modisette** has held leadership and mentoring roles in areas including health and safety, IT, process controls, and many others. During his career at various chemical manufacturing facilities in the United States, Richard developed many health and safety policies and procedures to ensure compliance with evolving OSHA standards. As a long-time member of numerous emergency response teams, he has been able to assist in the development of emergency procedures. Richard experienced the nationwide growth of emergency response planning efforts within the chemical manufacturing industry over many years. His current duties are primarily focused on developing process controls and safety instrumented systems for in-service operations and the development of new projects.

Table of Contents

Chapter 2: Critical Infrastructure Security and Resiliency 21

Preface

Critical infrastructure systems form the backbone of modern society, supporting essential services such as energy, water, transportation, manufacturing, and healthcare. These systems increasingly rely on interconnected industrial automation and control systems, blending **operational technology (OT)** with traditional **information technology (IT)**. While this connectivity brings efficiency and visibility, it also introduces new risks—where cyber incidents, operational failures, and safety events can quickly cascade across systems.

Incident management in industrial control systems is no longer a niche capability or a compliance exercise. It is a core operational discipline that determines how effectively organizations respond to disruptions, protect people and the environment, and restore operations under pressure. This book focuses on building a structured, practical approach to incident management for critical infrastructure by combining an understanding of control systems, cybersecurity, emergency operations, and the Incident Command System.

Rather than treating incidents as isolated technical events, this book emphasizes coordination, communication, and preparedness across IT, OT, safety, and emergency response teams. The goal is to help organizations move from reactive responses to disciplined, repeatable incident management practices that improve resilience over time.

Who this book is for

This book is intended for professionals and leaders who are responsible for protecting, operating, or supporting critical infrastructure and industrial control systems. It is particularly relevant for **cybersecurity officers (CySOs)**, **chief information security officers (CISOs)**, and IT/OT security leaders, as well as OT and **Incident Command System (ICS)** engineers, safety and reliability engineers, emergency operations and incident response teams, and compliance or risk management professionals working in regulated industries.

You are expected to have a basic familiarity with industrial environments, networking concepts, or cybersecurity fundamentals. However, deep expertise across all domains is not required. This book is designed to bridge gaps between disciplines and provide a common framework that enables cross-functional teams to work together effectively during incidents.

What this book covers

Chapter 1, *Introduction to Critical Infrastructure*, introduces critical infrastructure concepts, sectors, and real-world incidents, establishing why structured incident management is essential.

Chapter 2, *Critical Infrastructure Security and Resiliency*, explores dependencies, interdependencies, supply chains, and regulatory considerations that influence incident impact and recovery.

Chapter 3, *Industrial Automation and Control Systems in Critical Infrastructure*, explains the control systems landscape, including ICS, OT, and their role in modern industrial environments.

Chapter 4, *Industrial Automation and Control Systems Threat Landscape*, examines IT versus OT security considerations, common threat models, and case studies relevant to industrial systems.

Chapter 5, *Emergency Operations and Their Significance in an Organization*, focuses on emergency operations, incident types, and the role of emergency management in critical infrastructure.

Chapter 6, *Introduction to the Incident Command System (ICS)*, introduces the ICS framework, its principles, structure, and relevance to managing industrial incidents.

Chapter 7, *Practical Considerations for Incident Management in IACS*, addresses real-world challenges such as monitoring, forensics, access constraints, safety systems, and coordination during incidents.

Chapter 8, *Introduction to Incident Management Standards and Frameworks for Critical Infrastructure*, reviews commonly used frameworks and standards and how they complement ICS-based incident management.

Chapter 9, *Incident Command System Training and Exercises*, discusses training methods, tabletop exercises, drills, and functional exercises tailored to ICS and OT environments.

Chapter 10, *Running an ICS Exercise*, provides guidance on designing, conducting, and evaluating incident management exercises for industrial organizations.

Chapter 11, *Optimizing Single-Site Exercises with Multi-Site Considerations*, explores how to scale exercises across facilities, regions, or enterprise environments.

Chapter 12, *ICS Resources*, offers practical tools, worksheets, checklists, injects, and references to support ongoing incident readiness and continuous improvement.

To get the most out of this book

Before starting this book, you should be familiar with basic cybersecurity concepts, general networking fundamentals, and the operational context of industrial or critical infrastructure

environments. An understanding of safety culture and emergency response principles will be helpful, but not mandatory. The book assumes practical involvement in at least one domain, such as IT, OT, safety, or incident response, and builds a shared understanding across disciplines.

This book does not require specific software or hardware installations. Examples, worksheets, and exercises are designed to be technology-agnostic and applicable across industries and platforms. You may reference publicly available tools, frameworks, and documentation related to ICS, OT networks, incident management, and emergency operations.

Additional notes

Throughout the book, worksheets and reference materials are provided to support note-taking, gap analysis, and exercise planning. These resources are available in digital formats for customization and reuse within your organization (`https://durgeshkalya.com/icsbookresources/`).

This book contains no organization-specific or proprietary information. All concepts are based on public-domain material and professional experience in industrial environments.

Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: `https://packt.link/gbp/9781835469712`.

Conventions used

There are a number of text conventions used throughout this book.

Bold: Indicates a new term, an important word, or words that you see on the screen. For instance, words in menus or dialog boxes appear in the text like this. For example: “The US **Department of Homeland Security** (**DHS**) prioritizes cybersecurity and incident reporting within CI sectors. “

Warnings or important notes appear like this.

Tips and tricks appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book or have any general feedback, please email us at `customercare@packt.com` and mention the book's title in the subject of your message.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you reported this to us. Please visit `http://www.packt.com/submit-errata`, click **Submit Errata**, and fill in the form.

You can find the errata list updated on this github repo: `https://github.com/PacktPublishing/Incident-Management-for-Industrial-Control-Systems`

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `http://authors.packt.com/`

Share your thoughts

Once you've read *Incident Management for Industrial Control Systems*, we'd love to hear your thoughts! Please `click here to go straight to the Amazon review page` for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Free benefits with your book

This book comes with free benefits to support your learning. Activate them now for instant access (see the "*How to Unlock*" section for instructions).

Here's a quick overview of what you can instantly unlock with your purchase:

How to Unlock

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require one

Part 1

Pillar 1 — Critical Infrastructure as the Foundation

Pillar 1 establishes **Critical Infrastructure (CI)** as the foundation upon which all incident management capabilities are built. Industrial facilities, utilities, and essential services operate in environments where disruptions can have immediate and far-reaching consequences for safety, the environment, and society.

This pillar explains what makes infrastructure "critical," how dependencies and interdependencies increase risk, and why resilience must be understood before applying any incident response or command framework. A clear understanding of this foundational pillar is essential before examining control systems, command structures, or response activities.

This part of the book includes the following chapters:

- *Chapter 1, Introduction to Critical Infrastructure*
- *Chapter 2, Critical Infrastructure Security and Resiliency*

1

Introduction to Critical Infrastructure

Critical Infrastructure (CI) is an intricate network that connects various elements essential to our well-being and societal functioning. The following figure shows a vast tapestry, where each thread symbolizes fundamental human needs – the life-sustaining flow of clean water, the secure refuge of shelter, the abundant yield of food, and the overall health and safety of people and the environment.

Figure 1.1 – A tapestry representing critical infrastructure

In this chapter, we explore the fundamental elements of CI. From recognizing the importance of various sectors to analyzing past cyber incidents, we'll gain perspectives on concepts that highlight the significance of CI.

We will cover the following main topics in this chapter:

- CI and incident management
- An overview of relevant CI sectors
- Notable cyber incidents in CI

Free Benefits with Your Book

Your purchase includes a free PDF copy of this book along with other exclusive benefits. Check the Free Benefits with Your Book section in the Preface to unlock them instantly and maximize your learning experience.

Your purchase includes a free PDF copy + exclusive extras

Your purchase includes a DRM-free PDF copy of this book, 7-day trial to the Packt+ library (no credit card required), and additional exclusive extras. See the *Free benefits with your book* section in the *Preface* to unlock them instantly and maximize your learning.

CI and incident management

CI encompasses digital networks, communication systems, process control systems, and power systems. Our role as protectors and fixers encompasses safeguarding these vital components from cyber threats and efficiently managing incidents that could disrupt their seamless operation.

In this section, we will delve into the foundational CI components, introducing CI as an essential cornerstone for effective incident management.

Figure 1.2 presents an illustration outlining the four pillars vital for proficient incident management within CI. Throughout this chapter, our emphasis is on exploring these specific topics with respect to CI.

Figure 1.2 – The four pillars essential for successful incident management

The four pillars shown in *Figure 1.2* form a structured pathway to mastering incident management for CI. *Pillar 1*, **CI**, establishes the foundation by defining what CI is, why it matters, and how its disruption can impact society at large. *Pillar 2*, **Industrial Automation and Control Systems (IACS)**, explores the unique control system environment, bridging the operational side of industrial systems (ICS/OT) with the business and enterprise layers (IT). *Pillar 3*, **Incident Command Systems (ICS)**, involves the framework necessary to coordinate responses effectively during crises, tailoring command and control structures to the realities of industrial operations. Finally, *Pillar 4*, **Training and Exercises (T&E)**, involves translating theory into practice, emphasizing hands-on drills, scenario injects, and cross-disciplinary collaboration, so emergency responders, control system specialists, and IT professionals can speak the same language and act in unison.

Cybersecurity within CI sectors

Every nation defines CI sectors based on unique vulnerabilities, economic priorities, and political structures. However, the most common theme for representing the sectors is around national security and the well-being of citizens.

In 2012, a handful of countries, namely, **Australia**, **Canada**, **New Zealand**, the **United Kingdom**, and the **United States**, established a mutual interest group called the **Critical Five**. This group enhances information sharing and works on issues of mutual interest. One of the initial endeavors of the Critical Five involved gaining an understanding of how individual countries approach CI. They developed a collaborative narrative, *Forging a Common Understanding of Critical Infrastructure*, published in March 2014: `https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf`

This publication was intended to disseminate a unified message regarding CI's value, significance, and importance. Various countries defined sectors critical to their nation. The United States of America identified 16 sectors – a few have been discussed in the next section. A complete and current list is available on the **Cybersecurity and Infrastructure Security Agency (CISA)** website.

Table 1.1 provides an overview of the CI sectors, their descriptions, and examples within each sector as recognized by CISA.

CI Sector	**Description**	**Examples**
Chemical sector	The chemical sector involves manufacturing, storing, and distributing chemicals and related products essential for various industries and everyday life.	Chemical manufacturing plants, refineries, and chemical storage facilities.
Commercial facilities Sector	This sector includes facilities where people gather for shopping, entertainment, business, or lodging.	Shopping malls, stadiums, hotels, and office buildings.
Communications sector	The communications sector encompasses the infrastructure and services enabling communication and information sharing.	Telecommunication networks, internet service providers, and broadcast stations.
Critical manufacturing sector	The critical manufacturing sector involves manufacturing industries essential for national defense, infrastructure, and economic stability.	Automotive manufacturing plants, steel mills, and semiconductor factories.
Dams sector	The dams sector includes structures, reservoirs, and related systems used for water storage, flood control, and hydroelectric power generation.	Large dams, reservoirs, and flood control channels.
Defense industrial base sector	This sector consists of companies and facilities involved in designing, producing, and supporting military equipment and systems.	Aerospace manufacturers, defense contractors, and military research facilities.
Emergency services sector	The emergency services sector comprises organizations providing emergency response and public safety services during disasters and crises.	Fire departments, law enforcement agencies, and emergency medical services.

Energy sector	The energy sector involves the production, distribution, and storage of energy resources, including electricity, oil, natural gas, and renewable energy.	Power plants, oil refineries, natural gas pipelines, and wind farms.
Financial services sector	This sector encompasses institutions and systems facilitating financial transactions, investments, and economic activities.	Banks, stock exchanges, insurance companies, and investment firms.
Food and agriculture sector	The food and agriculture sector includes facilities and systems involved in food production, processing, distribution, and agriculture.	Farms, food processing plants, distribution warehouses, and agricultural equipment manufacturers.
Government facilities sector	The government facilities sector involves facilities owned or operated by government agencies at the federal, state, or local levels.	Government office buildings, military bases, and federal courthouses.
Healthcare and public health sector	The healthcare and public health sector comprises organizations and systems providing medical care, public health services, and disease prevention.	Hospitals, clinics, public health agencies, and medical research laboratories.
Information technology sector	The information technology sector includes hardware, software, networks, and data centers vital for information processing, communication, and technology services.	Technology companies, data centers, software development firms, and telecommunications providers.
Nuclear reactors, materials, and waste sector	The nuclear reactors, materials, and waste sector involves facilities and activities related to nuclear energy generation, radioactive materials, and nuclear waste management.	Nuclear power plants, uranium enrichment facilities, and nuclear waste storage sites.
Transportation systems sector	The transportation systems sector encompasses infrastructure, vehicles, and services facilitating the movement of people and goods.	Airports, seaports, railways, highways, and public transit systems.
Water and wastewater systems sector	The water and wastewater systems sector includes infrastructure and facilities providing drinking water, wastewater treatment, and sanitation services.	Water treatment plants, wastewater treatment facilities, sewage systems, and water distribution networks.

Table 1.1 – CI sectors recognized by CISA

Progress in addressing cybersecurity within CI sectors has been slow, but awareness of these threats has significantly increased. This heightened awareness stems from various factors, including the success of preparedness strategies that equip organizations to respond more effectively to incidents. Although challenges remain, CI organizations are becoming better positioned to handle ransomware and other cyberattacks through improved readiness and response measures.

Let's delve deeper into some of the critical sectors in the next section.

An overview of relevant CI sectors

In the previous section, we examined several CI sectors broadly. Now, we will focus on some of the specific sectors in the US where **IACS** play a vital role in operations. These systems are integral to managing and automating processes within industries such as the chemical industry, energy, critical manufacturing, transportation, food and agriculture, and so on.

Note

While this section highlights the sectors themselves, the detailed role of IACS within these environments will be explored in *Chapter 3*, where we examine how control systems support and secure CI operations.

The U.S. **Government Accountability Office (GAO)** report (`https://www.gao.gov/products/gao-24-106221`) underscores the increasing risk of ransomware attacks on critical infrastructure sectors such as energy, healthcare, and transportation, leading to severe financial losses and service interruptions. The GAO calls for improved federal oversight of cybersecurity practices and an assessment of the effectiveness of federal support in reducing these risks.The FBI also highlights this issue, reporting that 1,193 out of 2,825 ransomware incidents targeted critical infrastructure in 2023, with associated financial losses rising by 74% to nearly $60 million: `https://www.aha.org/system/files/media/file/2024/03/fbi-internet-crime-report-2023.pdf`

This section dives deep into the workings of some relevant CI sectors and the potential risks they face. Sectors such as commercial facilities, the defense industry, financial services, and government sectors are not covered in this section.

Chemical sector

The chemical sector is integral to the U.S. economy. It plays a vital role in transforming basic chemicals and raw materials, such as minerals, water, metals, petroleum derivatives, agricultural products, timber, and recycled materials, into the lifeblood of industries, from pharmaceuticals

to energy production, and designing and crafting the building blocks of modern living, from plastics to fertilizers. It also manufactures, stores, uses, and transports potentially dangerous chemicals upon which other CI sectors depend. For example, industries in this sector generally include manufacturers of specialty chemicals, industrial gases, consumer products, and so on.

Figure 1.3 illustrates the chemical manufacturing process at a high level, focusing on the general flow and key phases involved in chemical production.

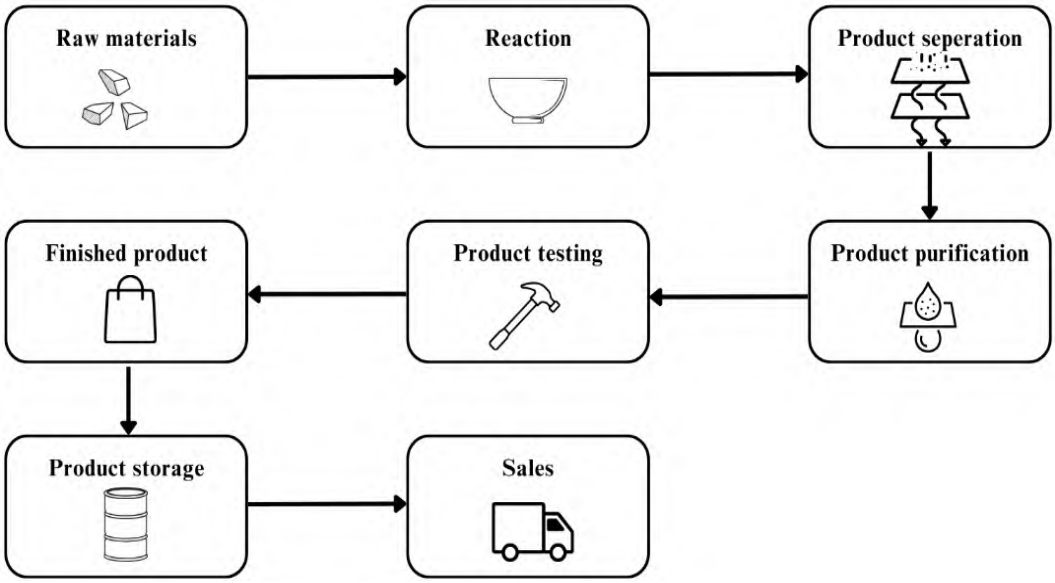


Figure 1.3 – Anatomy of the chemical manufacturing process

The diagram provides an overview of the sequential steps, equipment, and interactions in converting raw materials into finished chemical products. The chemical manufacturing process begins with raw materials that undergo a reaction to form the desired compounds. These are then passed through product separation, followed by purification to remove impurities. Once purified, the materials undergo product testing to ensure quality and standards. Approved products are transformed into finished products, which are then moved to product storage before being distributed through sales channels.

Any interruption in the chemical manufacturing process poses significant economic and safety risks. With tight schedules and reliance on efficient operations, disruptions, whether due to equipment failures, supply chain issues, or other factors, can lead to production delays, decreased output, and revenue losses.

Additionally, given the handling of potentially hazardous substances, deviations from standard procedures or unexpected events can result in accidents, the release of dangerous chemicals, and environmental damage. These incidents not only jeopardize the safety of workers and nearby communities but also entail regulatory fines, legal liabilities, and reputational damage for companies.

Hence, prioritizing robust safety measures, contingency plans, and risk mitigation strategies is essential to minimize the impact of disruptions and ensure the smooth operation of chemical manufacturing processes while safeguarding both the economy and public safety.

Communications sector

This sector is a complex industry of terrestrial, satellite, and wireless systems with many interdependencies. It relies on unseen threads of weaving voices, data, and images across continents to form the essential fabric of global connectivity.

Figure 1.4 shows a typical communication infrastructure consisting of the key components of a telecommunication system, such as transmission and switching equipment, multiplexers/demultiplexers, various transmission media, including copper wires, fiber-optic cables, and wireless radio waves, as well as networking equipment facilitating interconnection between different networks.

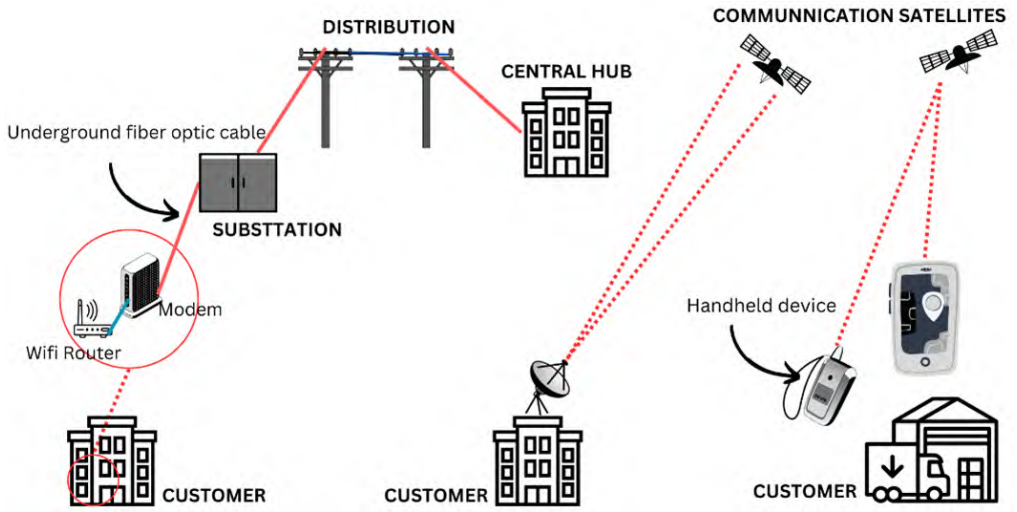


Figure 1.4 – Communication infrastructure

Additionally, **Customer Premises Equipment (CPE)** located at the user's end, such as telephones, modems, and routers, connects to the telecommunication network for data transmission. Distribution infrastructure, comprising cables, wires, and distribution points, ensures the delivery of telecommunication services to consumer locations. Finally, devices such as smartphones, computers,

landline phones, and smart TVs serve as the interface for accessing telecommunication services and communicating with others. This includes traditional phone and internet providers, the **Internet Service Providers (ISPs)** that connect us to the web, the critical infrastructure used by emergency services, and the ever-evolving fiber optic networks that transmit data at lightning speeds.

This sector faces growing risks ranging from cyberattacks (e.g., DDoS, ransomware) and espionage to physical sabotage of cables and towers, natural disasters, and insider threats. With its role as the backbone of global connectivity and support for all other critical infrastructure, securing this sector is essential to ensure national security, economic stability, public safety, and privacy.

Critical manufacturing sector

The critical manufacturing sector is dedicated to recognizing, evaluating, prioritizing, and safeguarding nationally significant manufacturing industries within its domain, considering their vulnerability to human-made and natural disasters. The products crafted by these manufacturing industries play a vital role in supporting various other CI sectors.

Some examples include the medical equipment that keeps us healthy, the metals that form the foundation of our infrastructure, the electrical components that power our homes, the appliances that make daily tasks easier, and the vehicles that help us travel the world.

This sector faces risks that can significantly disrupt operations and impact other critical infrastructure sectors, such as cybersecurity threats targeting industrial control systems, natural disasters damaging facilities and supply chains, and global supply chain disruptions due to geopolitical or logistical issues.

Dams sector

The dams sector plays a vital role in managing water resources across the United States, supporting functions such as power generation, water supply, flood mitigation, navigation, and recreation. Security incidents in this sector can include cyberattacks targeting control systems, physical sabotage of critical infrastructure, or unauthorized access to operational data. Such disruptions can lead to downstream flooding, compromised power supply, or service interruptions that affect entire communities and industries.

Examples include hydropower generation, flood control and management, ecosystem management, and so on.

The dams sector faces risks such as cyberattacks on control systems, physical sabotage, insider threats, and natural hazards. Disruptions could trigger flooding, compromise power generation, or disrupt water availability, with cascading effects on public safety and economic stability. Securing this sector is therefore crucial to ensure resilience, protect lives, and maintain essential services

Emergency services sector

The **Emergency Services Sector (ESS)**, as defined by CISA, encompasses a vast community comprising millions of highly skilled and trained individuals and physical and cyber resources. These resources are crucial in delivering a wide array of prevention, preparedness, response, and recovery services in day-to-day operations and during incident response scenarios. The ESS comprises geographically dispersed facilities and equipment, encompassing paid and volunteer capacities, primarily organized at federal, state, local, tribal, and territorial levels of government.

Examples include fire stations, city police departments, county sheriff's offices, town public works departments, and Department of Defense police and fire departments.

This sector faces risks such as cyberattacks on dispatch systems, physical assaults on facilities, insider threats, and disruptions from natural disasters. Because this sector supports prevention, preparedness, response, and recovery for all other sectors, any compromise could delay emergency response, hinder public safety operations, and erode community trust. Securing this sector is essential to ensure resilience, operational continuity, and rapid response in times of crisis.

Energy sector

This sector encompasses all industries producing, distributing, and consuming energy resources. This complex network can be divided into three segments: electricity, oil, and natural gas.

Some examples include power generation companies, transmission and distribution system operators, oil companies, and natural gas producers.

Security incidents in this sector can manifest as cyberattacks on power grids, oil refineries, or pipeline systems, leading to disruptions in service or safety hazards. Additionally, physical attacks or sabotage on infrastructure can cause widespread damage, impacting energy supply and triggering economic or environmental crises.

Food and agriculture sector

This sector is primarily driven by private businesses, which stretch from the fields of farms to the kitchens of restaurants and the shelves of grocery stores, encompassing everything from growing crops to processing ingredients and storing finished products.

Examples comprise dairy factories, meatpacking plants, refrigerated warehouses, and grain silos.

Security incidents in this sector can involve cyberattacks on food processing systems, which may disrupt production or contaminate products. Additionally, physical security breaches, such as tampering with food storage or distribution, can lead to contamination, product recalls, or harm to consumers. These incidents can have far-reaching consequences on public health and supply chains.

Healthcare and public health sector

The healthcare sector revolves around individual patients, offering services such as diagnosis, treatment, and prevention, including primary care, specialist consultations, and hospitalization.

In contrast, the public health sector emphasizes entire populations, safeguarding the collective well-being through disease prevention, health education, and environmental interventions, such as ensuring clean water and air. Examples include environmental health, primary and hospital care facilities, local health departments, and public health research institutions.

A cyber incident in the healthcare and public health sector has the potential to create chaos and pose a serious threat to public safety. A cyberattack, such as a crypto ransomware hit on a multidisciplinary medical institution, can severely disrupt operations, making it difficult for healthcare professionals to provide medical care, accurate diagnoses, and timely assistance to patients.

Information technology sector

This sector is responsible for creating, supplying, and maintaining hardware, software, and information technology systems and services, including the internet, in collaboration with the communications sector. Due to its intricate and ever-evolving nature, identifying threats and evaluating vulnerabilities in the information technology sector demands collaborative and innovative approaches.

For example, technology companies, software development firms, hardware manufacturers, cloud computing providers, and cybersecurity firms are included.

Security incidents in this sector often involve cyberattacks such as data breaches, ransomware, or **Distributed Denial of Service** (**DDoS**) attacks, which can disrupt services, compromise sensitive information, or incapacitate critical systems. Vulnerabilities in software and hardware can be exploited to access or manipulate vast amounts of data, causing significant financial and reputational damage.

Water and wastewater systems sector

The water and wastewater systems sector is integral to public health, environmental protection, and community well-being. It includes the infrastructure, facilities, and processes that source, treat, distribute, and dispose of water. This sector ensures access to clean and safe drinking water while managing wastewater treatment and disposal to safeguard public health and the environment.

For instance, water treatment plants, stormwater management infrastructure, water quality monitoring systems, water and wastewater facilities, and industrial water management are included. Security incidents in this sector can involve cyberattacks on control systems, leading to disruptions in water treatment or the contamination of drinking water supplies. Physical breaches, such as tampering with water distribution networks or wastewater facilities, can also result in environmental hazards or public health crises, making security in this sector vital for community safety.

Exercise

This worksheet aims to prompt participants to reflect on their responsibilities in safeguarding critical assets within their organization and identify the sector they belong to. Through this, participants gain insight into their role in cybersecurity and their organization's contribution to CI. The exercise helps them pinpoint areas for improving security measures while understanding their organization's broader impact.

Instructions:

- Take a few moments to reflect on your current role and responsibilities within your organization
- Describe in detail your present responsibilities in safeguarding the security of critical assets

Example: IT security analyst

Description of responsibilities: As an IT security analyst within my organization, my primary responsibility is to ensure the protection of critical assets from cyber threats and vulnerabilities. This includes maintaining and monitoring the security infrastructure, conducting regular vulnerability assessments, and implementing security controls to mitigate risks.

Instructions:

- Refer to the list of sectors provided in *Table 1.1*.
- Identify the sector that best aligns with the activities and functions of your organization:

- Describe briefly how your organization supports or belongs to the identified sector
- Provide examples or specific details to illustrate your organization's role within the sector

Example: Sector: transportation infrastructure

Description of organization's role: My organization provides logistical support services for transportation infrastructure projects, including construction and maintenance of roadways, bridges, and transit systems. We collaborate with government agencies and private contractors to ensure the efficient and safe operation of transportation networks.

Specifically, our organization does the following:

- Supplies construction materials, equipment, and machinery for infrastructure development projects
- Offers engineering and consulting services to design and plan transportation infrastructure improvements
- Implements technology solutions for traffic management and monitoring to enhance safety and efficiency
- Provides maintenance and repair services for existing transportation infrastructure assets, such as roadways and bridges

The aim of this exercise is to highlight the importance of CI, which is often overlooked. We often take the safety and security of these CI sectors for granted, yet they are vital for maintaining the quality of our lives. These sectors are where our present thrives, and our future is secured.

Cyber incidents often take place in areas of operation closest to the business or enterprise IT. However, such incidents carry the potential to trickle into industrial networks. Understanding the various real-world examples is key to creating scenarios that are realistic and specific to one's organization. In the next section, we are going to learn about some notable cyber incidents related to CI.

Notable cyber incidents in CI

Several notable cyberattacks have targeted CI, underscoring these essential systems' vulnerabilities and potential risks. Each attack is a valuable lesson, pushing us to develop more robust defenses and build resilience against future breaches. The message is clear: securing our CI is not just an IT issue; it's a national security imperative.

Exploring various cyberattacks on CI sheds light on the intricate challenges, existing vulnerabilities, and the shortage of expertise in safeguarding essential systems.

Table 1.2 provides insights into notable incidents, such as the Stuxnet Worm's impact on nuclear facilities; the Ukraine power grid attacks, revealing the potential for political manipulation; the global havoc caused by the NotPetya ransomware; the sophisticated SolarWinds supply chain attack, emphasizing interconnectedness; and the disruptive consequences of the Colonial Pipeline ransomware attack on vital energy infrastructure. Understanding these incidents is pivotal to addressing the complexities surrounding cybersecurity in critical sectors.

Cyberattack (Year)	**Targeted Sector(s)**	**Impact**
Stuxnet worm (2010)	Nuclear reactors, materials, and the waste sector	This worm, allegedly a joint US-Israeli creation, targeted Iranian nuclear facilities, disrupting centrifuges and delaying their nuclear program. It specifically aimed at disrupting uranium enrichment processes, causing significant damage to Iran's nuclear infrastructure.
Ukraine power grid attacks (2015 and 2016)	Energy sector	In December 2015 and again in December 2016, Ukraine experienced cyberattacks that resulted in power outages. These coordinated cyberattacks plunged parts of Ukraine into darkness, demonstrating the potential for attackers to manipulate CI for political gain.
NotPetya ransomware attack (2017)	Multiple sectors	This ransomware attack masquerading as legitimate software crippled hospitals, government agencies, and businesses worldwide. Although initially disguised as ransomware, NotPetya was later revealed to be a cyber weapon, with the primary target being Ukraine.
SolarWinds supply chain attack (2020)	Multiple sectors	The SolarWinds cyberattack was a sophisticated supply chain attack that compromised the software update mechanism of SolarWinds, a company providing IT management software. This widespread breach serves as a reminder of the interconnectedness of CI and the ripple effects of cyberattacks.

Colonial Pipeline ransomware attack (2021)	Energy sector	This ransomware attack shut down the largest fuel pipeline in the US, causing panic buying and fuel shortages across the East Coast. It exposed the vulnerability of vital energy infrastructure and the potential for economic and societal disruption.

Table 1.2 – Notable cybersecurity events in critical sectors

In this book, you will be examining several high-profile cyberattacks in the form of detailed case studies, each designed to shed light on the steps involved in real-world incidents and the lessons they provide for building stronger defenses. For example, in *Chapter 4*, *Industrial Automation and Control Systems Threat Landscape*, we study the 2015 cyberattack on the Ukrainian power grid, where attackers infiltrated utilities such as Kievoblenergo, causing widespread outages. This case is further dissected through the Cyber Kill Chain framework in the same chapter, helping you understand how each stage of an attack unfolds. Moving forward, *Chapter 5*, *Emergency Operations and Their Significance in an Organization*, explores the Colonial Pipeline cyberattack of 2021, a breach that disrupted fuel supplies across the southeastern United States and exposed vulnerabilities in operational networks. High-profile attacks, like those outlined in the table, emphasize the criticality of cybersecurity and infrastructure resilience in today's digital landscape. While often targeting large entities, they highlight vulnerabilities applicable to any organization.

Lessons from incidents such as Stuxnet, NotPetya, and SolarWinds stress the interconnectedness of digital systems and potential indirect impacts on CI, disrupting essential business functions. Therefore, organizations must prioritize robust security measures, incident management, and proactive risk mitigation strategies to safeguard against evolving cyber threats.

Summary

This chapter revealed the significance of CI, shedding light on its crucial role in supporting modern society. You delved into understanding CI's definition, recognizing its fundamental importance in facilitating essential services such as energy, transportation, and communication. Additionally, you explored the complex network of interconnected systems that constitute the foundation of our daily lives. This solidified your understanding of CI's criticality, paving the way for examining the digital age's challenges and vulnerabilities.

The journey continued by navigating the diverse sectors within CI, each playing a unique and interdependent role. From the pulse of energy grids to the heartbeat of healthcare systems, transportation arteries to the lifeblood of financial institutions, the narrative emphasized their interconnectedness. You learned how disruptions in one sector can ripple through others, driving home the need for robust cybersecurity. A brief overview of real-world examples and scenarios highlighted the crucial nature of safeguarding these sectors and the potential consequences of cyber threats. By appreciating the significance of each CI sector, you gained a deeper understanding of the complex landscape of historical cyber incidents impacting these essential systems.

In *Chapter 2*, *Critical Infrastructure Security and Resiliency*, we will explore how sectors such as energy, transportation, water, healthcare, and information technology are connected and often rely on each other. You will explore the difference between one-way dependencies, such as hospitals relying on electricity, and two-way interdependencies, such as the mutual reliance between energy and transportation systems, and also examine the risks these connections create.

Further reading

- CISA website: Provides a wide range of resources and tools for cybersecurity and infrastructure security and resilience. `https://www.cisa.gov/resources-tools/resources`
- *Critical Infrastructure Security and Resilience Agency*: Offers information, guidelines, and updates on CI security and resilience efforts by CISA: `https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience`
- *A Guide to CI Security and Resilience*: Provides a comprehensive guide to understanding CI security and resilience, including best practices and strategies: `https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf`
- Book - *Andy Greenberg – Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.* (Doubleday, 2019) – Explores Ukraine's power-grid attacks and their global implications.
- Book- *Kim Zetter – Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* (Crown, 2014) – Definitive narrative on Stuxnet and ICS cyber operations.

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

2

Critical Infrastructure Security and Resiliency

The seamless operation of our modern world hangs on an intricate network of **Critical Infrastructure (CI)** sectors, including energy, transportation, water and wastewater, food and agriculture, healthcare and public health, **Information Technology (IT)**, and financial services. These sectors are instrumental in our daily lives, from powering our homes and transporting goods to securing our information. However, this intricate interconnection presents a dual challenge: while interdependencies are essential, they also introduce vulnerabilities, and threats can cascade across sectors, causing extensive disruptions.

Resilience and perseverance are paramount qualities in safeguarding CI. Just as in the realm of sports, where athletes exhibit extraordinary determination in the face of adversity, so too must our infrastructure systems demonstrate the ability to withstand and recover from various threats and challenges.

Figure 2.1 – An athlete facing challenges but persevering without surrendering

Take, for instance, the case of Gabriela Andersen-Schiess, a Swiss athlete who participated in the inaugural women's Olympic marathon at the Los Angeles 1984 Summer Games (`https://www.olympics.com/en/athletes/gabriela-andersen-schiess`). Despite the scorching heat and the resulting dehydration, Andersen-Schiess's refusal to quit the race became an iconic Olympic moment. Her sheer determination saw her staggering over the finish line, symbolizing the power of resilience and perseverance in overcoming obstacles. Similarly, in CI, resilience ensures that systems can adapt and endure, even in the face of unforeseen challenges, thereby maintaining the essential functions upon which society relies.

Hence, this chapter covers some essential topics around critical resources and dependencies. We will cover the following main topics in this chapter:

- Exploring dependencies and interdependencies for CI
- Supply chain security for CI
- Manufacturing infrastructure and connection to supply chains
- Understanding security and resilience for CI
- Laws and regulations for CI
- Evaluating future challenges in CI

Exploring dependencies and interdependencies for CI

It is crucial to define and understand the interdependencies and dependencies within an organization, as this knowledge enables individuals and groups involved in security incident management to better comprehend the potential cascading effects of incidents, prioritize critical systems, and ensure coordinated and effective responses. By understanding these relationships, they can effectively plan for incident recovery and implement security controls to achieve both security and resilience.

Gaps often arise from these interdependencies, whether identified during exercises and drills—topics we will explore thoroughly in *Chapters 10* and *11*—or through risk assessments and audits. This chapter establishes the foundation for understanding the relationships between different sectors and resources, paving the way for a deeper exploration of exercises and drills in subsequent chapters.

A **Dependency** describes a one-way relationship between two elements in CI, where one state directly affects the other.

For example, hospitals depend on a steady supply of electricity from the power grid to operate essential equipment. If the power grid goes down, the hospital's ability to function is compromised.

The following figure illustrates a CI organization relying (D) on two resources:

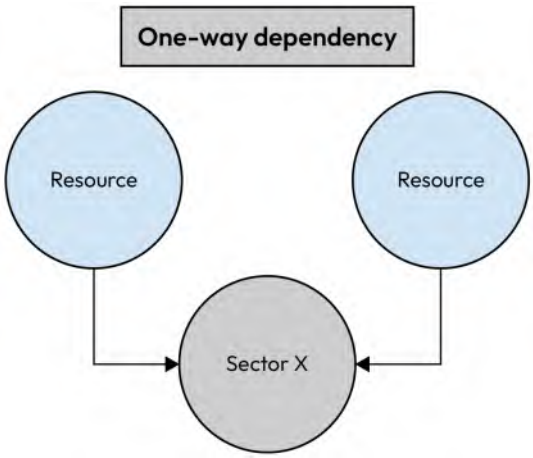


Figure 2.2 – Depiction of a CI organization reliant on two resources

An interdependency involves a more complex, two-way relationship between two or more elements. In this case, each element's state influences the others' state, creating a web of interconnectedness.

For example, the transportation sector depends on the energy sector for fuel to operate vehicles. But the energy sector also relies on transportation to deliver fuel and other resources. Disruptions in either sector can impact the other, creating a cascading effect.

The following figure depicts the **Interdependencies** with other CI sectors:

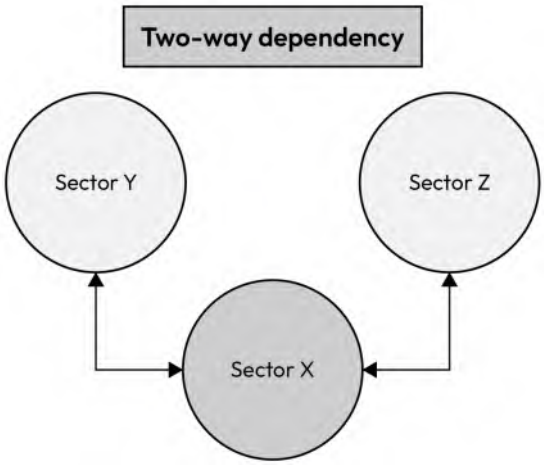


Figure 2.3 – Visualization of interdependencies with other CI sectors

Let us consider a few additional examples provided in the following table. In *Table 2.1*, three distinct sectors are outlined. The *Dependencies (D)* column indicates the sector upon which each respective sector relies, while the *Interdependencies (ID)* column identifies other sectors or industries that depend on the sector in question:

Sector	**Dependencies (D)**	**Interdependencies (ID)**	**Example**
Chemical sector	Energy supply, transportation networks, water resources, raw materials supply chain	Manufacturing and pharmaceuticals, agriculture and fertilizers, oil and gas industry, technology and innovation	(D) The chemical sector heavily depends on a consistent and secure supply chain of raw materials, such as petrochemicals, for its manufacturing processes. (ID) The chemical sector is closely interlinked with the agricultural industry. Chemical products from this sector, particularly fertilizers, are critical in enhancing crop yields and supporting agricultural productivity.
Energy sector	Natural resources, infrastructure networks, technology and innovation	Transportation sector, manufacturing industries, water resources	(D) The energy sector heavily depends on the availability of natural resources, such as crude oil, for the production of petroleum-based fuels, which are a significant source of energy for transportation, industry, and various other applications. (ID) The energy sector is closely interlinked with the transportation sector. The availability and affordability of energy resources, particularly fuels derived from natural resources, directly influence the operational costs and efficiency of the transportation industry.

IT sector	Energy supply, infrastructure networks, hardware and software manufacturing	Healthcare sector, manufacturing industry, communication sector, business and finance sector	(D) The IT sector heavily relies on a stable and continuous power supply to sustain the operation of data centers, servers, and electronic devices. Interruptions or fluctuations in power can lead to disruptions in IT services and data loss. (ID) The IT sector is closely interdependent on the healthcare sector. Electronic health records, telemedicine platforms, and medical information systems rely on a robust IT infrastructure. Simultaneously, advancements in IT contribute to medical research, diagnostic technologies, and the development of healthcare solutions, showcasing the reciprocal relationship between IT and healthcare services.

Table 2.1 – Instances of dependencies and interdependencies in CI

Now that you've visualized how interconnections form the backbone of multiple sectors, it's time to test your understanding. The following exercise helps you distinguish between dependencies, the internal components your operations rely on, and interdependencies, the external systems, organizations, or sectors your success depends upon. Recognizing this distinction is essential for effective incident management and resilience planning.

Exercise 1: Identifying dependencies and interdependencies

The following is the objective: Enhance your understanding of dependencies and interdependencies within your organization's CI. By identifying these relationships, you'll gain insights into the essential elements that sustain your operations and the external links that could affect continuity and recovery.

The following are the instructions: Review the sample components listed *Table 2.2*. For each item, mark whether it represents a dependency or an interdependency by placing an × in the appropriate column:

Component/Example	**Dependency**	**Interdependency**	**More Info**
Fiber optic cables			Internal network backbone, essential for communications
Network infrastructure (routers, switches, servers)			Required to manage internal data flow and operations
Power supply			Electricity needed to sustain operational systems
Equipment suppliers			Dependence on vendors for replacement parts or hardware
Power utility companies			External entity providing consistent power
Internet service providers			Connectivity to external networks and customers
Cloud hosting service			Third-party platform supporting data storage or redundancy
On-site IT support team			Internal staff managing system health and troubleshooting
Transportation and logistics provider			External dependency for material delivery and shipping
Water treatment plant			Municipal/city service supporting industrial processes

Table 2.2: Identifying dependencies and interdependencies

The answers are provided at the end of the chapter.

Note

When tailoring this exercise, identify both dependencies and interdependencies specific to your organization's operations.

Dependencies are the critical internal elements or resources your organization needs to function effectively.

Interdependencies refer to the external factors or entities your organization relies on, such as partners, vendors, or service providers, that influence your ability to operate without disruption.

Identifying dependencies and interdependencies within CI is essential because it reveals how different systems and processes rely on one another. This knowledge enables organizations to anticipate potential vulnerabilities and prepare for disruptions that could impact interconnected components, thereby strengthening their resilience, improving risk management, and creating more effective response strategies.

Another important topic that needs to be addressed is the supply chain within CI. Any disruption in the delivery or supply of essential products and services can have serious consequences that impact safety, security, financial stability, or even national security. These aspects will be explored in more detail in the following sections.

Supply chain security for CI

A supply chain is the interconnected network of people, processes, resources, organizations, and information that enables an organization to source raw materials, support the technology and systems needed to produce products or services, and deliver the final products or services to end customers. While supply chain management has always been a topic of discussion among manufacturers and consumers, in 2019, major industries underwent a stress test on their supply chains and discovered whether they were well prepared or lacking in resilience.

Operations in critical manufacturing can be disrupted by cyberattacks that break supply chain processes. For example, to process and sell milk, a dairy company relies on sourcing milk from internal and external farmers. Any disruption to this small community of farmers can cause reduced milk availability, leading to a shortage in milk production. An ice cream manufacturer, for instance, could suffer immense losses due to this shortage.

Supply chain security is also vital in the context of cybersecurity, especially regarding the suppliers of software and hardware systems. For example, an organization sourcing hardware or computer systems from a manufacturer might face significant challenges due to supply chain disruptions. This was evident during the chip shortage of early 2020, caused by the COVID-19 pandemic and the resulting surge in demand for computers and electronics. This disruption adversely affected manufacturing, as companies relying on the periodic life cycle of their computer hardware experienced performance issues, production losses, and, ultimately, economic instability.

Understanding and having a well-defined supply chain strategy is important because it ensures continuity of operations when disruptions occur. In the following section, we will highlight the necessity for building a supply chain strategy and its importance during incident management.

Building a supply chain strategy

Organizations can start building a supply chain strategy by focusing on visibility and collaboration with their suppliers. The first step is to map the entire supply chain, identifying all suppliers, vendors, and partners involved, including those further down the chain (e.g., your supplier's suppliers). This comprehensive view helps organizations understand the scope of their supply chain and pinpoint potential vulnerabilities that could impact operations.

The next step is to assess risks at each stage of the supply chain. These risks could include financial instability, cybersecurity weaknesses, compliance gaps, or exposure to natural disasters. Conducting regular risk assessments allows organizations to prioritize areas that require immediate attention, ensuring they are prepared to handle disruptions effectively.

Establishing clear communication channels with suppliers is another crucial step. Building strong relationships and setting expectations for transparency and data sharing can improve collaboration during normal operations and emergencies. This also includes agreeing on shared standards for data protection, performance metrics, and response protocols to ensure alignment.

Organizations should also work with their suppliers to define resilience plans. These plans may include identifying alternative suppliers, stockpiling critical materials, or creating digital backups of key data. Proactively preparing for potential disruptions ensures that organizations can adapt quickly to unexpected events.

Finally, investing in technology for supply chain management is essential. Real-time monitoring tools and software can provide valuable insights into performance and risks, enabling organizations to track and respond to issues as they arise.

Importance of the supply chain in incident management

A robust supply chain strategy is crucial for effective incident management. It helps reduce downtime by enabling quick identification of affected areas and faster recovery. Risk assessments conducted earlier in the process help mitigate potential problems, preventing incidents from escalating into larger crises. Strong collaboration with suppliers ensures everyone is aligned and ready to act during disruptions, which strengthens the overall response effort. Ultimately, a well-managed supply chain not only protects operations but also maintains trust with customers and stakeholders.

To illustrate the significance of supply chain security, let us revisit the SolarWinds supply chain attack, one of the most impactful cybersecurity breaches in recent history (`https://www.solarwinds.com/sa-overview/securityadvisory`). In December 2020, the world became aware of this major cybersecurity attack due to the extensive exposure and far-reaching impact of the breach. This attack compromised SolarWinds' Orion software, a widely used platform by public and private organizations to manage and monitor IT resources and assets.

Applications such as Orion are typically maintained through routine updates, including security patches and maintenance fixes. In this case, organizations that subscribed to these updates unknowingly downloaded and installed a maliciously modified patch. The patch was automatically delivered to systems running Orion, effectively introducing spyware and other malicious tools into these environments.

The consequences of this breach were staggering. The compromised patch enabled espionage across various sectors, affecting over a dozen US federal and governmental agencies, 40+ defense contractors and supporting organizations, and more than 18,000 public and private entities globally.

The attackers exploited the trust placed in SolarWinds as a software provider to infiltrate organizations undetected, a tactic that is a hallmark of supply chain attacks. This incident underscores the devastating potential of such attacks, particularly when sophisticated adversaries target CI and sensitive information systems.

Understanding the timeline of this attack—from its initial stages to the ultimate impact—is crucial. Analyzing the attack through the lens of the Cyber Kill Chain provides valuable insights into its various phases.

The concept of the **Cyber Kill Chain** is discussed in detail in *Chapter 4*. Briefly, the Cyber Kill Chain outlines the stages of a cyberattack from initial reconnaissance to the final objective, helping defenders understand and disrupt each phase. It's important to view a cyber incident through multiple lenses, and the kill chain is one particularly useful perspective.

The following table maps the SolarWinds incident against the key stages of the Cyber Kill Chain:

Kill Chain Stage	**Date**	**What Happened?**
1. Reconnaissance	September 2019	Unknown attackers gained access to SolarWinds systems, exploiting vulnerabilities to compromise its software supply chain.
2. Weaponization	February 2020	The hackers tested their attack by injecting trial code. They then inserted the SUNBURST malware into SolarWinds' Orion platform software using a sophisticated method. To avoid detection, the attackers used multiple US-based servers and disguised their activity as normal network traffic.
3. Delivery	March–June 2020	SolarWinds started releasing Orion updates that included the hackers' malicious code.
4. Exploitation	June–November 2020	SolarWinds distributed compromised Orion updates to its customers, inadvertently delivering the malware. When installed, SUNBURST created backdoors within customer networks, granting attackers access.
5. Installation, 6. Command and Control (C2), 7. Actions on Objectives	December 2020–January 2021	Once inside, the SUNBURST malware was activated. It installed backdoor payloads on infected systems and began establishing persistent access while avoiding detection. The malware communicated with attacker-controlled servers, which were disguised to resemble legitimate traffic. These servers issued commands to compromised systems and collected sensitive data. The attackers exploited their access to steal sensitive data, monitor communications, and potentially compromise CI. They targeted high-value entities, including US federal agencies, defense contractors, and private organizations.

Table 2.3 – Mapping the incident across the Cyber Kill Chain stages

This timeline highlights the complexity and sophistication of the attack, emphasizing the critical need for securing supply chains at each stage and implementing robust detection systems.

Manufacturing infrastructure and connection to supply chains

While this book focuses on CI sectors, note that manufacturing industries form the backbone of global industry, producing essential goods and components that drive economies and support these various CI sectors. Therefore, incident management in manufacturing infrastructure involves addressing a wide range of risks, including supply chain disruptions, equipment failures, and cybersecurity threats. Manufacturing companies implement robust supply chain management practices, quality control measures, and risk mitigation strategies to ensure the reliability and efficiency of production processes. Proactive measures such as inventory management, supplier diversification, and business continuity planning help mitigate risks and maintain the resilience of manufacturing operations.

Standards and frameworks also play a crucial role in guiding manufacturing practices and ensuring product quality and safety. For example, ISO 9001 provides guidelines for quality management systems, helping organizations establish processes to meet customer requirements and enhance product consistency and reliability. Adherence to standards such as ISO 9001 helps manufacturers improve operational efficiency, reduce waste, and build trust and confidence among customers and stakeholders.

In the previous section, we looked at some of the dependencies and interdependencies on CI and how identifying these for your organization can strengthen your organization's incident response capabilities. When it comes to the manufacturing sector, these dependencies and interdependencies came to light in the *National Infrastructure Protection Plan and Resource (NIPP) of 2013: Partnering for Critical Infrastructure Security and Resilience*. This plan highlighted the need for a systematic and integrated approach to enhancing the physical security and cybersecurity of CI, and also laid out 12 call-to-action items spread across 3 sections focused on building collaboration and partnerships, innovating risk management, and focusing on outcomes by prioritizing the joint effort of both public and private sectors to track progress and evaluation through lessons learned during exercises and real incidents.

The call-to-action items include the need to analyze CI dependencies, interdependencies, and their associated cascading effects, highlighting how critical manufacturing sector industries are interconnected with various CI sectors, and how they are critical in supporting operations and supply chains. Here is an example to illustrate this further:

- In the energy sector, manufacturing facilities produce equipment and components used in power generation, transmission, and distribution systems, including turbines, transformers, and solar panels

- In the transportation sector, manufacturing plays a key role in producing vehicles, aircraft, and maritime vessels, as well as components such as engines, brakes, and navigation systems
- In the healthcare sector, manufacturing facilities produce pharmaceuticals, medical devices, and **Personal Protective Equipment** (**PPE**), supporting healthcare delivery and pandemic response efforts
- In the telecommunications sector, manufacturing facilities produce network equipment, electronics, and telecommunications devices essential for communication networks and digital infrastructure

Exercise 2: Supply chain risk assessment worksheet

Just-in-time manufacturing, global sourcing, and complex supply networks have only increased the vulnerability of manufacturing supply chains to risks such as natural disasters, geopolitical tensions, and cyberattacks.

Several strategies can be used to identify and take proactive steps to respond to potential disruptions before your organization faces significant challenges. Most of these strategies come in the form of risk assessment of suppliers. Depending on the type of organization, these risk audits can help you recognize potential problems related to raw materials, equipment, replacement parts, and services. *Table 2.4* provides a good starting point.

Organization/ Supplier Name	**Type of Product/Service Provided**	**Contact Information**	**Notes**
ABC Manufacturing	PLCs, HMIs, sensors	Contact: `tech@abc.com`	Tier 1 supplier for IACS components
XYZ Electronics	Control panels, switches	Phone: 123-456-7890	Specializes in custom control panel design
Acme Industrial Solutions	Industrial networking equipment	Website: `www.acmeindustrial.com`	Provides Ethernet switches, routers, and firewalls
DEF instrumentation	Flow meters, pressure transmitters	Email: `support@def.com`	Offers calibration and maintenance services
GHI Automation	Robotic arms, automated machinery	Phone: 987-654-3210	Expertise in robotic integration for manufacturing processes
JKL Maintenance Services	Preventive maintenance contracts	Contact: `support@jkl.com`	Provides on-site maintenance for IACS equipment
MNO Software Solutions	SCADA software, data analytics	Website: `www.mnosoftware.com`	Offers customizable SCADA solutions for IACSs

Table 2.4 – A sample table showing a list of suppliers and contact information for IACSs

Objective: As part of this exercise, identify the various organizations and suppliers providing raw materials, replacement parts, and third-party vendor services, also known as subcontractors, third-party contractors, and service providers, to your organization.

As this is a big undertaking, in our sample table, we have focused on the **Industrial Control and Automation System (IACS)** and related supply chain. However, a similar inventory or resource list should also be developed for all other critical assets and systems that your organization relies on.

Note

While this chapter focuses primarily on the broader concepts of security and resilience, it's important not to overlook the role of supporting subsystems such as IT systems, **Operational Technology (OT)** systems, and physical access control systems. These components, though often viewed as separate technical or operational layers, are closely integrated into the functioning and protection of CI.

Ensuring resilience means more than protecting each system in isolation. It involves understanding how these subsystems interact, identifying their asset owners, and knowing how to prioritize their recovery during incidents. While these topics are explored in more detail in later chapters, you should begin considering how a failure or compromise in one of these areas could ripple through your organization's security posture and operational continuity.

With a foundational understanding of security and resilience in place, the next step is to explore what threatens that state, namely, vulnerabilities and the threats that exploit them, as discussed in the next section.

Understanding security and resilience for CIA is critical. Security is about protection, creating safeguards that reduce exposure to harm. It is the lock on a door, the fence around a facility, or the control you apply to protect valuable assets. Each measure represents a deliberate effort to stay one step ahead of potential threats.

Resilience, as defined by the **National Institute of Standards and Technology (NIST)** *SP 800-172*, is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises affecting systems that rely on cyber resources. In simpler terms, resilience is what allows an organization to bend without breaking and to continue operating despite disruptions.

Achieving security and resilience is no simple task. Both require an understanding of how disruptions in one sector can cascade into others. To strengthen your organization's posture, it is essential to recognize how vulnerabilities and threats interact within your environment. This understanding forms the foundation for effective risk assessments, business continuity planning, and the identification of gaps that need to be addressed.

CI security relies on the interplay of three core elements: physical, cyber, and human. Each must be considered in your organization's incident response and continuity plans, along with supporting subsystems such as IT and IACS. Together, these systems define how prepared your organization truly is when an incident occurs.

In the next subsections, we will explore threats and vulnerabilities, the main forces that challenge both security and resilience, and examine how identifying and addressing them builds a stronger foundation for protecting CI.

Vulnerabilities

Consider a knight in shining armor, appearing invulnerable. However, even the most resilient armor harbors vulnerabilities, those vulnerable points where a well-aimed strike could breach its defenses. Like these weak points in armor, vulnerability in security denotes the susceptibility of individuals, systems, or organizations to potential attacks or harm.

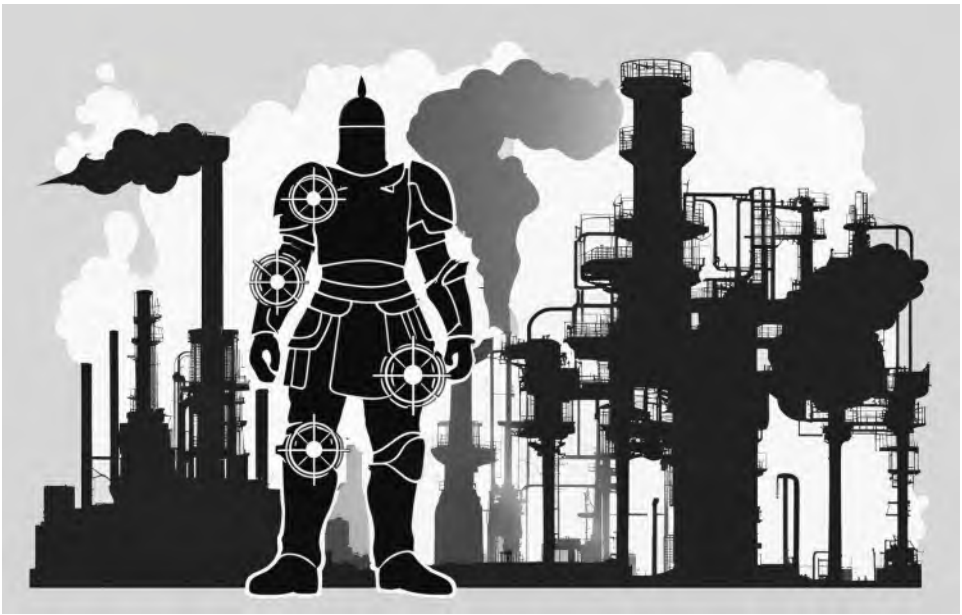


Figure 2.4 – A knight in armor standing against the backdrop of CI

In CI systems, these weak points can manifest in various ways:

- **Aging infrastructure**: Much of our CI is aging and needs repair or replacement, making it susceptible to breakdowns and failures
- **Cybersecurity weaknesses**: Many CI systems are inadequately protected against cyberattacks, leaving them vulnerable to hackers and malware
- **Physical security gaps**: Physical security measures might not be robust enough to withstand deliberate attacks or natural disasters
- **Supply chain dependence**: Dependence on single sources for critical materials or equipment can be disrupted by cyberattacks, accidents, political instability, or trade disputes

Threats

A threat represents the potential for a security breach. In CI, danger arises when a malicious actor or entity exploits vulnerabilities in systems, processes, or personnel, leading to disruptions, incidents, or attacks.

Numerous threats could exist for an organization within the CI space.

Figure 2.5 – A malicious actor against the backdrop of CI

A threat assessment is essential for effective incident planning. Once you've identified the threats to your organization, there are two primary approaches to bolstering incident response and management capabilities:

- The first involves proactive measures, including anticipating scenarios through exercises and practicing procedures.
- The second relies on reacting to actual incidents, which may be a more viable but less preferable option. While valuable lessons can be learned from the reactive approach, the proactive method presents numerous advantages.

Now, let's consider the perspective of a potential threat actor. The dynamic and evolving nature of the threat landscape emphasizes the importance of thinking comprehensively. For instance, vulnerabilities related to physical security or supply chain dependencies might be heightened due to a natural disaster, providing opportunities for exploitation by another bad actor. Therefore, it is crucial to approach security with a comprehensive mindset.

Note

In the context of our discussion, a *bad actor* could be an individual, a malicious group, a nation-state, or even a natural disaster.

Here are a few commonly seen threats to CI:

- **Insider threat**: An insider threat occurs when someone authorized to access your organization's systems, information, or assets misuses that access to harm your security, data, or resources. This person could be an employee, contractor, or business associate.

  For example, in a chemical manufacturing plant, an employee with authorized access intentionally tampers with the production equipment, causing a hazardous chemical spill.

- **Cyberattacks**: Cybercriminals may target CI systems to steal data, disrupt operations, or cause physical damage. Various cybersecurity threats exist, including organized crime, hacktivists, and state-sponsored intelligence agencies.

  For example, a chemical manufacturing facility experiences a cyberattack orchestrated by hacktivists, compromising sensitive operational data and disrupting production processes.

- **Natural disasters**: Extreme weather events such as floods, earthquakes, and hurricanes can damage infrastructure and disrupt essential services within CI organizations.

  For example, a severe flood hits a chemical manufacturing site, damaging equipment and causing a temporary production shutdown due to safety concerns.

- **Physical attacks**: Terrorist attacks, sabotage, or accidental damage can significantly impact CI systems and threaten their functionality and security.

  For example, a terrorist group targets a CI facility, causing a deliberate explosion that damages key infrastructure components and disrupts the facility's operations.

Table 2.5 outlines instances of threats, risks, and vulnerabilities in CI that are crucial for understanding security and resilience within these sectors:

Threat	**Risk**	**Vulnerability**	**Example**
Nation-state cyberattacks Level: Low threat Medium threat High threat **Extreme threat**	Computer malware infecting the critical equipment.	Unpatched Windows OS and IACS vendor software.	Stuxnet (2009–2010), malware infiltrated PLC systems, manipulating them to malfunction and damage the centrifuges.
Insider threat Level: Low threat Medium threat **High threat** Extreme threat	Unauthorized action using privileged access credentials on control equipment.	Inadequate knowledge of process safety.	Field instrumentation technician issues a shutdown command to a piece of equipment, causing upsets in the process and shutting down a unit.
Natural disaster Level: Low threat Medium threat High threat **Extreme threat**	Flooding, disabled critical refrigeration systems.	Lack of protection against common mode failures of critical safeguards or equipment in emergency response plan.	Arkema Inc. chemical plant fire (2017) The plant was submerged in floodwaters, leading to the malfunction of essential refrigeration systems, resulting in the overheating of peroxides and subsequent explosions over several days, releasing toxic fumes and necessitating the evacuation of nearby residents.

Physical security threat Level: Low threat Medium threat High threat **Extreme threat**	Physically infiltrating a power substation.		California power grid attack (2018) Unidentified individuals physically infiltrated a substation near Metcalf, California, manipulating circuit breakers to cause cascading outages impacting over 500,000 people.

Table 2.5 – Instances of threats, risks, and vulnerabilities in CI

A comprehensive view of potential hazards helps stakeholders identify key concerns, conduct risk assessments, and implement effective decision-making processes.

Having explored the importance of understanding threats and vulnerabilities, we will now turn to a practical application. The following exercise will help reinforce the role of threat identification in incident management for CI.

Exercise 3: Identifying vulnerabilities and threats

Objective: The objective of this exercise is to enhance your awareness of vulnerabilities and threats facing your organization. By identifying these potential risks, you can develop more robust defense mechanisms and incident response strategies, thereby strengthening your organization's security posture.

The following are the instructions:

- Review the different methods used to identify vulnerabilities and threats, including vulnerability assessments, physical security assessments, supply chain risk assessments, and competitor analysis
- Reflect on your organization's operations and context to identify potential vulnerabilities and threats across various domains, including cyber, insider threats, and external risks
- Complete the worksheet by listing the identified vulnerabilities and threats, along with brief descriptions of each and their potential impact on your organization

For example, imagine you work for a financial institution. Here's how you might conduct this exercise.

The following are identified vulnerabilities and threats:

- **Cyber threats**:
    - **Phishing attacks targeting employees**: Employees may inadvertently disclose sensitive information or credentials, leading to unauthorized access to the organization's systems
    - **Outdated software and systems**: Legacy systems may contain vulnerabilities that could be exploited by cybercriminals to gain unauthorized access or disrupt operations
- **Insider threats**:
    - **Employee negligence**: Unintentional actions by employees, such as mishandling of sensitive data or clicking on malicious links, pose a risk to the organization's security
    - **Malicious insiders**: Disgruntled employees or those with malicious intent may intentionally leak confidential information or sabotage systems
- **External risks**:
    - **Regulatory changes**: Changes in financial regulations may require the organization to update its compliance measures, potentially leading to disruptions or financial penalties
    - **Economic instability**: Economic downturns or market fluctuations could impact the organization's financial stability and increase the likelihood of fraud or cyberattacks targeting financial institutions

This section covered threats and vulnerabilities, which are the driving factors behind investing time, resources, and funds to implement effective controls that mitigate risks associated with CI incidents, our primary focus.

Additionally, adhering to laws and regulations introduces an extra layer of protective controls, an additional opportunity to strengthen your CI systems and processes. Compliance is not only beneficial for security but also essential for maintaining operational authorization, often referred to as the "license to operate." The importance of laws and regulations for your CI is discussed in the next section.

Laws and regulations for CI

Driven by a surge in cyberattacks, CI regulations have undergone significant transformations in recent years.

Historically, public service entities such as water treatment facilities have lagged behind the consumer and commercial sectors when it comes to implementing stricter cybersecurity regulations. However, the rise of new and disruptive threats, particularly ransomware attacks targeting critical services, has prompted a necessary reevaluation of their cybersecurity posture. Governments worldwide are overhauling existing CI regulations, emphasizing cybersecurity. Examining these evolving regulations across different regions is essential for businesses that have a global presence as the reporting obligations may be different across regions for organizational compliance with federal, state, and security agencies.

The US **Securities and Exchange Commission** (**SEC**), for example, mandates publicly traded companies within CI sectors to adhere to specific cybersecurity requirements. Exploring these regulations will provide organizations with expectations for reporting during incident response.

In the following subsections, we'll take a closer look at some of the key regulations that have been introduced and are relevant to various CI sectors. The goal here isn't to provide an exhaustive list, but rather to highlight the differences and unique aspects of these regulations.

US

The US **Department of Homeland Security** (**DHS**) prioritizes cybersecurity and incident reporting within CI sectors. To achieve this, they've created the **Cybersecurity and Infrastructure Security Agency** (**CISA**). This agency works to strengthen the security and overall resilience of the nation's CI.

NIST offers a valuable resource for CI operators: *Framework for Improving Critical Infrastructure Cybersecurity*. This framework acts as a guide, outlining best practices and recommendations for organizations to effectively manage and mitigate cybersecurity risks.

The **Federal Energy Regulatory Commission** (**FERC**) regulates the cybersecurity of the electric grid and has issued regulations such as the **Critical Infrastructure Protection** (**CIP**) standards.

The **Environmental Protection Agency** (**EPA**) has regulations in place to protect the cybersecurity of the water and wastewater sector.

The **Maritime Transportation Security Act** (**MTSA**) requires security assessments and plans for maritime facilities and vessels.

The **Federal Communications Commission** (**FCC**) has regulations related to the cybersecurity of telecommunications networks.

Europe

The **European Union** (**EU**) has implemented the **Network and Information Security** (**NIS**) Directive, which sets out cybersecurity requirements for operators of essential services and digital service providers.

The **General Data Protection Regulation** (**GDPR**) includes provisions for protecting personal data and imposes obligations on organizations to ensure the security of personal data.

The **European Union Agency for Cybersecurity** (**ENISA**) provides cybersecurity guidance and support to EU member states.

The European Commission has proposed the **Digital Operational Resilience Act** (**DORA**), which aims to enhance the financial sector's resilience to cyber threats.

China

China has implemented the Cybersecurity Law, which sets out requirements for network operators, critical information infrastructure operators, and cybersecurity assessments.

The **National Cyberspace Administration of China** (**CAC**) oversees and enforces cybersecurity regulations in China.

China has also established the **Multi-Level Protection Scheme** (**MLPS**), which classifies information systems into different levels based on their importance and sets corresponding security requirements.

India

India has enacted the Information Technology Act, which includes provisions for protecting electronic data and preventing cybercrimes.

The **Indian Computer Emergency Response Team** (**CERT-In**) coordinates cybersecurity incidents and provides organizations with guidelines and advisories.

The **Reserve Bank of India** (**RBI**) has issued guidelines for cybersecurity in the banking sector.

UK

The UK has implemented the **Network and Information Systems Regulations** (**NIS Regulations**), which transpose the EU NIS Directive into UK law.

The UK government has also published the **Cyber Assessment Framework** (**CAF**) to help organizations assess their cybersecurity risks and implement appropriate measures.

The **National Cyber Security Centre (NCSC)** provides guidance and support to organizations in the UK on cybersecurity matters.

Reporting requirements

In CI sectors worldwide, there is a growing trend toward mandating reporting requirements, emphasizing the need for swift and transparent communication in the face of cyber incidents. The timeframes allocated for reporting have become increasingly stringent, typically 24 to 72 hours after an incident. These reports are also required to provide specific details, encompassing the nature of the incident, the systems affected, potential harm incurred, and the response measures implemented. The precision of this information is crucial for effective response and mitigation efforts. Non-compliance with these reporting mandates carries substantial consequences, including imposing significant fines and possibly criminal charges. As a result, organizations operating within CI sectors are under heightened pressure to adhere to these reporting obligations, recognizing the seriousness of the penalties associated with lapses in transparency and accountability.

Exploring country-specific requirements for reporting during and after a cyberattack is crucial for ensuring compliance and effective incident response in CI sectors. Let's examine how this is addressed in different regions around the globe:

- **US**: The CISA **Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)** mandates reporting within a 72-hour timeframe for cyberattacks impacting critical sectors such as energy, finance, and health. The NIST **Cybersecurity Framework (CSF)** provides the best incident response and reporting practices. Sector-specific regulations, such as those for banking (GLBA) and healthcare (HIPAA), may impose additional reporting requirements.
- **Europe**: The NIS2 Directive necessitates EU member states to enforce mandatory reporting for entities in vital sectors such as energy, transport, and waste management. DORA sets cybersecurity and reporting standards for high-impact entities in essential sectors.

  National regulations within EU member states may introduce supplementary reporting requirements beyond NIS2 and DORA.

- **China**: China's **Critical Information Infrastructure Security Protection Regulation (CI-ISPR)** demands reporting security incidents within a stringent 24-hour timeframe for designated CI operators. The Cybersecurity Law requires entities to collaborate in cyber investigations and report serious incidents promptly.
- **India**: The CERT-In guidelines recommend reporting cyberattacks within 24 hours, particularly for sectors such as power and telecom. Once enacted, the draft CIIP Bill may introduce mandatory reporting requirements for CI sectors.

- **UK**: The NIS Regulations implement NIS2 requirements, compelling mandatory reporting within 72 hours for affected entities. NCSC recommends reporting all cyberattacks, regardless of sector.

Many countries provide hotlines or online platforms for reporting cyberattacks. Third-party service providers may impose their reporting requirements. The specific details reported can vary based on the incident type and sector involved, while international cooperation is encouraged to address cross-border incidents.

Significance of reporting

Understanding the reporting requirements for incidents affecting CI, whether cyber-related or not, is extremely important. These mandates exist for several key reasons, including ensuring timely response, maintaining transparency, and supporting coordinated recovery efforts. In the following subsections, we will explore these various key reasons:

- For swift response and mitigation:
    - **Early reporting**: Prompt incident reporting enables authorities and affected entities to swiftly initiate mitigation measures, potentially minimizing damage and averting widespread disruption
    - **Resource allocation**: Timely reports empower authorities to prioritize essential resources, such as investigators and technical assistance, where they are most needed
    - **Shared awareness**: Reporting contributes to a comprehensive understanding of the threat landscape, enabling authorities to identify trends, predict future attacks, and proactively enhance defenses across the CI ecosystem
- For enhanced preparedness and resilience:
    - **Identifying vulnerabilities**: Incident reports provide valuable data for scrutinizing weaknesses in CI systems and practices, facilitating the patching of vulnerabilities, implementation of improved security measures, and enhancement of incident response plans
    - **Learning and improvement**: Each incident is a valuable learning opportunity that can inform training programs, risk assessments, and future infrastructure development, enabling better preparation for forthcoming incidents
    - **Building trust and transparency**: Open and transparent reporting fosters trust among CI operators, authorities, and the public, enabling better cooperation and communication during incidents and ultimately strengthening societal resilience

- For legal and regulatory compliance:
    - **Avoiding penalties**: Non-compliance with reporting requirements may lead to significant fines and legal consequences. Understanding specific regulations ensures adherence and mitigates the risk of costly penalties.
    - **Maintaining operational licenses**: Certain sectors mandate incident reporting as a condition for retaining operational licenses, safeguarding CI operators from the potential loss of their license to operate.
    - **Contributing to a safer infrastructure**: Collective adherence to reporting requirements fortifies the overall security posture of CI, benefiting all stakeholders and creating a safer and more dependable system for everyone.
- Beyond cyberattacks

  The importance of reporting transcends cyber incidents, encompassing non-cyber events such as natural disasters, equipment failures, and physical sabotage:

    - **Coordinating emergency response**: Timely reports of non-cyber incidents ensure the rapid deployment of emergency responders and resources, minimizing loss of life and property damage
    - **Investigating causes**: Reporting non-cyber incidents facilitates investigations into their root causes, promoting better planning and risk prevention strategies for future occurrences
    - **Sharing operational best practices**: Reporting successes and failures in handling non-cyber incidents allows operators to learn from each other, fostering the development of improved response protocols for various disruptions

One aspect of government oversight carries a very important need for organizations to be able to continue running their operations. Also known as a **license to operate**, it is the authorization that organizations need to legally and ethically conduct their activities. In CI sectors, this entails meeting strict regulatory and compliance standards aimed at safeguarding public safety, security, and the environment.

To maintain this license, organizations must continually adhere to laws and industry standards, along with implementing proactive risk management and security measures. Failing to uphold these requirements can result in legal penalties, but more importantly, it can lead to severe damage to reputation and, ultimately, the inability to operate.

In summary, having a thorough grasp of reporting requirements for incidents in CI, including cyber and non-cyber incidents, is crucial for prompt response, enhancing preparedness, maintaining compliance, and fostering a resilient and secure infrastructure. By actively reporting and analyzing incidents, stakeholders can work together to create a safer and more dependable future for CI and its services.

We'll incorporate some of these requirements into *Chapter 10, Running an ICS Exercise* to help develop appropriate reporting guidelines and ensure they're included in **Incident Management Plans (IMPs)**. To report effectively, it's also important to become familiar with your industry's specific regulations and reporting obligations. The following exercise is intended to support that exploration.

Exercise 4: Government reporting requirements

Objective: The objective of this exercise is to assist organizations in understanding and complying with government reporting requirements related to cyber incidents within CI sectors. By completing this exercise, you can ensure compliance with regulations and gain insights into your organization's crisis communication strategy for the IMP. This will give you a good head start in addressing any gaps and enhancing your incident reporting processes or the development of a communication plan.

The following are the instructions:

- Review the relevant government regulations and reporting requirements applicable to your organization's CI sector
- Identify the specific reporting obligations mandated by these regulations in the event of a cyber incident
- Assess your organization's current practices and procedures for reporting cyber incidents to determine compliance with regulatory requirements
- Complete the worksheet by documenting your findings and any actions needed to enhance compliance with reporting regulations

For example, suppose you work for a telecommunications company in the US. Here's how you might approach this exercise using current reporting obligations under CISA and SEC requirements:

- **Review government regulations**. Begin by reviewing CIRCIA, which requires the reporting of substantial cyber incidents to the CISA within 72 hours.
- **Review SEC regulations**, which mandate that public companies disclose any material cybersecurity incidents on Form 8-K within four business days of determining materiality.

- **Identify reporting obligations**; determine which types of incidents trigger these reporting requirements, such as the following:
    - A ransomware attack or data breach affecting operational systems or customer data may require a CISA report within 72 hours.
    - If the same incident has a material impact on financial performance or business operations, it may also require an SEC Form 8-K disclosure within four business days.
    - Understand the timelines and procedures for reporting incidents, including the required information to be included in incident reports.
- **Evaluate** your organization's existing incident reporting processes to determine whether they align with regulatory requirements:
    - Do you have a documented workflow that ensures the timely escalation of incidents to the compliance or legal team?
    - Is your reporting process aligned with the 12-hour, 72-hour, and 4-day windows specified by these agencies?
    - Are the required points of contact (such as CISA's reporting portal and the SEC filing system) clearly documented and accessible during an emergency?
- **Document** your assessment findings regarding compliance with government reporting requirements.
    - Develop an action plan to address any identified gaps or deficiencies, such as updating incident reporting procedures, providing staff training on reporting protocols, or enhancing incident documentation practices.

This exercise outlined a framework for understanding and meeting cyber incident reporting requirements in CI. Organizations can enhance compliance and improve incident management by identifying regulatory obligations, assessing current practices, and pinpointing areas for improvement. A key aspect of security and resilience is the importance of breaking down silos between IT and OT. So far, this chapter has covered security in detail. The next section will address future challenges, which you will also examine further in *Chapter 4, Industrial Automation Control Systems Threat Landscape*.

Evaluating future challenges in CI

Addressing the evolving challenges of CI demands a dual focus: strengthening defenses against cyber threats and enhancing incident management capabilities. With the complexity of IT/OT integrations and the growing attack surface, the risk of cybersecurity incidents rises significantly. Thus, CI sectors must prioritize developing robust incident management strategies to detect, respond to, and recover from disruptions effectively.

One approach is conducting exercises and workshops simulating cybersecurity scenarios. These activities help identify response plan gaps, evaluate security measures, and refine incident protocols. By engaging in hands-on training, participants gain practical experience, improving preparedness for real-world situations.

Looking ahead, the future of CI underscores the importance of IT, IT/OT integration, and sector convergence. IT plays a central role, facilitating operations and communication. However, integrating IT with OT introduces complexities and vulnerabilities, expanding the attack surface. To navigate these challenges, a strategic balance is crucial, leveraging new technologies while addressing security risks. Advancements offer benefits but also vulnerabilities, necessitating robust cybersecurity measures such as encryption and regular assessments. Additionally, fostering a culture of cybersecurity awareness is vital.

Summary

In this chapter, we focused on the essential task of identifying dependencies and interdependencies within CI, emphasizing how this understanding enhances incident response, speeds up recovery, and reduces the overall impact of cyber incidents. We also clarified the distinctions between resilience and security—highlighting that while security focuses on preventing attacks, resilience prepares an organization to absorb and recover from them. Furthermore, we explored foundational cybersecurity concepts, such as vulnerabilities and threats, along with the vital role of laws and regulations in shaping the security landscape for CI.

With these insights, you can now better identify and manage dependencies, improving your organization's preparedness for cyber incidents. Equipped with a stronger grasp of resilience, security measures, and legal requirements, you will be ready to apply these skills to strengthen CI protection and response efforts.

In *Chapter 3*, *Industrial Automation and Control Systems in Critical Infrastructure* you will explore **Industrial Automation and Control Systems (IACS),** one of the primary pillars of incident management for critical infrastructure.

Answers to Exercise 1:

Component/Example	Dependency	Interdependency	More Info
Fiber optic cables	×		Internal network backbone, essential for communications
Network infrastructure (routers, switches, servers)	×		Required to manage internal data flow and operations
Power supply	×		Electricity needed to sustain operational systems
Equipment suppliers		×	Dependence on vendors for replacement parts or hardware
Power utility companies		×	External entity providing consistent power
Internet service providers		×	Connectivity to external networks and customers
Cloud hosting service		×	Third-party platform supporting data storage or redundancy
On-site IT support team	×		Internal staff managing system health and troubleshooting
Transportation and logistics provider		×	External dependency for material delivery and shipping
Water treatment plant		×	Municipal/city service supporting industrial processes

Further reading

The following is a curated list of online resources tailored to assist readers seeking deeper insights into the reporting requirements and regulations governing CI worldwide. While comprehensive, please note that these resources are not exhaustive. You are encouraged to reach out to your local authorities and governments for more detailed information about specific requirements applicable to your region:

- **US**:
    - **Cybersecurity and Infrastructure Security Agency (CISA)**: Provides guidelines and best practices for managing and reducing cybersecurity risks in critical infrastructure sectors. `https://www.cisa.gov/`.

    - **National Institute of Standards and Technology (NIST)**: Offers the Framework for Improving Critical Infrastructure Cybersecurity. `https://www.nist.gov/cybersecurity`.
    - **Federal Energy Regulatory Commission (FERC)**: Regulates cybersecurity for the electric grid, including **Critical Infrastructure Protection (CIP)** standards. `https://www.ferc.gov/`.
    - **Environmental Protection Agency (EPA)**: Manages regulations safeguarding cybersecurity in the water and wastewater sector. `https://www.epa.gov/`.
    - **Federal Communications Commission (FCC)**: Oversees regulations concerning the cybersecurity of telecommunications networks. `https://www.fcc.gov/`.
- **Europe**:
    - **European Union Agency for Cybersecurity (ENISA)**: Provides cybersecurity guidance and support to EU member states. `https://www.enisa.europa.eu`.
    - **European Commission**: Contains information on the NIS2 Directive and the proposed DORA. `https://ec.europa.eu/`.
    - **General Data Protection Regulation (GDPR)**: Includes provisions for protecting personal data and ensuring cybersecurity. `https://gdpr.eu/`.
- **China**:
    - **National Cyberspace Administration of China (CAC)**: Oversees and enforces cybersecurity regulations in China. `http://www.cac.gov.cn/`.
    - **Multi-Level Protection Scheme (MLPS)**: Provides information on classifying information systems and corresponding security requirements. `https://www.mnr.gov.in/` (In case the website is inaccessible, please use a VPN).
- **India**:
    - **Indian Computer Emergency Response Team (CERT-In)**: Coordinates cybersecurity incidents and provides guidelines and advisories. `https://www.cert-in.org.in/`.
    - **Reserve Bank of India (RBI)**: Offers guidelines for cybersecurity in the banking sector. `https://www.rbi.org.in/`.

- **UK:**
    - **National Cyber Security Centre (NCSC)**: Provides guidance and support on cybersecurity matters. `https://www.ncsc.gov.uk/`.
    - **Cyber Assessment Framework (CAF)**: Assists organizations in assessing their cybersecurity risks and implementing appropriate measures. `https://www.ncsc.gov.uk/collection/caf`.

Part 2

Pillar 2 – Industrial Automation and Control Systems (IACS)

Pillar 2 focuses on **Industrial Automation and Control Systems (IACS)**, which form the operational backbone of critical infrastructure. These environments differ fundamentally from traditional IT systems, prioritizing safety, availability, and deterministic behavior over rapid change.

This pillar examines how control systems, operational technology, and enterprise systems intersect, and why incidents affecting IACS require specialized consideration. Understanding this pillar clarifies why traditional IT security and incident response approaches are often insufficient in industrial environments.

This part of the book includes the following chapters:

- *Chapter 3*, *Industrial Automation and Control Systems in Critical Infrastructure*
- *Chapter 4*, *Industrial Automation and Control Systems Threat Landscape*

3

Industrial Automation and Control Systems in Critical Infrastructure

Industrial Automation and Control Systems (IACS) holds significant importance as it constitutes one of the primary pillars of incident management for critical infrastructure. Moreover, it stands out as a captivating study area due to the surge in connectivity within industrial networks, the automation of industrial processes, the strategic use of data and intelligence by businesses to enhance productivity, and advancements in computing and communication over the past decade. Previously concealed, this sector has now come under the spotlight due to these transformative developments.

Furthermore, the relevance of this topic is underscored by the growing threat posed by hackers who recognize the substantial benefits of disrupting critical infrastructure. The intersection of technological advancements and the strategic targeting of critical systems by malicious actors makes understanding and managing incidents effectively within the context of IACS even more crucial in safeguarding the integrity and functionality of critical infrastructure.

Figure 3.1 – IACS highlighted as one of the pillars of incident management for critical infrastructure

In this chapter, we will explore the essential components of IACS that are crucial for incident management and recovery efforts. This chapter aims to provide insights into the distinctions among enterprise, business, and operations **Information Technology (IT)** and **Operational Technology (OT)** systems, helping you understand the various functions, roles, and responsibilities within IACS.

We will cover the following main topics in this chapter:

- Introduction to IACS
- Types of IACS in critical infrastructure
- Security challenges in IACS

Introduction to IACS

According to *IEC 62443-1-1*, IACS is a "*collection of processes, personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.*"

IACS refers to systems that are responsible for regulating the physical characteristics of a given process. These systems oversee and manage various components, including valves, solenoids, and electrical relays, while offering monitoring capabilities.

The transition from traditionally isolated, manually operated systems to connected and networked automation systems, driven by advancements in both automation philosophies and technology, has increased the susceptibility of numerous IACS components to cyber threats, either through direct targeting or indirect exposure.

In the past, **Industrial Control Systems (ICSs)** operated independently, somewhat shielded from external cyber threats. But with the push toward modernization, incorporating wireless communications, **Industrial Internet of Things (IIoT)**, and cloud technologies, these systems are more interconnected than ever. This convergence, driven largely by adopting standard Ethernet and TCP/IP protocols, has significantly widened the attack surface. It has also exposed industrial systems to a broader range of threats, making them easier targets for attackers who can leverage mature IT tools and established methods of cyberattacks and exploitation already common in traditional IT environments.

Therefore, critical infrastructure organizations must recognize the historical shift in IACS architectures and adopt a proactive and adaptive cybersecurity strategy in safeguarding against the potential cyber threats that could compromise the integrity and functionality of IACS.Before we dive into the various types of IACS, it's important to note that IACS is part of a broader category known as OT systems. OT refers to systems that use control components such as computers, automated machinery, and specialized devices to monitor and manage industrial processes, often reducing or eliminating the need for direct human involvement.

Examples of OT systems include core IACS components such as **Programmable Logic Controllers (PLCs)**, **Distributed Control Systems (DCSs)**, **Supervisory Control and Data Acquisition (SCADA)** systems, **Human-Machine Interfaces (HMIs)**, **Remote Terminal Units (RTUs)**, and industrial analyzers. These systems work in conjunction with essential supporting infrastructure such as network switches, industrial routers, firewalls, protocol converters, engineering workstations, and data historians. Sensors, actuators, and instrumentation also form a critical part of the OT ecosystem, providing the physical interface between the digital systems and the industrial environment.

Figure 3.2 shows a modern-day control room following a similar setup, where operators oversee processes through computer screens.

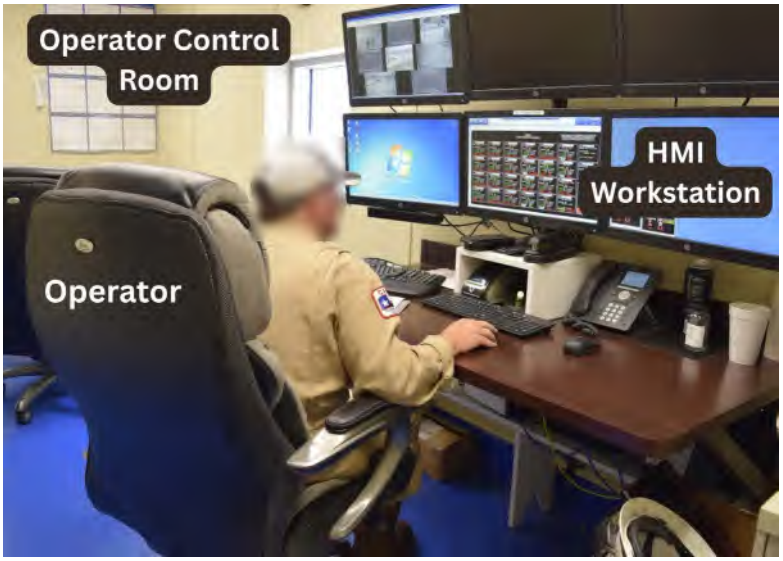


Figure 3.2 – Inside a typical control room of a modern industrial plant

In contrast, older control rooms relied on analog systems, with operators using hand switches, dials, and indicator lights. Illuminated diagrammatic plans were the primary visual displays back then, and orders to the shop floor were transmitted via engine telegraphs.

Figure 3.3 shows an older control room:

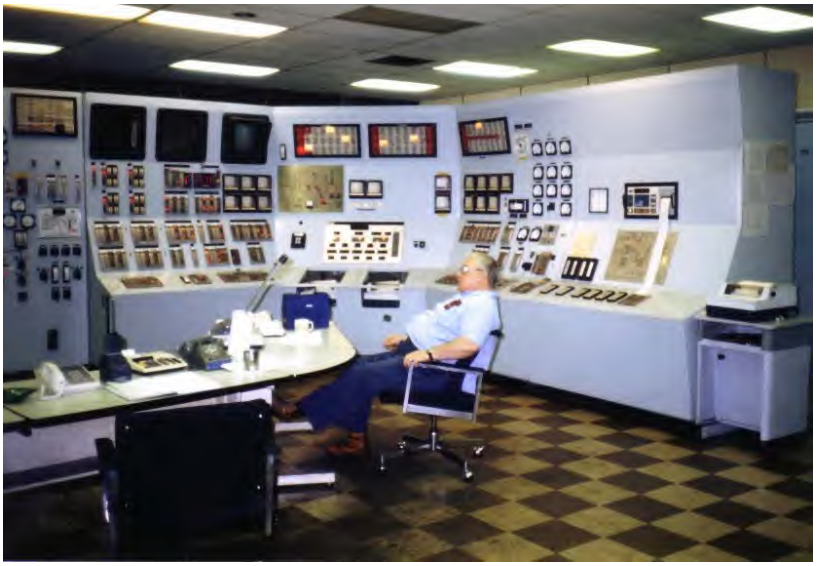


Figure 3.3 – Legacy control room with analog instrumentation

Broad classifications of industrial automation

The primary objectives of IACS are to improve efficiency, reliability, and consistency in manufacturing processes and reduce human intervention in tasks that may be hazardous or repetitive. Industrial automation can be broadly categorized into several foundational components, each playing a vital role in automated operations:

- **Controllers**: These are the central components that manage and regulate the operation of machinery and processes. They receive input from sensors, process that data based on predefined logic or programs, and then send commands to actuators or other devices to control a process or machine. They can include PLCs, DCSs, and other specialized controllers.
- **Field instruments, sensors, and actuators**: These are the eyes, ears, and hands of an automation system. Sensors collect data from the environment, and actuators respond to that data by initiating actions. Together, they form a feedback loop that allows the control system to make decisions and adjust processes. Some commonly found examples include temperature sensors, flow meters, level sensors, control valves, and solenoid valves.
- **HMI**: This is the interface through which human operators interact with the automation system. It includes graphical user interfaces, touchscreens, and other devices that provide real-time information and allow manual control when needed. These are located in protected areas and air-conditioned rooms such as control rooms, operator rooms, and maintenance workshops.
- **Communications networks**: Industrial automation systems often involve communication networks to enable data exchange between different components. This can include wired or wireless communication protocols, which are supported by contemporary network devices such as managed switches, routers, and firewalls.
- **Programming and industrial software**: Automation systems are designed to perform specific tasks and sequences. Software is essential in establishing the logic and behavior of these systems. Examples include PLC programming tools, such as Rockwell Studio 5000 and Schneider's EcoStruxure Control Expert, and DCS software, such as Honeywell Experion and Yokogawa CENTUM. Additionally, other types of software, such as historians, record data, conduct analytics, provide advanced process control applications, and create prediction models.
- **Robots and smart factories and Industry 4.0**: In many industrial automation scenarios, robots perform tasks such as assembly, welding, packaging, and material handling. Industrial robots can operate autonomously or be programmed to collaborate with human workers.

A smart factory is a manufacturing facility that leverages digital technologies to enhance efficiency and productivity. Integrating sensors, actuators, and communication technologies into industrial processes is part of a broader trend known as IIoT. This integration enables increased connectivity, data exchange, and advanced analytics in industrial settings, facilitating the realization of smart factory initiatives. This forms the basis of the *Industry 4.0* era, something that will be discussed in detail in *Chapter 5*.

IACS vs. ICS:

The term Industrial Automation and Control Systems (IACS) is often used interchangeably with Industrial Control Systems (ICS). In the title of this book, you will see references to ICS in this broader sense. However, to maintain clarity and avoid confusion with another commonly used acronym ICS, which stands for Incident Command System, this book will primarily use the term IACS throughout the chapters.

Components of the control system

While broad classifications offer a high-level understanding of IACS, it is essential to grasp the underlying concepts, especially when planning for or responding to incidents. A solid understanding of these fundamentals enables cybersecurity professionals, automation engineers, and incident response teams to identify where a disruption has occurred and how it may propagate across the system. *Figure 3.4* illustrates a simplified representation of an IACS using a layered model. The numbers **1**, **2**, and **3** represent different functional tiers in the control process:

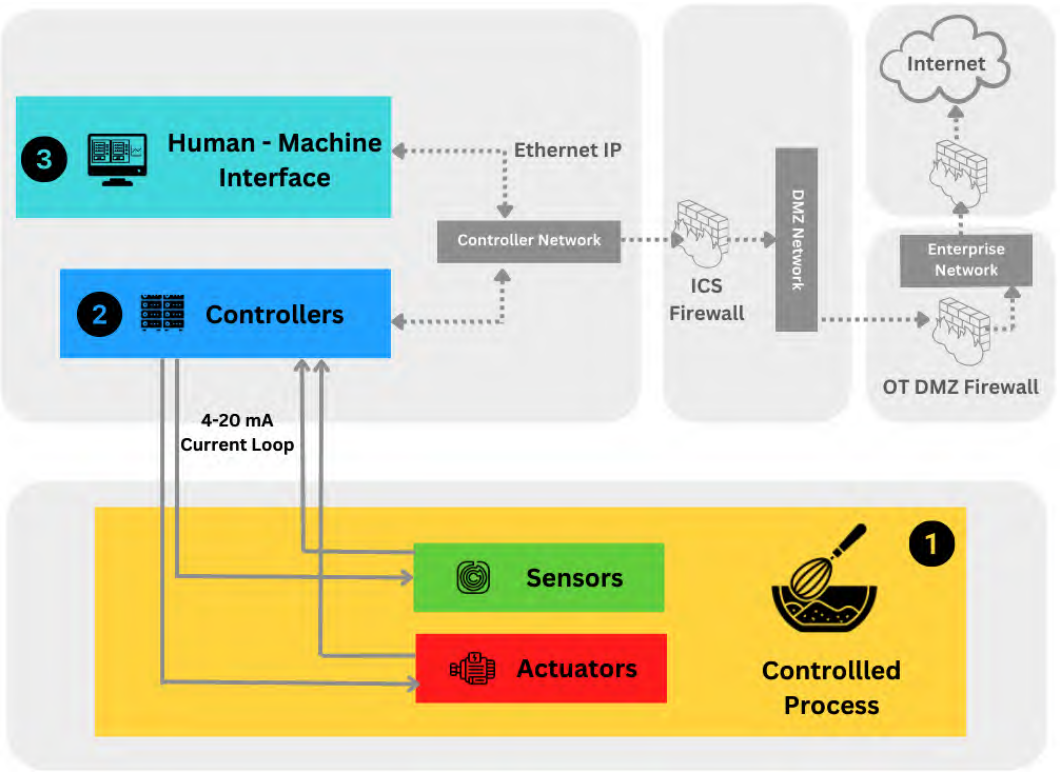


Figure 3.4 – A typical representation of a control system

Let's take a closer look at these three main functional areas:

1. **Controlled process (field level)**

   This is where the physical process takes place, whether it's mixing chemicals, moving a conveyor belt, or opening a valve. Sensors (shown in green) monitor key variables such as temperature, pressure, and flow rate. Actuators (shown in red) respond to control signals by performing actions such as opening a valve or starting a motor. These components often use analog signals, such as the 4-20 milliamp current loop, to communicate with controllers and maintain proper system operation.

2. **Controllers (control level)**

   These systems serve as the brains of the operation. They include devices such as PLCs and DCS. Their role is to collect data from sensors, process it based on control logic, and send commands to actuators. By executing control logic in real time, they help maintain safe, stable, and efficient operations throughout the facility.

3. **HMI (supervisory level)**

   This is the visual interface that operators use to monitor and interact with the system. It displays real-time process data received from the controllers and allows for manual overrides and system configuration when needed. The interface typically connects to the controller network using standard network protocols such as Ethernet/IP, providing a clear window into system performance and control.

Also worth noting are the security zones shown on the right. The ICS firewall plays a critical role by separating the control system network from the corporate or enterprise network, reducing the risk of external threats reaching core operations. The **DMZ**, or **demilitarized zone**, acts as a buffer layer that allows for controlled data exchange. It prevents direct access from the internet into the ICS network, helping to maintain both security and operational integrity.

Various frameworks help define and organize these components. The Purdue model, for example, provides a structured way to separate and manage different levels of industrial operations and IT systems. Similarly, the ISA 99 standard—also known as ISA/IEC 62443—offers a cybersecurity framework specifically designed for control systems, helping organizations identify, segment, and secure critical assets within an OT environment. Both are discussed in detail in the following subsections.

The Purdue model

The **Purdue model**, developed by researchers at Purdue University in the late 1990s, provides a hierarchical structure for control system components. It divides the system into distinct levels, as shown in *Figure 3.5*.

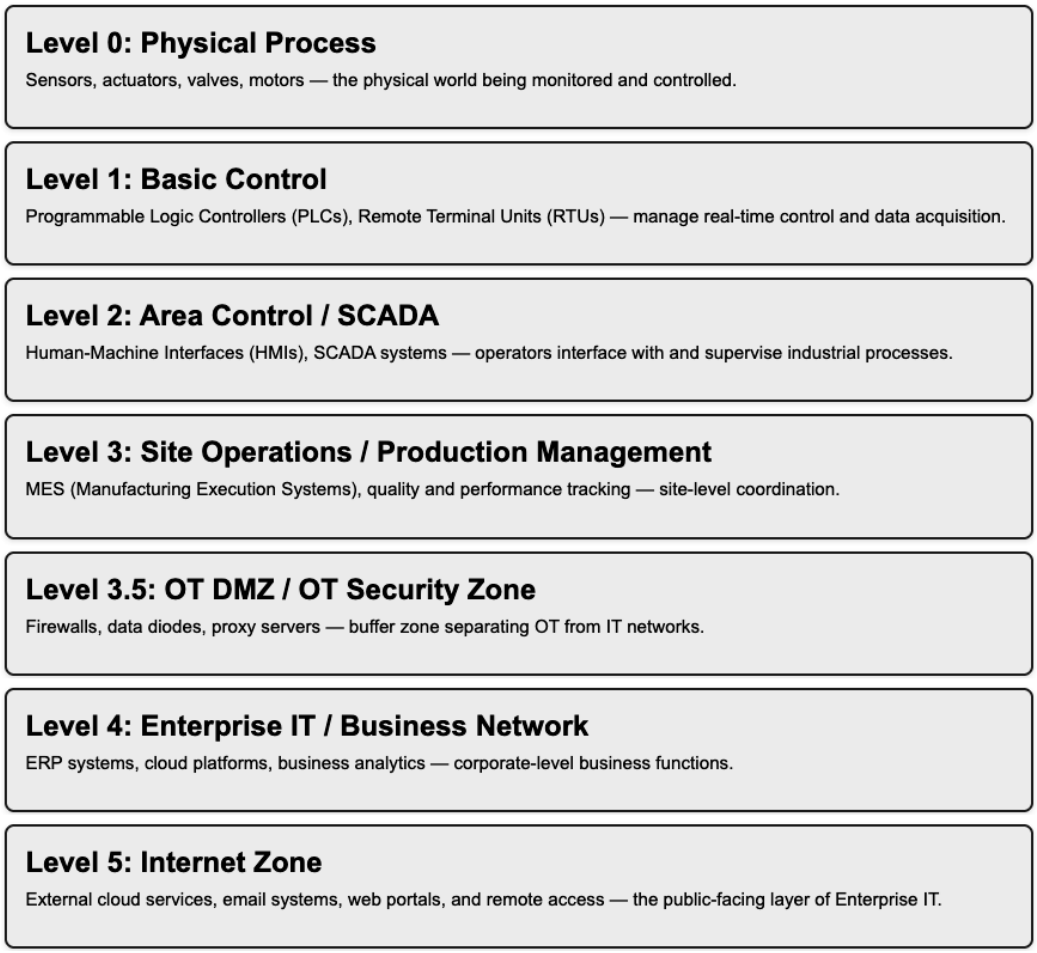


Figure 3.5 – Different levels of the Purdue model

This model is foundational in both industrial automation and OT cybersecurity, especially in defining zones for segmentation, security policies, and risk analysis.

Often confused with the Purdue model, the **Purdue Enterprise Reference Architecture (PERA)** is a broader framework that goes beyond just control systems. PERA addresses the full life cycle of industrial operations, including business processes, organizational functions, and engineering activities. Unlike the Purdue model, which focuses on technical segmentation and control hierarchies, PERA aims to align enterprise goals with operational design and management across an industrial facility.

As you can see, each level has specific roles and responsibilities within the control system architecture:

- **Level 0: Physical Process**: This is the lowest layer and is where sensors, actuators, motors, and field instruments interact directly with the physical environment (e.g., temperature, flow, pressure).
- **Level 1: Basic Control**: This level includes devices such as PLCs and RTUs that execute real-time control logic and interface with Level 0 devices.
- **Level 2: Area Control/SCADA**: This level encompasses HMIs, SCADA systems, and local monitoring tools that supervise the control processes and visualize system performance.
- **Level 3: Site Operations/Production Management**: This level manages workflows, production scheduling, quality assurance, maintenance, and logistics. Systems at this level include **Manufacturing Execution Systems (MES)**, asset tracking tools, and data historians.

The DMZ is often placed between Levels 3 and 4—marked as Level 3.5 in *Figure 3.5*—to act as a secure buffer that facilitates limited and controlled data exchange between the business and operations networks.

- **Level 4: Enterprise IT/Business Network**: This top layer handles business planning, supply chain, financial systems, and enterprise-level analytics. Systems such as **Enterprise Resource Planning (ERP)** platforms reside here.
- **Level 5: Internet Zone**: This layer typically falls outside the scope of business or industrial control networks and is part of the broader enterprise IT environment. It includes services such as cloud platforms, email systems, public-facing web portals, and other internet-based applications.

The ISA/IEC 62443 standard

The ISA/IEC 62443 standard—originally known as ISA 99—provides a robust framework for securing IACS. It introduced the concepts of zones and conduits to logically segment networks and control communication paths between assets, helping manage cyber risk through isolation and well-defined trust boundaries.

While the Purdue model offers a hierarchical view of industrial systems—grouping technologies into layered levels based on function—the ISA/IEC 62443 standard's framework focuses on defining security requirements, roles, and countermeasures for each zone, regardless of its level. In essence, Purdue helps you understand where systems live in an industrial architecture, while ISA/IEC 62443 helps you define how to secure them.

- Together, they provide complementary perspectives: Purdue guides structure and ISA/IEC 62443 guides protection.

  Figure 3.6 shows the main components of the ISA/IEC 62443 standard:

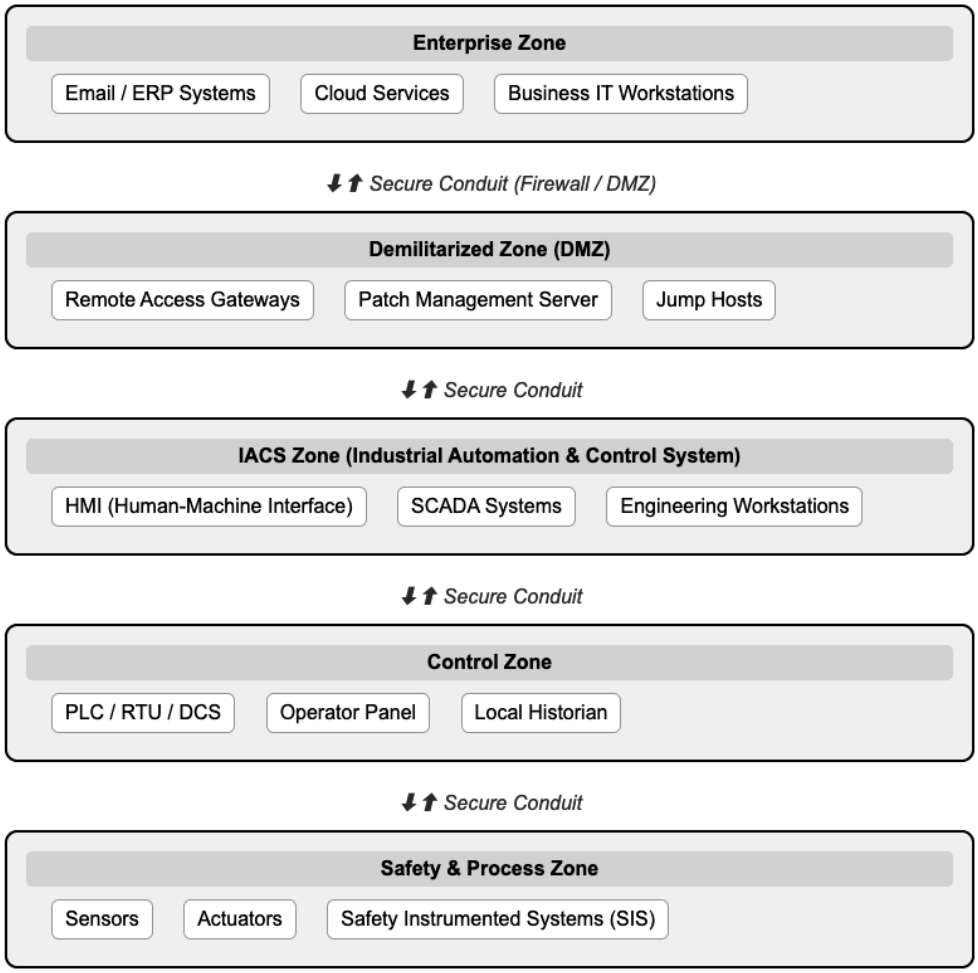


Figure 3.6 – ISA/IEC 62443 zones and conduits

As we can see, each zone groups assets with similar security requirements, while conduits manage and secure the data flows between them. Here's a breakdown of the main zones and how they contribute to securing an industrial environment:

- **Enterprise Zone**: This zone includes systems that support business operations such as ERP platforms, cloud applications, and email systems. While not directly involved in industrial control, this zone often exchanges data with the OT environment and must be separated securely.
- **DMZ**: The DMZ acts as a neutral buffer between the enterprise and control networks. It hosts services that need to interact with both worlds—such as patch servers, jump hosts, and remote access systems—while minimizing the risk of lateral threats reaching critical OT assets.
- **IACS Zone**: This zone houses supervisory and control applications such as HMIs, SCADA systems, and engineering workstations. It serves as the nerve center of industrial operations and requires strict access controls and monitoring.
- **Control Zone**: This layer includes devices such as PLCs, RTUs, and DCSs. These components receive logic instructions and communicate directly with field-level devices to execute process controls.
- **Safety and Process Zone**: This is the lowest and most critical level of the control system and is where physical interaction with the process occurs. It includes sensors, actuators, and **Safety Instrumented Systems (SISs)**, which monitor and protect against hazardous conditions.
- **Conduits**: Conduits are the secure, controlled communication paths between zones. They enforce access rules, encryption, and inspection to ensure that data crossing zone boundaries does not introduce vulnerabilities or bypass security controls.

The ISA/IEC 62443 series is composed of multiple parts, each addressing a specific aspect of industrial cybersecurity. Here is a breakdown:

- **ISA/IEC 62443-1-1**: Terminology, concepts, and models
- **ISA/IEC 62443-2-1**: Establishing an IACS security program
- **ISA/IEC 62443-2-2**: Security program requirements for IACS service providers
- **ISA/IEC 62443-3-1**: Security technologies for IACS
- **ISA/IEC 62443-3-2**: Security risk assessment and system design
- **ISA/IEC 62443-3-3**: System security requirements and security levels
- **ISA/IEC 62443-4-1 and 4-2**: Secure product development life cycle and component requirements

In particular, ISA/IEC 62443-3-3 is widely used to define cybersecurity requirements for ICSs and to evaluate system security levels.

While this overview introduces the foundational concepts and zone-based architecture of ISA/IEC 62443, a full exploration of the entire standard and its implementation guidelines is beyond the scope of this book. The following section explores the various types of IACS and highlights their importance within your organization. Understanding the different types of IACS is essential for managing and protecting critical infrastructure effectively.

Types of IACS in critical infrastructure

IACS is used in various industries and critical infrastructure to monitor and control industrial processes. There are several types of IACS, each designed for specific applications. Let's take a closer look at the main ones.

SCADA systems

SCADA systems are essential for monitoring and controlling industrial operations across dispersed geographic areas. These systems offer real-time visibility and control, enabling centralized oversight of field equipment such as pumps, relays, sensors, actuators, and process controllers.

SCADA is used extensively in industries such as water and wastewater treatment, oil and gas, electric power transmission and distribution, manufacturing, and transportation systems. It is especially valuable in environments where operations are spread out or located in hard-to-access areas, making manual monitoring and control inefficient or impossible. By reducing downtime, minimizing waste, and improving safety, SCADA plays a pivotal role in ensuring the reliable and efficient operation of critical infrastructure.

The architecture of a typical SCADA system includes the following aspects:

- **Field devices**: These include sensors and actuators that interact with the physical process (e.g., pressure sensors, flow meters, valve actuators)
- **RTUs and PLCs**: These interface with field devices, collect data, and execute local control logic
- **Modems and communication interfaces**: These facilitate communication between the field and the central control system
- **Control centers**: These include the local control base stations and the regional control centers, which oversee operations, analyze incoming data, and issue control commands

Figure 3.7 illustrates a simplified SCADA system, including two field sites connected via Modbus-based communication to a central gateway:

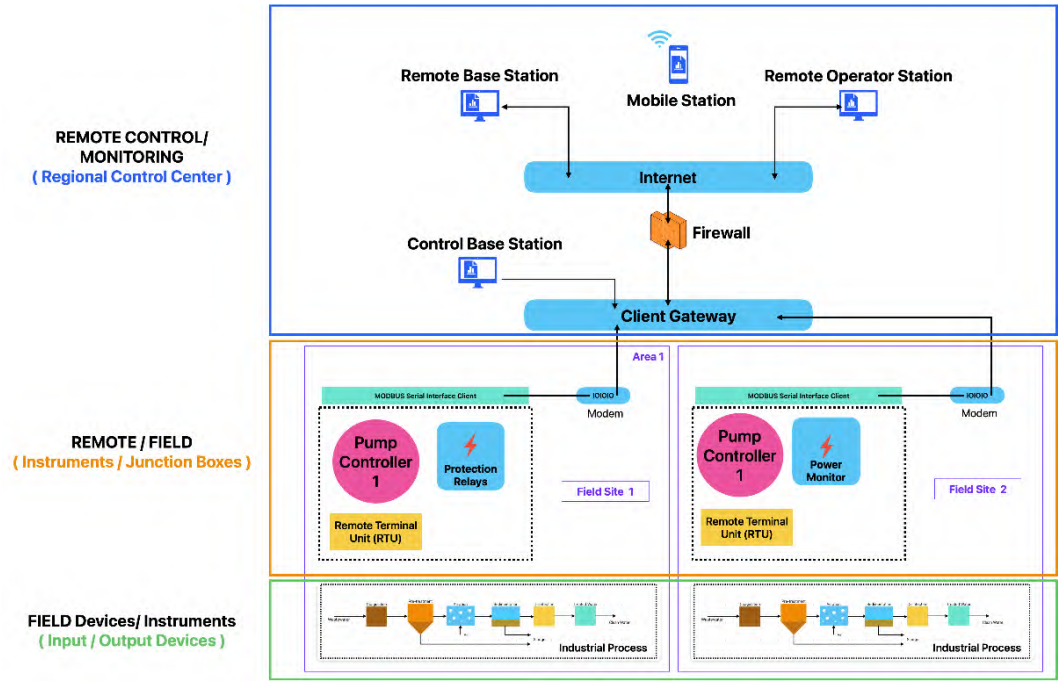


Figure 3.7 – A simplified version of a SCADA system

A firewall protects the client gateway, which connects to both local control stations and remote monitoring platforms (e.g., operator and mobile stations) over the internet. RTUs at each field site connect to protection relays, pump controllers, and power monitors, demonstrating how various components collaborate within a distributed control environment.

Communication protocols in SCADA

While Modbus is one of the most widely adopted protocols in SCADA systems due to its simplicity and interoperability, it is not the only option. The following are some other industrial communication protocols that can be used:

- **Distributed Network Protocol 3 (DNP3)**: Commonly used in electric utilities for secure, reliable communication
- **IEC 60870-5-101/104**: Used in European and international utility SCADA systems

- **Profibus/Profinet**: Popular in factory automation for high-speed communication between controllers and field devices
- **EtherNet/IP**: Based on standard Ethernet, this is often used in Rockwell Automation environments
- **BACnet and LonWorks**: Typically used in building automation

Modbus itself is available in two serial formats known as Modbus ASCII and Modbus RTU, as well as Modbus/TCP, which runs over Ethernet. As industrial networks evolve, many legacy systems still rely on serial communication, making device servers and protocol bridges critical for integrating legacy systems with modern SCADA architectures.

For example, a serial Modbus RTU-based pump controller can be connected to an Ethernet-based SCADA system using a serial-to-Ethernet converter, such as an IO-LAN Device Server. These tools help bridge communication between old and new systems, enabling centralized control without complete infrastructure replacement being required.

This section provided an overview of a SCADA system's components and communication protocols. More advanced configurations, including network security, redundancy, and protocol interoperability, are beyond the scope of this section.

Distributed Control Systems (DCSs)

A DCS is a control system where control elements are distributed throughout a system rather than being centrally located. They are commonly used in manufacturing and process control industries.

DCSs are integral in various industries for monitoring and optimizing complex processes. For instance, DCSs ensure precise control of chemical plants' overreactions, mixing, and separation processes. Furthermore, power generation facilities rely heavily on DCSs to operate turbines and generators efficiently, ensuring optimal electricity production and distribution. Whether in chemical or power industries, DCSs are pivotal tools for real-time coordination, enhancing safety, and optimizing overall efficiency. *Figure 3.8* shows the key components of a DCS, highlighting their physical layout across different operational zones.

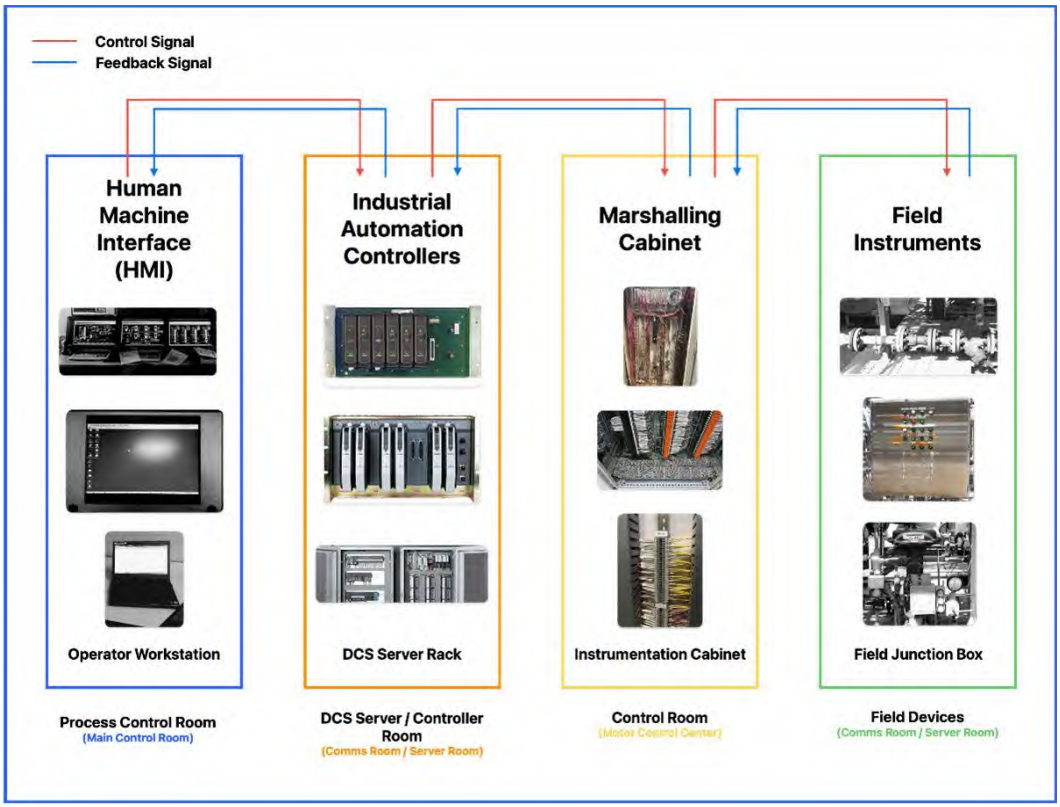


Figure 3.8 – The standard elements of a DCS

The architecture of a typical DCS is designed to distribute control logic, enhance reliability, and allow for scalable process management. The preceding figure illustrates four main functional areas:

- The **main control room (Blue box/first box from the left)** is the central hub where operators interact with the system through computer systems with the help of a keyboard and mouse. It usually consists of **operator workstations (HMIs)**, which provide visualization of real-time plant processes, alarms, trends, and manual control capabilities. Engineering workstations are used to configure, deploy, and manage the control logic, perform diagnostics, and update process graphics or controller firmware.

  Monitoring terminals or laptops are also sometimes used by maintenance personnel or engineers to troubleshoot or make temporary control modifications.

- **Controller and processing units (Orange box/second box from the left)** are located in secure environments such as communication rooms. These consist of DCS controllers/**Central Processing Units** (**CPUs**), which execute the control logic and PID loops defined by engineering stations. These are ruggedized for industrial applications. Another important component is the input/output modules, which act as the interface between the field signals and control logic, converting analog/digital inputs into actionable control parameters.
- The **motor control center (Yellow box/third box from the left)** contains electrical and control wiring that's located within the field termination panels, which serve as junction points for signals coming from field instruments. Other routing components, such as relay panels and terminal blocks, facilitate signal routing to and from actuators such as motors, solenoids, or contactors. Other electrical systems that can be considered protection devices or safety systems are housed within the control cabinets. These cabinets contain the cabling, interlocks, fuses, and power supplies needed to energize field devices and implement safety interlocks.
- **Field and input/output devices (Green box/fourth box from the left)** are located in the comms room or field panels. This is where the physical process is connected. Some of the most commonly found field devices are in the form of transmitters and sensors, which are responsible for measuring variables such as temperature, pressure, flow, and level. Control devices such as actuators and final control elements—such as valves, drives, and motors—carry out control commands from the DCS. Any automation system is incomplete without manual and bypass controls, which are also located near the field devices in the local panels and allow manual overrides or status checks in case of remote system failure.

The arrows in *Figure 3.8* denote signal or data flows:

- Arrows going from left to right represent control and data signals from DCS controllers to field instruments and actuators
- Arrows going from right to left represent monitoring and feedback data from field instruments back to the operator and engineering stations

This modular layout of a DCS, where each function is physically and logically separated, supports enhanced fault tolerance, scalability, and real-time process control across large-scale industrial environments.

PLCs

PLCs are ruggedized computers that are used for industrial automation. They are programmable and can control various processes and machinery on the factory floor.

PLCs are indispensable in various industries, offering automation and control capabilities tailored to specific processes. For instance, in manufacturing, PLCs oversee assembly lines, optimizing production efficiency and ensuring stringent quality control. The automotive industry relies on these controllers to regulate diverse manufacturing processes, from machining to assembly, thereby contributing to the precision and reliability of production lines.

Notably, while DCSs and PLCs serve vital roles in industrial automation, a key distinction lies in their scope. DCSs are typically employed for complex and continuous processes across an entire facility, providing centralized control and monitoring.

In contrast, PLCs focus more on specific, discrete tasks within a process or machine, offering decentralized control. This distinction highlights their complementary roles in enhancing operational efficiency in different industrial settings.

Let's consider a water treatment plant to illustrate the application of DCSs, PLCs, and SCADA systems.

PLCs come into play for specific tasks within the water treatment process. For example, PLCs could control the pumping station, regulating water flow from the source to the treatment facility. Additionally, PLCs might be deployed to automate specific equipment, such as valves and pumps, ensuring efficient and reliable operation.

Figure 3.9 shows the standard elements of a PLC implementation. It highlights three main areas within a typical PLC-based architecture:

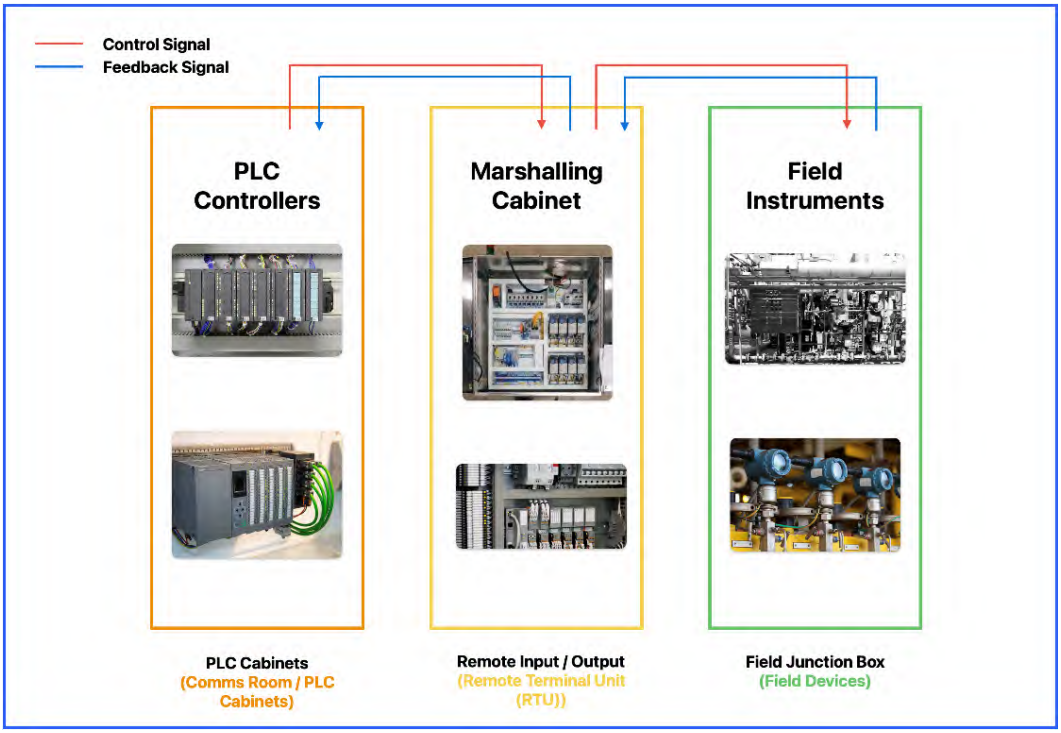


Figure 3.9 – The standard elements of a PLC

Let's take a closer look at the three main functional areas shown in this figure:

- **Comms Room/PLC Cabinets**: This section houses the core PLC hardware, including the main controller modules, power supplies, I/O cards, and communication modules. These components are typically mounted inside industrial-grade cabinets located in communication rooms or local control panels. The PLC hardware shown here provides the central processing and communication functions needed to control equipment in the field.
- **RTU**: This section acts as the intermediary between the PLC system and field equipment. It contains terminal blocks, circuit breakers, relays, and wiring used to receive signals from sensors or send commands to actuators. These cabinets are usually closer to the actual process or machinery, helping to decentralize and distribute control while minimizing wiring complexity.
- **Field Devices**: This section represents the actual instruments and equipment installed in the field. Devices such as transmitters, pressure sensors, flow meters, control valves, and pump motors are shown here. These field devices collect real-time data and execute physical actions, as instructed by the PLC.

The arrows in *Figure 3.9* indicate the typical direction of communication and control signals:

- Arrows going from left to right represent command or control signals being sent from the PLC or RTU to field devices
- Arrows going from right to left represent monitoring or feedback signals coming from field devices that go back to the RTU and PLC

This setup demonstrates a standard implementation of a PLC-based automation system, with centralized hardware in secure enclosures and distributed interfaces that connect to real-world equipment in the field. The modular and scalable nature of this design makes it well-suited for applications where discrete control, reliability, and flexibility are essential.

Other forms of IACS

IACS is intricate and versatile, with diverse applications leading to the development of several types. These systems are often named based on their application or to describe a particular implementation approach. It's crucial to highlight additional IACS systems that play significant roles in various industries:

- **Building Automation Systems (BASs)**: BASs are used to control and monitor building systems such as **Heating, Ventilation, and Air Conditioning (HVAC)**, lighting, and security. While not exclusively industrial, these systems are crucial in critical infrastructure.
- **Process control systems**: These systems are designed to control and monitor continuous processes such as chemical manufacturing, oil refining, and power generation.
- **Integrated control systems**: These systems integrate multiple control disciplines, such as process control, motion control, and discrete control, into a single platform for more comprehensive automation.
- **SIS**: An SIS is specifically designed to ensure the safety of industrial processes. It involves implementing safety controls and emergency shutdown systems to mitigate potential hazards.
- **Power Management Systems (PMS)**: PMSs are used in power plants to monitor and control electrical power generation, transmission, and distribution.
- **Telecontrol systems**: These systems monitor and control geographically dispersed facilities. They are common in utilities and energy distribution.

It's important to note that the specific types and configurations of IACS can vary widely depending on the industry and the nature of the controlled processes.

Now that we've explored what IACS is, along with its core components, such as DCSs, PLCs, SCADA systems, RTUs, and field devices, and looked at how they are applied across various industries, it's important to shift our focus. With these systems playing such a critical role in operations, they naturally become high-value targets.

In the next section, we'll examine the unique security challenges that exist within the ICS ecosystem that differ significantly from those in traditional IT environments. From legacy systems and protocol vulnerabilities to physical exposure and limited patching windows, understanding these risks is the first step toward building resilient and secure industrial operations.

Security challenges in IACS

IACS often lacks robust defenses against contemporary cyber threats. Understanding these security challenges is crucial for building resilience and ensuring effective **Incident Response (IR)** and **Incident Management (IM)** during attacks.

One scenario that often comes to mind, especially in regions near the equator, is a hot summer evening when the power suddenly goes out, plunging entire neighborhoods into darkness. Homes fall silent, refrigerators stop, and the steady hum of air conditioners disappears. As the blackout spreads, frustration and confusion set in.

Now, imagine that this isn't just a routine outage, but a deliberate cyberattack—one that takes advantage of vulnerabilities in the IACS at the core of a power plant.

This scenario isn't fiction. In 2016, a cyberattack disrupted parts of Ukraine's power grid, leaving hundreds of thousands of people without electricity for hours. Similar incidents have affected power plants, water treatment facilities, and other critical infrastructure around the world.

Such attacks are especially concerning due to the unique security challenges within IACS environments. Unlike standard IT systems, IACS often relies on legacy technologies, lacks built-in security features, and is typically isolated from traditional IT networks. While some organizations have made progress in modernizing operating systems, computing platforms, and network infrastructure, keeping these systems up to date remains difficult. This is especially true in environments where uptime requirements are strict, or where upgrading to newer technologies is not practical or even possible. As a result, many systems cannot support modern security controls, leaving vulnerabilities exposed and giving attackers opportunities to disrupt critical operations.

This makes implementing the right controls critical, starting with training the personnel who operate, manage, and interact with OT systems. Additionally, setting up strong perimeter defenses such as firewalls, DMZs, and zero-trust policies to restrict access paths, along with strategies for resilience, such as proper network zoning and incident response planning, form the first line of defense against cyberattacks on IACS.

To better understand the security challenges facing IACS, it helps to take a closer look at the areas within critical infrastructure where these threats commonly emerge. The following subsections focus on the specific challenges IACS faces, from network architecture and workforce limitations to supply chain risks, IT/OT integration issues, regulatory pressures, and the evolving threat landscape. These challenges not only expose underlying vulnerabilities but also highlight the complexity of securing modern industrial environments.

Network challenges

The core of IACS relies on communication networks. Like a crucial blood vessel, these networks have vulnerabilities that can open the whole system to attack. Let's delve into the shaky parts of network vulnerabilities and explore three essential areas:

- **Insecure protocols**: Consider the analogy of sending sensitive messages on a postcard, which are susceptible to interception by anyone passing by. This analogy aligns with the vulnerability of insecure protocols such as Modbus and DNP3, both of which are commonly utilized in IACS communication. These protocols lack essential security features such as encryption and authentication, rendering them susceptible to eavesdropping and manipulation.
- **Insufficient network segmentation**: Visualize a scenario akin to a medieval castle with only one inadequately guarded gate. This metaphor reflects the security concern of an unsegmented network in IACS. The coexistence of critical control systems with administrative and guest traffic creates an environment where attackers can move laterally, potentially gaining access to sensitive areas.
- **Unauthorized access**: Consider a concealed backdoor in a castle to grasp the risk associated with unauthorized access. Weak passwords, misconfigured devices, and a lack of access control present potential entry points for attackers into the network. This unauthorized access could lead to data theft, operational disruptions, or even critical systems being compromised.

Human factors and insider threats

Human factors form the core elements of organizational functionality. Picture them as a trio comprising the guidelines for doing things (process), the individuals executing these tasks (people), and the tools and technology supporting these activities. The process involves considering situations where people might make mistakes due to factors such as tiredness or stress, potentially posing a risk to the system. Simultaneously, addressing insider threats means being vigilant about the potential harm that can be caused by individuals with insider access, whether it's fueled by personal grievances or financial motives. Ensuring the seamless collaboration of these three elements is vital for organizational security and effectiveness:

- **The double-edged sword**: Visualize a seasoned operator swiftly optimizing a refinery process. They act as the guardian of the control panel, using their expertise to handle unexpected issues. However, like a warrior equipped with a suboptimal sword, human vulnerabilities, such as over-reliance on technology and a lack of security awareness, can become significant security challenges.
- **Mistakes happen**: Picture a technician unintentionally installing harmful software on a maintenance computer—a small error with potentially major consequences. Furthermore, factors such as tiredness, stress, insufficient training, or confusion about complex instructions can lead to unintentional mistakes, such as misconfigurations, protocol violations, or attempts to access unauthorized areas.
- **Watch out for insider threats**: A disgruntled employee, well-versed in the system, could exploit their knowledge to cause trouble. Insider threats come in various forms, from resentful employees seeking revenge to individuals attempting to profit by leveraging their authorized access. These threats can sidestep initial defensive measures, making them particularly tricky to address.

Supply chain risks

Supply chain risks pose significant threats to IACS, often introducing vulnerabilities before equipment even reaches the plant floor. For example, a compromised firmware update from a trusted vendor or a third-party software library with hidden backdoors can slip into critical systems undetected, undermining the integrity of essential infrastructure. Imagine building a robust SCADA system with strong physical security, only for you to discover hidden backdoors in the hardware or critical flaws in third-party software. These vulnerabilities don't usually originate from the plant itself; they come through the supply chain. For instance, a vendor may ship PLCs with compromised firmware, a supplier might include counterfeit hardware components, or an

integrator could unknowingly embed open source libraries with known exploits. Or, imagine building a robust SCADA system with strong physical security, only to discover hidden backdoors in the hardware or critical flaws in third-party software. These vulnerabilities don't usually originate from the plant itself, they come through the supply chain. For instance, a vendor may ship PLCs with compromised firmware, a supplier might include counterfeit hardware components, or an integrator could unknowingly embed open-source libraries with known exploits. Because these elements enter the environment through trusted vendors and suppliers, they represent classic supply chain risks to IACS. Such scenarios underscore the intricate challenges that are embedded in the supply chain and affect IACS.

Addressing sneaky hardware issues involves uncovering hidden problems in components such as **Field-Programmable Gate Arrays (FPGAs)** or **Application-Specific Integrated Circuits (ASICs)**. Because these chips are often designed or manufactured by third parties, a malicious actor could embed covert logic during production, leaving *backdoors* that stay dormant until triggered. This makes them a supply chain risk as organizations may be shipping or operating devices with compromised hardware before the issue is even detectable. Additionally, third-party risks arise from using **Software Development Kits (SDKs)** with known vulnerabilities or libraries with unpatched **Common Vulnerabilities and Exposures (CVEs)**. These vulnerabilities create weaknesses, exposing the entire system to potential attacks. Adopting smart sourcing practices becomes crucial in navigating these risks; this includes thoroughly checking vendors' security practices, scrutinizing software development processes, and demanding transparent information about the supply chain. Identifying and mitigating potential issues early is an essential step in fortifying the security of IACS.

Legacy system challenges

Legacy systems in IACS are aging structures, often decades old, and lack the security features needed for today's digital threats. Updating their software is challenging when manufacturers no longer provide support; this exposes them to known exploits such as the Stuxnet worm, which targets specific controllers. Furthermore, integrating modern security measures with these systems is difficult and expensive due to compatibility issues. Maintaining these systems relies on aging experts, and when they retire, a skills gap emerges, making it challenging to keep them secure.

Regulatory compliance and standards

Handling regulatory compliance and standards in IACS is a challenging process that involves following the specific rules for your industry. It can be akin to figuring out a puzzle because the requirements are complex. At the same time, meeting the security standards to protect IACS from

different threats needs a flexible approach. Staying compliant means actively trying to avoid new threats, quickly fixing problems, and always being ready to adapt. The cybersecurity world keeps changing, so keeping up with regulations in IACS isn't just about following the rules now; it's about expecting and adjusting to the new things industries might need in the future.

Integration of IT and OT security

Addressing the integration of IT and OT security poses a complex task. Bridging the gap between these realms involves overcoming challenges to align security practices and safeguard enterprise IT and IACS environments. It's akin to ensuring that the digital side of the business and the technology controlling industrial processes work together seamlessly, sharing information without compromising security.

The emergence of newer technologies

The emergence of the **Internet of Things** (**IoT**) and its industrial counterpart, IIoT, has transformed the way devices and systems interact. By connecting sensors, machines, and applications, these technologies enable smarter decisions and greater efficiency, but they also introduce new challenges. When a connected device is compromised, the impact may spread beyond traditional IT or OT boundaries, making it difficult to pinpoint the source or contain the issue. To understand why this matters, it is important to look at what IoT is, why it came into existence, and how IIoT extends these concepts into industrial environments.

IoT refers to the growing network of everyday devices and systems connected to the internet, able to collect, exchange, and act on data. It came into existence to extend computing and connectivity beyond traditional computers and phones, allowing devices such as smart thermostats, wearable health trackers, vehicles, and household appliances to interact intelligently. The core idea was to improve convenience, efficiency, and decision-making by integrating sensors, processors, connectivity, and applications into physical objects.

At a high level, as shown in *Figure 3.10*, IoT systems are made up of four main components:

- Sensors/devices, which are used to collect data (temperature, pressure, motion, etc.).
- Connectivity for these devices for transmitting data (Wi-Fi, Bluetooth, cellular, LPWAN, etc.).
- Data processing via the edge or the cloud. Since these devices produce a large amount of data, the data needs to be analyzed and converted into meaningful insights.

- Applications/interfaces, which provide the true value for end users or other systems to interact with the processed data and to make decisions for the business and its operations.

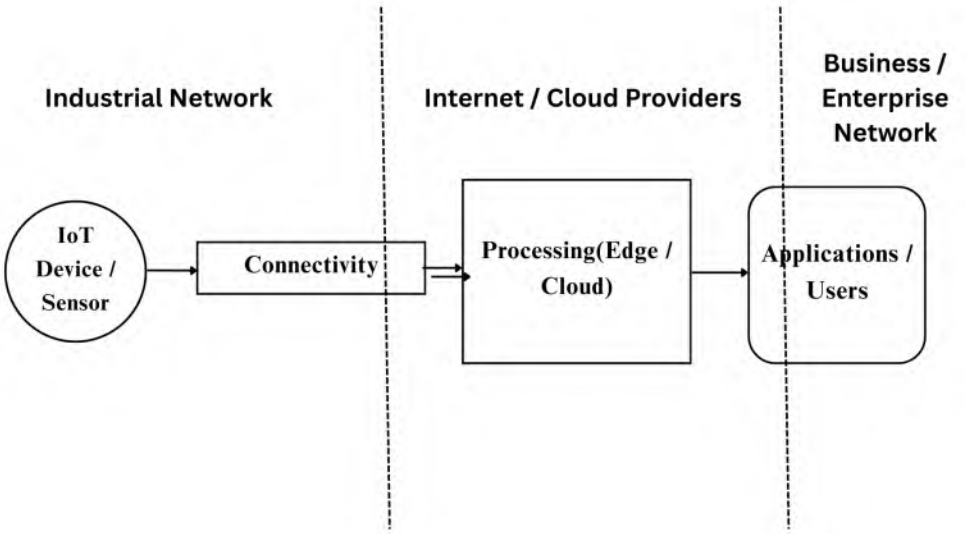


Figure 3.10 – IoT architecture at a glance

An example of an IoT system is a smart city traffic system where cameras and sensors detect congestion, feed the data to cloud systems, and adjust traffic lights in real time to improve flow. Another example is a connected healthcare device, such as a wearable heart monitor that streams patient data to doctors for proactive treatment. While there are many other examples in the commercial world, in the next section, we will focus on industrial systems so that when the same concept is applied to industrial settings, it becomes IIoT.

IIoT integrates smart sensors, devices, and advanced analytics into industrial environments such as factories, power plants, chemical processing units, and logistics systems. The goal is to enhance operational efficiency, predictive maintenance, safety, and overall reliability in critical infrastructure. For example, vibration sensors on rotating equipment can detect anomalies early, allowing maintenance to take place before a catastrophic failure occurs.

As depicted in *Figure 3.10*, IoT and IIoT environments can also be understood across three connectivity layers. At the base is the industrial network, where devices and sensors reside, gathering data directly from machines, equipment, or the surrounding environment. This information is transmitted using wireless connectivity such as GSM, LoRaWAN, 5G, or other communication technologies to the internet or cloud layer, where edge computing and advanced processing take

place. The processed insights then move into the business or enterprise network, where applications and systems use the data to deliver value, whether through improved decision-making, predictive maintenance, or streamlined operations.

While IoT and IIoT bring intelligence and connectivity into consumer and industrial devices, OT and IACS represent the foundational systems that already monitor and control physical processes. IIoT builds on these by adding connectivity, cloud-based analytics, and AI-driven optimization, but unlike traditional IoT, it must meet much stricter safety, reliability, and availability requirements.

Emerging threat landscape

Navigating the evolving threat landscape in IACS poses a dynamic challenge in terms of incident management and response. The changing nature of cyber threats, including the rise of sophisticated malware and the increased frequency of ransomware attacks, significantly impacts critical infrastructure security. Moreover, the potential impact of nation-state-sponsored cyber activities adds another layer of risk to the resilience of essential systems.

Additionally, the integration of **Artificial Intelligence (AI)** into both industrial systems and adversarial toolkits introduces new challenges for incident management. Unlike traditional malware, AI-driven threats can continuously adapt and learn from defensive measures in real time, making them elusive and difficult to contain. For example, imagine a compromised FPGA inside a turbine control module that quietly hosts an embedded AI routine. Once activated, it could analyze operator commands and sensor data on the fly, selectively altering readings to mask abnormal conditions while gradually manipulating setpoints to push equipment toward unsafe states. In such a scenario, defenders would not only be dealing with a hardware-based backdoor but also an intelligent adversary capable of evading signature-based detection and even mimicking normal process behavior.

An FPGA is an integrated circuit that can be configured by the user even after it has been manufactured. Unlike ASICs, which are built for a single fixed purpose, FPGAs are reprogrammable and flexible, allowing engineers to adapt them for different functions or update them as system needs change. This versatility is what makes them valuable across many industrial and critical infrastructure applications.

Preparing for this level of sophistication requires proactive strategies such as anomaly detection tuned for adaptive behavior, layered monitoring across hardware and software, and incident response playbooks that anticipate AI-driven manipulation so that critical operations can remain resilient against future intelligent threats.

In the upcoming exercise, you will test your knowledge by identifying IACS within your own environment, with example answers provided. This step is important because knowing where IACS components exist and how they connect to critical operations is the foundation of effective incident management.

Exercise

Objective: The objective of this worksheet is to enhance your understanding of IACS within your organization's critical infrastructure. In this guided exercise, you will identify IACS components, types, security challenges, and vulnerabilities, and then apply scenario analysis to propose mitigation steps.

Instructions: Review each section and provide relevant information based on your organization's setup and infrastructure. For each exercise, fill in the blanks with accurate details and examples applicable to your organization's IACS.

Section A: Understanding IACS in your organization

1. Provide a brief explanation of what IACS means in the context of your organization.

   Example Answer: In our organization, IACS refers to the integrated systems responsible for monitoring and controlling critical processes in our manufacturing facilities. These systems automate tasks, manage equipment, and ensure operational efficiency:

IACS	Manufacturer	Unit Area
PLC- FA-M3	Yokogawa Electric Corporation	Chemical pulping
SIMATIC SCADA Systems	Siemens	Power distribution area

Table 3.1: Sample IACS table

1. Provide examples of IACS components in your organization.
2. *Example Answer*: Examples of IACS components in our organization include PLCs, HMIs, and SCADA systems.

Section B: The main uses or applications of IACS in your organization's critical infrastructure

1. Name types of IACS and how they are utilized in your organization's critical infrastructure.

   Example Answer: The types of IACS that are utilized in our organization's critical infrastructure include SCADA systems for monitoring and controlling our power distribution network, and PLCs for regulating production processes in our manufacturing plants

2. Briefly outline the primary functions of the identified types within your organizational context.

   Example Answer: SCADA systems monitor energy distribution, PLCs automate manufacturing processes, and DCSs coordinate chemical production operations, ensuring efficiency and safety.

Section C: Security challenges in your organization's IACS

1. Share your understanding of security challenges concerning IACS within your organization.

   Example Answer: Security challenges concerning IACS in our organization include vulnerabilities to cyberattacks, outdated software that's still supported by the IACS vendor, inadequate access controls, and not using multi-factor authentication.

2. Identify vulnerabilities that IACS in your organization may face.

   Example Answer: Vulnerabilities in our organization's IACS include unpatched software, default passwords, a lack of encryption—some of the data may be in cleartext—and insufficient network segmentation. IACS and business systems might have connectivity that could enable the lateral movement of a cyberattack.

3. List all individuals with access to the IACS, specifying their roles and corresponding access levels.

   Example Answer: Individuals with access to our IACS include engineers, operators, and maintenance staff, each assigned specific roles and access levels based on job responsibilities.

The following is an example RACI chart for IACS access:

Role/Individual	Access Level	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Control system engineers	Full system configuration and admin rights	System configuration, patching, and architecture changes	System integrity and design decisions	With operators, maintenance, and IT security	Management and compliance
Operators	HMI access, process monitoring, and control commands	Daily operation and monitoring	Safe operation during shifts)	With engineers for system changes, with maintenance for outages	Shift supervisors and management
Maintenance staff	Limited system access, troubleshooting, patching, and firmware updates	Field device replacement, patching, and system health checks	Maintenance activity effectiveness	Engineers for configuration, operators for downtime scheduling	Management, with operators for when downtime occurs
OT security officer	Read and audit access, security monitoring tools	Security monitoring, incident response, and log reviews	Compliance and risk management	With engineers, operators, and IT security)	Plant management and compliance teams
Plant/operations manager	Oversight, reporting access	–	A (Overall operational accountability)	C (Engineers, Operators, OT Security)	I (Executive Leadership)
IT/network admin (OT DMZ support)	Network/firewall configuration, segmented access	Network security controls and firewall rules	Secure connectivity between IT/OT zones	Engineers and the OT security officer	Management

Table 3.2: Sample RACI chart

The following is an example document containing the RACI matrix to be included:

Role/Individual	Access Level	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Control System Engineers	Full system configuration & admin rights	System configuration, patching	System integrity & design decisions	With Operators, Maintenance, IT Security	Management, Compliance
Operators	HMI access, process monitoring, control commands	Daily operation & monitoring	Safe operation during shifts	Engineers for system changes, Maintenance for outages	Shift Supervisors, Management
Maintenance Staff	Limited system access, troubleshooting, patching	Field device replacement, patching	Maintenance activity effectiveness	Engineers, Operators	Management, Operators
OT Security Officer	Read & audit access, security monitoring	Security monitoring, Incident response	Compliance & risk management	Engineers, IT Security	Plant Management, Compliance
Plant/Operations Manager	Oversight, reporting access	—	Overall operational accountability	Engineers, Operators, OT Security	Executive Leadership
IT/Network Admin (OT DMZ support)	Network/firewall configuration, segmented access	Network security controls, Firewall rules	Secure IT/OT connectivity	Engineers, OT Security	Management

R = Responsible **A** = Accountable **C** = Consulted **I** = Informed

Figure 3.11: Sample RACI matrix

Section D: Application exercise for your organization

1. Create a fictional scenario involving IACS in your organization's critical infrastructure.

   Scenario analysis: A fictional scenario involves a cyberattack targeting our SCADA system, disrupting power distribution, and causing widespread outages:

   - **Scenario 1**: A hacker spends several days probing a company's network until they manage to steal valid ICS operator credentials. Using these, they log into the SCADA system that controls power distribution and insert a malicious program, which triggers outages by switching breakers and altering setpoints. The company's security team eventually detects the unusual activity and begins responding.
   - **Scenario 2**: In this scenario, during a severe storm, a hacker targets a city's water treatment plant. They exploit vulnerabilities in the plant's control systems, gaining unauthorized access. The hacker then manipulates the system to release excess chemicals into the water supply, causing contamination. As a result, many residents fall ill after consuming the contaminated water. Authorities investigate the incident and discover the cyberattack. The water treatment plant enhances its cybersecurity measures to prevent similar attacks in the future.

2. Identify potential security challenges and propose basic mitigation steps based on your organizational setup.

   Answer: Basic mitigation steps include conducting a risk assessment, updating software patches, enhancing network security measures, and providing cybersecurity training to staff.

Creating scenarios like the ones outlined in this exercise is a crucial aspect of cybersecurity preparedness for organizations. By envisioning potential cyber threats and attacks, security analysts can better understand the vulnerabilities within their systems and infrastructure, assess risks, and devise effective mitigation strategies.

Additionally, developing scenarios with timelines allows organizations to simulate and run exercises and drills, helping them prepare for real-life incidents, test their incident response capabilities, identify weaknesses, and refine their procedures to enhance overall cybersecurity readiness.

Summary

This chapter introduced the foundational concepts of IACS and its critical role in modern industrial environments. We explored how IACS differs from traditional IT systems and examined the various components, architectures, and frameworks that define these systems. This chapter highlighted the growing need for adaptive security strategies and proactive incident management in light of increasing connectivity and technological integration. We also looked at the vulnerabilities and evolving risks that make securing IACS both essential and challenging.

In *Chapter 4*, we'll take a deeper dive into the specific security challenges facing OT environments, examining areas such as network architecture, IT/OT boundaries, supply chain risks, and regulatory pressures. We'll also explore the OT Cyber Kill Chain to better understand how attacks unfold and where defenses can be most effective.

Futher Reading

- *ICS Training through CISA*: CISA offers free training programs and resources designed to help professionals enhance their understanding of Industrial Control Systems (ICS) security and operational resilience. `https://www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa`
- *edX Manufacturing Courses*: Provides open online courses on manufacturing systems, industrial automation, and the digital transformation of industry , ideal for understanding the broader context of IACS. `https://www.edx.org/learn/manufacturing`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

4

Industrial Automation and Control Systems Threat Landscape

In the previous chapter, we explored the foundational concepts of **Industrial Automation Control Systems** (**IACS**) and their pivotal role in **Critical Infrastructure** (**CI**) and modern industries. We explored the diverse types and components of IACS deployed across energy, transportation, and manufacturing sectors. Moreover, we examined the security challenges encountered by IACS, especially in CI, shedding light on their vulnerabilities and the prevalent threats they confront.

This chapter examines the multifaceted challenges inherent in IACS and places them within the broader **Operational Technology** (**OT**) context. It highlights why organizations must clearly define what constitutes their IACS in order to determine appropriate security levels and understand the potential impact of cyber threats. You will also learn about the Cyber Kill Chain, a crucial framework that is instrumental in identifying and understanding the stages of a cyberattack. We will also be looking into the distinctions and parallels between **Information Technology** (**IT**) and OT domains, so we can better allocate resources during incident management through the following topics:

- Introduction to IT and OT
- Understanding security considerations for OT systems
- Security considerations for OT systems
- Case study of an OT security incident
- The significance of the Cyber Kill Chain in incident management

Introduction to IT and OT

IT and OT form the backbone of modern industrial systems. While IT focuses on data processing, communication, and business systems, OT governs the physical processes that keep industries running monitoring sensors, controlling actuators, and ensuring safety and continuity in production. These two domains, once separate, now operate side by side in what we call Industry 4.0, where digital intelligence meets industrial automation.

The roots of this convergence stretch back to the Industrial Revolutions, from steam and mechanization in *Industry 1.0*, to electrification and mass production in *Industry 2.0*, to the rise of computing and automation in *Industry 3.0*. The current era, *Industry 4.0*, is defined by cyber-physical systems, Internet of Things (IoT), and Industrial IoT devices that blend IT's analytical capabilities with OT's real-time control. Technologies such as digital twins, artificial intelligence, and augmented reality now bridge the gap between virtual design and physical operation, offering unprecedented insight and efficiency.

However, this integration also brings new challenges. As organizations connect legacy systems with modern networks, they introduce *interoperability gaps* and security risks. A single compromised IoT device or misconfigured control system can trigger cascading impacts across entire operations. This is where incident management becomes critical—requiring collaboration between IT and OT teams to detect, respond to, and learn from disruptions.

Before exploring the specifics of IT, OT, and their respective security domains, it is important to understand the broader discipline they all stem from—**Information Systems (IS)**. IS represents the integrated study of people, processes, and technology working together to collect, store, analyze, and distribute information in support of decision-making and operations across an organization, with the goal of supporting both business and operational goals. *Figure 4.1* shows how IS encompasses several interrelated domains, including **Computer Information Systems (CIS)**, IT, and OT:

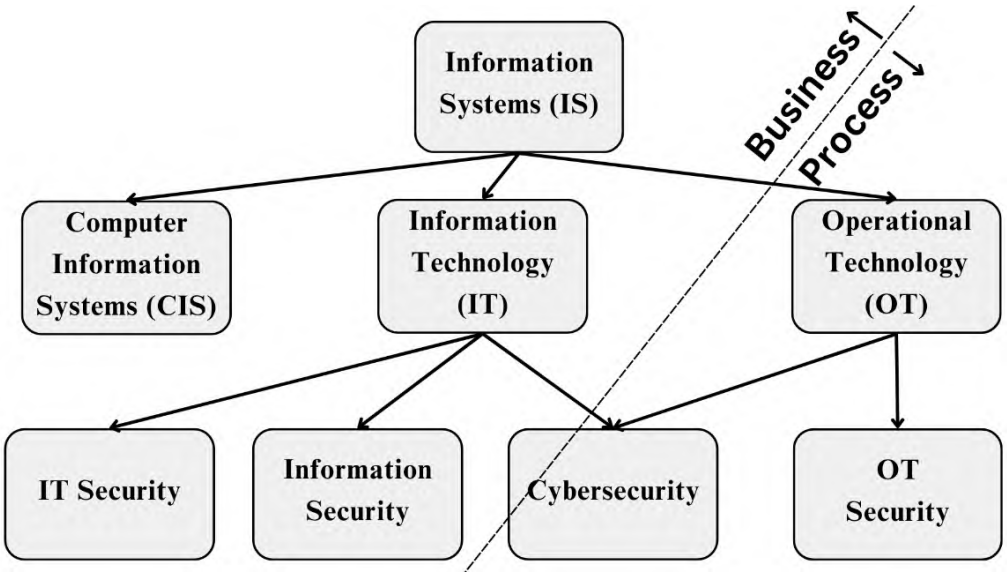


Figure 4.1 – Relationships between information systems, CIS, IT, and OT

Within this framework, CIS emphasizes the integration of people, processes, and technology to support organizational decision-making, while IT manages digital systems that facilitate communication and data flow across the enterprise. OT, in contrast, governs the technologies that monitor, control, and automate physical processes within industrial environments.

Note

Figure 4.1 is provided primarily for reference and ease of understanding; the boundaries between these domains are often blurred in modern organizations—especially with the convergence of IT and OT under Industry 4.0 and integrated cybersecurity practices. The line between IT and OT varies by organization and even by department. For readers interested in exploring how IT and OT evolved into the inseparable siblings of modern CI, visit `https://durgeshkalya.com/it-and-ot-siblings-of-modern-critical-infrastructure/`.

As we move forward, it is essential to understand how these two domains, IT and OT, function individually before exploring how they converge and share responsibility for securing today's interconnected industrial environments. The following sections define each domain, highlight their unique purposes, and examine how information security and OT security intersect to protect both data and operations within critical infrastructure systems.

IT

IT encompasses the hardware, software, and networks used to manage and process data. Examples of IT include computers, servers, software applications, and networking infrastructure. IT systems facilitate tasks such as data storage, retrieval, processing, and communication, enabling organizations to streamline operations and enhance productivity.

Figure 4.2 presents a breakdown of common IT components:

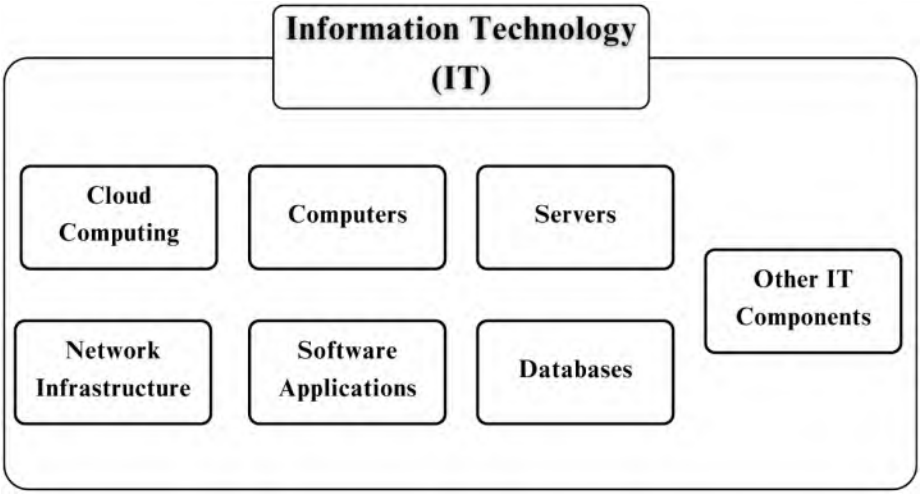


Figure 4.2 – General breakdown of Information Technology (IT)

Information security

In the context of CI, **information security** or IT security is the state in which systems and components of information systems are protected against unauthorized use of information, especially electronic data, or the measures taken to achieve this. CI sectors such as energy, transportation, healthcare, and finance are particularly vulnerable to cyber threats due to their reliance on interconnected IT systems.

Remember

Data refers to raw facts and figures, whereas information is processed data that provides context and meaning. Information is derived from analyzing and interpreting data, enabling informed decision-making and problem-solving.

Figure 4.3 shows some of the main domains of IT security:

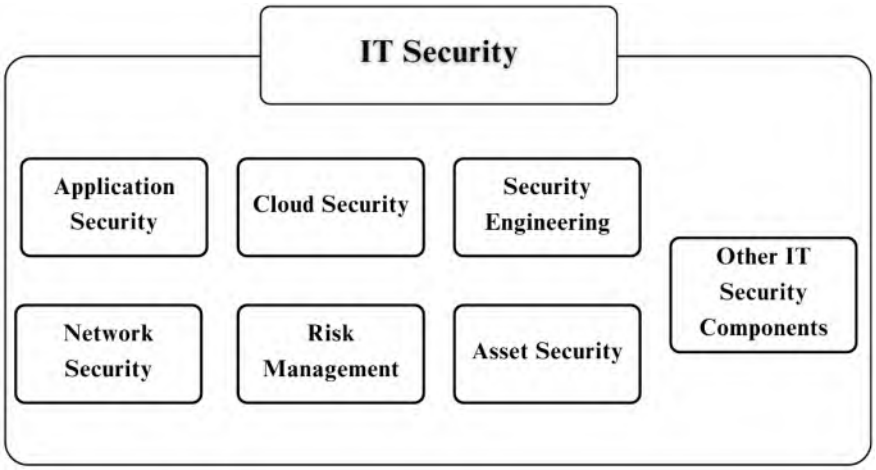


Figure 4.3 – General breakdown of IT security

Information security measures include implementing access controls, encryption, intrusion detection systems, and regular security audits to mitigate risks and protect critical assets from cyberattacks.

OT

OT refers to the hardware and software systems used to monitor, control, and automate physical processes within industrial environments. Unlike IT, which focuses on managing digital data and communications, OT is primarily concerned with managing and optimizing industrial operations in sectors such as manufacturing, energy, transportation, and utilities. *Figure 4.4* shows the various components and general breakdown of OT systems:

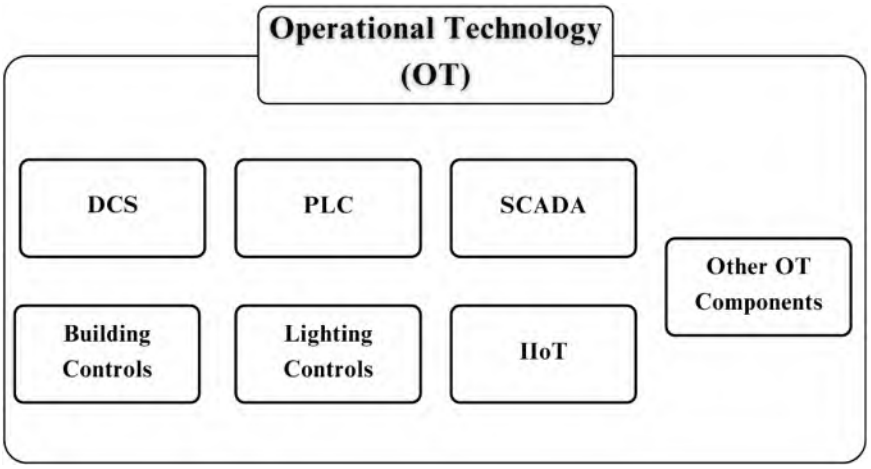


Figure 4.4 – General breakdown of Operational Technology (OT)

Chapter 3 discussed the core principles of IACS within CI, highlighting the pivotal role of OT. OT forms the foundation of IACS, though its definition often varies across organizations, making it essential to clearly establish what OT encompasses within each operational environment.

When it comes to securing OT systems, commonly referred to as OT security, one of the most critical steps is to delineate and define system boundaries. This isn't just a conceptual task; it's a practical step toward achieving effective protection. Every organization's OT landscape is unique, shaped by its processes, assets, and degree of integration with IT systems.

To begin defining these boundaries, identify what truly belongs to the OT domain—the equipment, networks, and systems that directly monitor or control physical processes. This typically includes **programmable logic controllers (PLCs)**, SCADA systems, **Human-Machine Interfaces (HMIs)**, **Safety Instrumented Systems (SIS)**, and industrial communication networks such as control and field buses.

Once these assets are identified, map their interactions with other systems, especially where OT connects to enterprise networks, cloud services, or remote access gateways. These interaction points often represent the *edges* of OT, where most vulnerabilities and security risks emerge. Using network segmentation diagrams or data flow maps helps visualize these boundaries, guiding the placement of safeguards such as firewalls, **demilitarized zones (DMZs)**, and continuous monitoring systems.

Equally important is defining what lies outside the OT boundary – for example, business systems, office workstations, or analytics servers that consume data but don't control processes. This clarity allows teams to focus security resources where they have the greatest impact.

In essence, delineating OT boundaries is about achieving visibility, control, and intent, understanding what you are protecting, where it resides, and how it communicates. Without that clarity, OT security programs risk being incomplete or misaligned with the realities of industrial operations.

OT security involves defending control systems from cyber threats, implementing network segmentation, access controls, real-time monitoring, and incident response plans. Effective OT security is essential for maintaining operational continuity and protecting CI from evolving cyber threats.

Remember

While OT refers to the hardware and software systems used to control and monitor physical processes and machinery in environments such as manufacturing, utilities, and CI, OT security focuses on protecting these systems from cyber threats and vulnerabilities. OT encompasses the actual devices and systems that interact with physical processes, such as SCADA systems and PLCs, whereas OT security involves implementing strategies and measures to safeguard these devices and systems from malicious attacks, unauthorized access, and other security risks.

Figure 4.5 shows some of the most important domains that could be considered part of OT security, such as **IACS Security**, **Asset Security**, **Security Engineering**, **IACS Vulnerability Management**, and other components like Identity and Access Management (refer to *Table 4.1* for explanations of these core OT security principles):

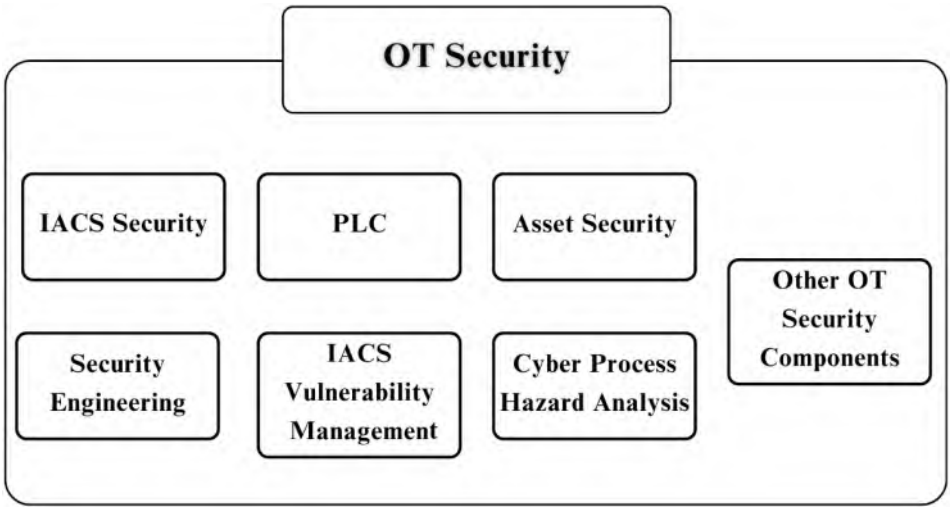


Figure 4.5 – General breakdown of Operational Technology Security (OT Security)

OT security, IT security — It is all security nonetheless

Despite their different focuses—physical process control versus business/enterprise information management—both OT and IT security are integral components of a comprehensive security

strategy. They work together to protect an organization's critical assets and ensure operational resilience in the face of evolving cyber threats. *Table 4.1* shows the various domains of IT/OT security:

Security Domain	Description	Example
Security Principles	Core principles that guide the implementation of security measures.	**Confidentiality, Integrity, Availability (CIA)**, access control, least privilege, need-to-know, defense in depth
Risk Management	The process of identifying, assessing, and mitigating risks to reduce the impact of security threats.	Threat assessment, vulnerability management, risk assessment, risk mitigation, **Business Impact Analysis (BIA)**
Security Governance and Compliance	Establishing policies, standards, and procedures to ensure adherence to legal and regulatory requirements.	Security policies, standards, procedures, laws, and regulations (e.g., GDPR, CCPA, HIPAA)
Network Security	Measures and technologies used to protect network infrastructure and data.	Firewalls, **Intrusion Detection/Prevention Systems (IDS/IPS)**, **Virtual Private Networks (VPNs)**, network segmentation
Endpoint Security	Protection of individual devices from threats and vulnerabilities.	Antivirus, anti-malware, **Host-based Intrusion Prevention Systems (HIPS)**, **Endpoint Detection and Response (EDR)**
Identity and Access Management (IAM)	Systems and practices for managing user identities and controlling access to resources.	Authentication, authorization, account management, **Single Sign-On (SSO)**, Identity Federation
Security Architecture and Engineering	Designing and implementing secure systems and infrastructure.	Security design, cryptography, secure coding practices, system hardening

Security Operations	Ongoing practices for monitoring, managing, and responding to security incidents.	Incident response, threat hunting, security monitoring, log management, digital forensics
Cloud Security	Protection of cloud-based resources and services.	**Infrastructure as a Service (IaaS)**, **Platform as a Service (PaaS)**, **Software as a Service (SaaS)**, Security controls in cloud environments
Application Security	Ensuring the security of software applications throughout their lifecycle.	**Secure Software Development Lifecycle (SDLC)**, vulnerability scanning, penetration testing, **Web Application Firewalls (WAF)**
Data Security	Measures and technologies to protect data from unauthorized access and breaches.	**Data Classification, Encryption, Data Loss Prevention (DLP)**, data masking, database security
Mobile Security	Protection of mobile devices and applications from security threats.	**Mobile Device Management (MDM)**, **Mobile Application Management (MAM)**, secure mobile applications
IoT Security	Security measures specific to Internet of Things (IoT) devices and networks.	Secure IoT device management, IoT data protection, IoT network security
Artificial Intelligence (AI) and Machine Learning (ML) Security	Protecting AI/ML systems from attacks and ensuring their integrity.	AI/ML model security, bias and fairness, adversarial attacks
Cybersecurity Governance and Risk Management	Frameworks and practices for managing enterprise-wide cybersecurity risks and ensuring compliance.	**Enterprise Risk Management (ERM)**, Cybersecurity Frameworks (NIST, ISO 27001), Compliance Management

Table 4.1 – Core security principles of IT and OT security

We have now established the critical differences between IT and OT environments, as well as the distinct worlds of IT security and OT security. The next section will delve into the security considerations specific to OT systems. Understanding these concepts is crucial because OT systems operate in unique contexts that demand specialized knowledge due to their reliance on real-time data and control processes. Security measures and response strategies should be tailored to the complexities of OT systems.

Understanding security considerations for OT systems

In this section, we will dig deeper into several security considerations and concepts specific to OT systems. We will explore how safety standards have shaped security practices within OT environments, emphasizing the crucial intersection between safety and security in industrial settings.

To effectively secure IACS within CI, organizations must undertake the initial step of identifying all OT systems and subsequently classifying them according to their security and criticality levels. This classification involves referencing standards such as **ISA/IEC 62443**, which provides guidelines for establishing cybersecurity management systems for IACS. The standard defines **Security Levels** (**SLs**) to help organizations manage cyber risks in OT systems. These levels establish a target level (or desired levels) of security for IACS. As ISA/IEC 62443 doesn't explicitly define specific criticality levels, they are not exactly criticality levels, but they are informed by the criticality of the assets being protected.

Security Levels

SLs range from **0** (minimal security) to **4** (highest security). Systems with very low risk might be assigned **SL 0**. **SL 2** defends against basic intentional attacks, which require minimal effort and expertise. **SL 3** is designed to withstand intentional attacks with some planning and expertise, and lastly, **SL 4** provides the highest level of security against highly skilled and well-funded attackers. *Table 4.2* shows security levels as defined in the ISA/IEC 62443 standard:

Security Level (SL)	**Security**	**Level of attack**	**Description**
SL 0	Minimal security	No attacks/attacks with no effects	This foundational level entails basic security measures and may be applicable to systems with negligible risk.
SL 1	Defense against incidental breaches	Accidental or opportunistic attacks	Designed to counteract inadvertent or opportunistic attacks, this level provides protection against casual violations.

SL 2	Defense against simple attacks	Intentional attacks with limited resources and skills	At this level, systems are fortified against targeted attacks employing rudimentary methods.
SL 3	Defense against moderate threats	Determined attackers with some resources and knowledge	Systems classified under this level are equipped to withstand deliberate attacks orchestrated by adversaries with moderate resources and expertise.
SL 4	Defense against advanced threats	Highly skilled and well-funded attackers	This highest tier entails comprehensive measures to withstand sophisticated attacks orchestrated by highly skilled and well-resourced adversaries.

Table 4.2 – Security levels as defined in the ISA/IEC 62443 standard

The security levels in ISA/IEC 62443 represent confidence in the absence of vulnerabilities and the intended functionality of an IACS system.

There are three types of SLs used within the ISA/IEC 62443 series; **Target Security Levels (SL-T)**, **Capability Security Levels (SL-C)**, and **Achieved Security Levels (SL-A)**. SL-T defines the desired level of security, SL-C represents the native technical security countermeasures, and SL-A reflects the actual measured security levels for an automation solution.

Let us consider an example of a pharmaceutical manufacturing facility that deploys an automation solution, a **Distributed Control System (DCS)** that controls batch processing, monitors tank levels, and manages safety interlocks through **Safety Instrumented Systems (SIS)**. This solution integrates PLCs, operator HMIs, an engineering workstation, and network switches distributed across multiple zones and conduits.

As part of its cybersecurity risk management process, the organization performs a risk assessment and determines that specific SL-T should be achieved for each automation component. To meet these targets, the organization must carefully select automation components that possess the SL-C required to support the desired protection goals. Once implemented and tested, the SL-A reflect the actual performance of these security measures within the operational environment.

Target Security Levels (SL-T)

Based on a detailed threat modeling and consequence analysis, the plant concludes that different areas of its control architecture face varying degrees of risk. The process control systems are more likely to be targeted by external threat actors seeking to disrupt production, rather than cause direct physical harm.

The resulting SL-T are defined as follows:

- **Process Control Zone: SL-T = 2** – Protection against intentional violations using simple means, limited resources, and generic skills
- **Safety Instrumented System (SIS) Zone: SL-T = 3** – Protection against more sophisticated adversaries with moderate resources, motivation, and technical capabilities
- **Corporate IT Zone: SL-T = 1** – Basic protection against accidental misuse or casual threat

These target levels define the desired security posture for each zone and serve as the benchmark for design and implementation.

Capability Security Levels (SL-C)

The DCS vendor provides detailed documentation outlining the technical security capabilities of each system component. These define the SL-C—the maximum level of security that the component can support when correctly configured and maintained.

Here are some examples:

- The DCS controller firmware supports user authentication, role-based access control, secure communication (TLS), and logging, allowing it to meet SL-C = 3
- The HMI software supports only SL-C = 2, limited by weaker session handling and the absence of multifactor authentication
- The SIS controller, supplied by a different vendor, supports SL-C = 4 for safety-critical operations with robust integrity and access control features

These capabilities define the inherent technical potential of each system element and guide the selection and configuration process to meet the target objectives.

Achieved Security Levels (SL-A)

Following integration, configuration, and deployment, the plant conducts a security validation assessment to measure the SL-A, which is the actual security performance realized in the operating environment.

Due to legacy components, incomplete network segmentation, and procedural gaps, the assessment reveals the following:

- The overall automation system achieves SL-A = 2 across most zones, aligning with baseline targets but leaving a limited margin for advanced threats
- The SIS network successfully achieves SL-A = 3, meeting its design objectives

- The HMI and engineering workstation achieve only SL-A = 1–2, constrained by outdated operating systems and shared credential practices

The SL-A values reflect the real-world implementation maturity and help identify areas for continuous improvement, such as patch management, segmentation, and credential hardening.

Figure 4.6 illustrates how security levels are applied for our example, the pharmaceutical organization, within an automation solution based on the ISA/IEC 62443 framework:

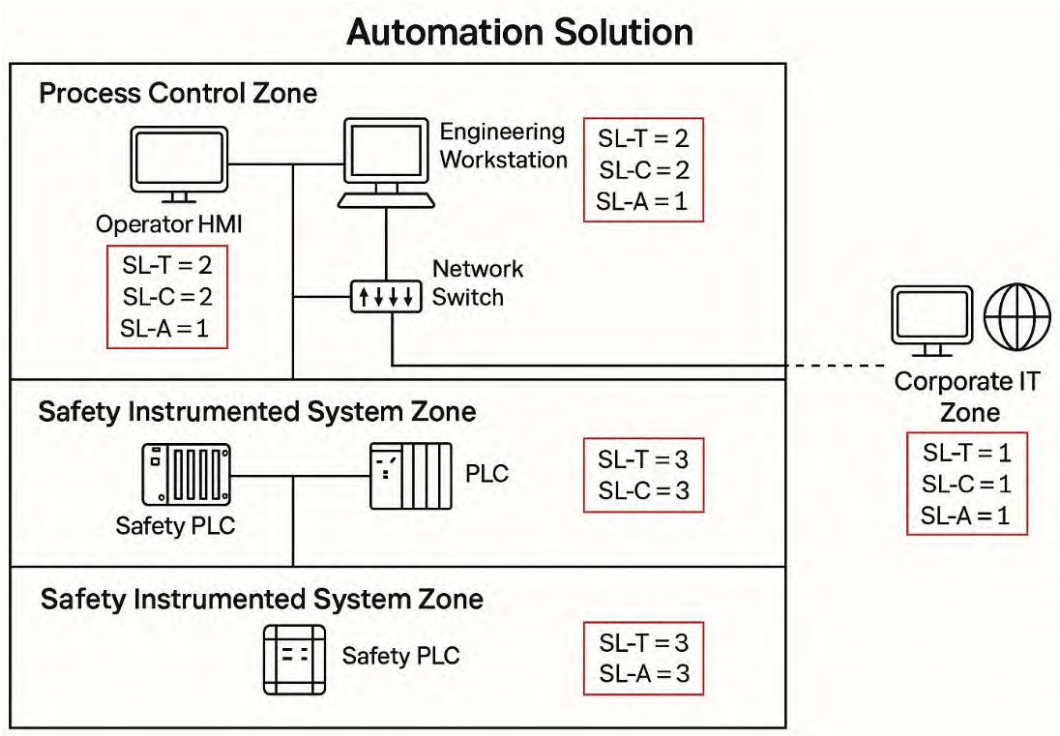


Figure 4.6 – Example of SLs (SL-T, SL-C, and SL-A) applied to an automation solution in a pharmaceutical manufacturing facility

The architecture is divided into multiple zones: **Corporate IT Zone**, **Process Control Zone**, and **Safety Instrumented System Zone**, each assigned a target (**SL-T**), capability (**SL-C**), and achieved (**SL-A**) SL. These values represent, respectively, the desired level of protection, the inherent capability of system components, and the actual level achieved after implementation and validation.

Evaluating target, capability, and achieved SLs provides organizations with a structured method to measure and improve cybersecurity maturity. When discrepancies exist between SL-T and SL-A, they highlight gaps that drive remediation actions, such as upgrading component capabilities,

enhancing network segmentation, or tightening access controls. Over time, these assessments form a continuous improvement cycle, ensuring that the automation system evolves alongside emerging threats, maintains regulatory alignment, and strengthens resilience in accordance with the ISA/IEC 62443 principles.

Note

Organizations may also use a risk matrix to assess threats. Also known as a heat map, it is a simple but powerful tool for understanding how likely a threat is to occur and how severe its impact could be. It helps organizations decide which risks require action, which can be monitored, and which can be accepted as part of normal operations. *Figure 4.7* presents an example risk matrix.

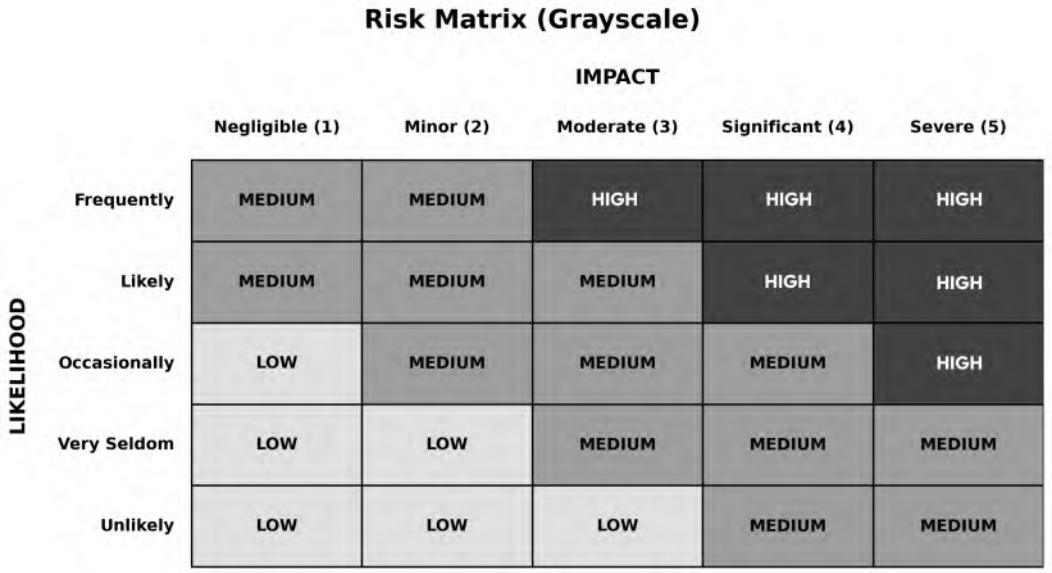


Figure 4.7 – Example risk matrix

Functional Safety

While SLs address how cyber threats are prevented or contained, another equally important discipline ensures that process safety is maintained even when failures occur; this is known as **Functional Safety (FS)**.

FS focuses on ensuring that systems operate correctly in response to their inputs and that, when a failure does occur, it is managed safely to avoid unacceptable risks to people, the environment, or assets. This is done through **Safety Instrumented Systems (SIS)**, **Safety Integrity Levels (SIL)**, and **Safety Instrumented Functions (SIF)**, which measures failure response and risk reduction.. Together, these disciplines provide complement industrial resilience, where cybersecurity safeguards prevent intentional disruption, and safety systems ensure that even in the event of a fault or compromise, the process remains stable and controlled. Although this topic extends beyond the direct scope of cybersecurity, it is an essential concept for professionals working in OT and industrial environments.

In industrial sectors such as energy, chemicals, pharmaceuticals, and oil and gas, FS serves as a foundational pillar of operational reliability. Understanding its core elements – SIS, SIL, and SIF – provides valuable context for appreciating how safety and security coexist within modern automation systems. These are discussed as follows.

Safety Instrumented System (SIS)

An SIS is a specialized control system designed to detect hazardous conditions and automatically bring the process to a safe state.

An SIS typically includes sensors, logic solvers (such as safety PLCs), and final control elements (such as shutdown valves or actuators). Together, these components execute predefined SIFs that reduce the risk of catastrophic incidents. In the earlier SLs example, the SIS zone demonstrated how such systems are segregated to ensure independence from the main process control network.

Safety Instrumented Function (SIF)

An SIF is an individual protective function within an SIS. Each SIF performs a specific safety task, such as shutting down a reactor when the temperature exceeds safe limits or venting pressure in the event of an overpressure scenario.

Depending on its purpose, an SIF may operate continuously (providing constant protection) or on demand (activating only during a specific hazardous event). Each function is evaluated for its reliability, speed of response, and failure tolerance—parameters that directly influence its SIL classification.

Safety Integrity Level (SIL)

A SIL provides a quantitative measure of how reliably an SIF performs its intended function.

The SIL scale ranges from SIL 1 (providing the least risk reduction) to SIL 4 (providing the highest). Each level corresponds to a specific **Probability of Failure on Demand** (**PFD**), defining how often the safety function might fail to act when required.

Establishing the appropriate SIL typically involves structured analyses such as **Hazard and Operability Study** (**HAZOP**) or **Layer of Protection Analysis** (**LOPA**), which identify hazards, evaluate the effectiveness of safeguards, and quantify the level of risk reduction required.

By aligning with international standards such as IEC 61508 (for electrical and electronic safety systems) and IEC 61511 (specific to process industries), organizations can design and maintain safety systems that are consistent, auditable, and aligned with global best practices.

While FS primarily focuses on preventing or mitigating process hazards, its principles are deeply intertwined with both cybersecurity and incident management. For instance, a compromised control system can disable or falsify inputs to an SIS, just as a failed SIS can worsen the consequences of a cyber incident. These interdependencies highlight why safety and security cannot be treated in isolation. Understanding SIS, SIL, and SIF helps organizations design protection layers that are not only preventive but also detective and responsive when failures occur.

Additionally, from an incident management perspective, FS plays a critical role in maintaining operational stability during and after an event. Integrating FS into the broader incident response framework ensures that technical, operational, and emergency response teams share a unified understanding of how safety functions behave under stress.

Consider the previous example of the pharmaceutical manufacturing facility. During normal operations, the SIS continuously monitors critical process variables such as temperature, pressure, and flow rate. Each of these is associated with an SIF that defines a protective response. If reactor pressure rises above a defined safe limit, a pressure relief SIF automatically isolates the reactor feed and opens a vent valve to prevent an explosion.

Now imagine a cyber incident in which a malicious actor compromises the DCS through a phishing attack, altering setpoints and disabling alarms to mask process deviations. While the control system's integrity is affected, the independent SIS detects the abnormal condition through direct sensor inputs and executes the shutdown sequence based on its predefined logic.

In this scenario, FS and cybersecurity converge. The SIS prevents a potentially catastrophic event even as the control network experiences a cyber compromise. From an incident management perspective, this becomes a key containment success:

- The SIS response acts as an automated first line of defense
- The incident management team classifies and escalates the event as a safety-integrity incident with cyber implications
- The post-incident review identifies opportunities for improved segmentation, alarm management, and coordination between OT and emergency response teams

Therefore, FS mechanisms (SIS, SIF, SIL) serve as integral layers within an organization's broader incident management strategy, helping to limit cascading operational, environmental, and reputational impacts during cyber-physical events.

However, not all events carry the same level of consequence. Understanding the magnitude of impact, whether it involves safety, production loss, environmental damage, or reputational harm, is essential to prioritize response actions and allocate resources effectively.

This is where the concepts of impact levels and system criticality become important. While FS and SLs define how well systems are protected and how reliably they respond, impact and criticality determine what is at stake when those protections fail or are exceeded. They are discussed next.

Impact levels

Impact levels refer to the potential consequences of a security breach on an IACS component or system. Rather than being a predefined set of levels, it involves an evaluation of the severity of potential impacts. Incidents with higher impact levels, such as those affecting critical systems or causing widespread disruptions, necessitate immediate attention and resources for the swift restoration of operations.

These impacts are typically assessed across three primary categories:

- **Safety**: Pertains to the potential harm posed to people, the environment, or property due to a system breach
- **Availability**: Involves the potential disruption to operations, production loss, or financial impact caused by a breach affecting system availability
- **Environmental impact**: Encompasses the pollution, damage, or safety hazards resulting from a system failure

On the IT side, impact assessments are conducted across the following dimensions:

- **Confidentiality**: Ensuring that only authorized users can access and view sensitive information, safeguarding against unauthorized disclosure
- **Integrity**: Ensuring the accuracy and reliability of data and system functions, preventing unauthorized alteration or manipulation
- **Availability**: Ensuring authorized users can access information and systems as needed, guarding against disruptions that could impede operations

Other security considerations when impact is assessed are as follows:

- **Non-repudiation**: Ensures that the sender of a message cannot deny sending it, and the recipient cannot deny receiving it
- **Resiliency**: Ensures that systems and networks can withstand and recover from cyberattacks
- **Privacy**: Ensures that individuals have control over their personal information and that it is only used for the purposes for which it was collected

Criticality of OT systems

The criticality of OT systems lies in their role in managing and controlling industrial processes, where any disruption can have far-reaching consequences for safety, productivity, and national security:

- **High-criticality systems**: These systems are essential to safety, health, or environmental protection. A failure or compromise could result in loss of life, serious injury, significant environmental damage, or major operational disruption.
- Typical examples include SIS in chemical plants, **Emergency Shutdown Systems (ESD)** in refineries, and **turbine control systems** in power generation facilities. Such systems generally require higher SLs (SL 3 or SL 4) and rigorous monitoring, given that their malfunction or compromise could lead to severe incidents or national-level consequences.
- **Moderate-criticality systems**: These systems are important for maintaining operational efficiency and product quality but are not directly linked to immediate safety or environmental hazards. Disruption in these systems could cause production downtime, financial losses, or non-compliance with quality or environmental standards.

  Examples include **Programmable Logic Controllers (PLCs)** used for process control in batch operations, **SCADA systems** used for pipeline or utility monitoring, and **automated blending systems** in pharmaceuticals. These systems often require a balanced level of protection (typically SL 2 or SL 3) based on specific risk assessments and process importance.

- **Low-criticality systems**: These systems have limited influence on operational continuity or safety. Their compromise may cause inconvenience, minor data loss, or non-critical operational delays, but would not threaten safety or the environment.

  Examples include **Human-Machine Interfaces (HMIs)** used for local equipment monitoring, **historian databases** collecting non-real-time data, and **auxiliary equipment monitoring panels**. SLs for these systems are typically SL 1 or SL 2, ensuring basic authentication, integrity, and access controls without the need for advanced protection mechanisms. While ISA/IEC 62443 doesn't explicitly define specific criticality levels, there are common frameworks used to assess the criticality of IACS components.

Each system's criticality and security requirements must be meticulously evaluated to determine the appropriate level of security measures to be implemented.

Table 4.3 compiles some systems classified as OT, and their security, impact, and criticality levels, serving as a reference for organizations when delineating their OT systems:

System(s)	Security Level (SL)	Impact Level	IT Criticality	IACS Criticality	Description
Distributed Control System (DCS)	SL 3 or SL 4 (depending on criticality)	High	Confidentiality (Critical), Integrity (Critical), Availability (Critical)	Safety (Critical), Environmental (High), Availability (Critical)	Manages complex industrial processes. Security breaches could cause safety hazards, environmental damage, and significant production losses.
Programmable Logic Controller (PLC)	SL 2 or SL 3 (depending on criticality)	Moderate-High	Confidentiality (Moderate), Integrity (High), Availability (High)	Safety (High), Environmental (Moderate), Availability (High)	Controls specific industrial machines or processes. A breach could disrupt production, impact product quality, or cause safety incidents.

Supervisory Control and Data Acquisition (SCADA)	SL 2 or SL 3 (depending on criticality)	Moderate	Confidentiality (Moderate), Integrity (High), Availability (High)	Safety (Moderate), Environmental (Moderate), Availability (High)	Monitors and controls industrial processes remotely. An attack could disrupt operations, cause data breaches, or lead to equipment damage.
Human-Machine Interface (HMI)	SL 1 or SL 2 (depending on criticality)	Low-Moderate	Confidentiality (Low-Moderate), Integrity (Moderate), Availability (Moderate)	Safety (Low-Moderate), Environmental (Low), Availability (Moderate)	Provides an operator interface for monitoring and controlling IACS. Compromise could lead to the manipulation of data or unauthorized access, potentially impacting operations.
Safety Instrumented System (SIS)	SL 3 or SL 4 (typically)	High	Confidentiality (N/A), Integrity (Critical), Availability (Critical)	Safety (Critical), Environmental (Critical), Availability (Critical)	Provides critical safety functions to prevent accidents or mitigate hazards. Failure could result in severe injuries, environmental damage, or equipment destruction.

Table 4.3 – Compilation of Security Levels (SL), with impact and criticalities based on IT and OT impact categories

Note

Although not directly mentioned in the ISA/IEC 62443 standard, SIS usually needs the highest level of security because they play a crucial role in ensuring safety. Security measures for SIS should be planned to meet the IEC 61508 functional safety standards, along with cybersecurity considerations.

Table 4.3 gives a general idea, a starting point based on common impact levels. The exact impact level of an IACS component should be evaluated based on things such as potential safety risks, how much it could disrupt operations, and its environmental impact.

Historical cyber incidents in OT environments

OT systems have historically been isolated from corporate and external networks, operating in what was once considered a *safe* or air-gapped environment. This isolation provided inherent protection against cyber threats. However, the growing integration of OT and IT networks, along with the rise of **Industrial Internet of Things** (**IIoT**) devices and cloud-based monitoring, has significantly expanded the attack surface.

Modern OT environments now rely on interconnected systems for analytics, remote access, and maintenance connections that introduce pathways for adversaries. This evolution means that cyber incidents once confined to IT networks can now cascade directly into industrial operations, affecting safety, reliability, and national resilience.

OT-specific threats

Threats to OT environments differ fundamentally from those in traditional IT systems. While IT attacks often target data theft or extortion, OT attacks focus on the disruption, manipulation, or destruction of physical processes. The consequences extend beyond information loss to tangible impacts such as equipment failure, safety incidents, or environmental harm.

Common threat vectors include the following:

- Ransomware propagation through shared IT-OT networks, causing process interruptions
- Supply-chain compromises that introduce malicious code into trusted industrial software or firmware
- Spear-phishing and credential theft, leading to unauthorized access to engineering workstations or HMI interfaces
- Malware injection targeting PLCs, safety controllers, or SCADA servers to alter process behavior
- State-sponsored espionage or sabotage, where adversaries seek strategic control over energy grids, pipelines, or chemical facilities

These attack vectors emphasize that security incidents in OT can rapidly evolve into safety events, requiring an integrated approach across both domains.

Table 4.4 presents some notable attacks:

Year	Attack	Description
2008	Conficker Worm	Exploited vulnerabilities in Microsoft Windows operating systems, spreading rapidly across networks and infecting millions of computers worldwide.
2009	Titan Rain	A large-scale cyberespionage campaign targeting multiple CI sectors, including energy and transportation. This attack highlighted the growing interest of nation-states in gaining access to industrial control systems for potential disruption or information theft.
2010	Stuxnet	Targeted SCADA systems—particularly those used in Iran's nuclear facilities—to sabotage centrifuges by altering their operating parameters.
2012	Shamoon Malware	Targeted energy sector organizations in the Middle East, infecting computers and overwriting data, leading to substantial financial losses and operational downtime.
2015	Ukraine Power Grid	Cyberattack orchestrated by hackers targeting Ukraine's power grid, resulting in widespread power outages by remotely manipulating CI components.
2017	WannaCry Ransomware	Exploited vulnerabilities in Microsoft Windows operating systems, infecting hundreds of thousands of computers worldwide and demanding ransom payments for data decryption.
2011	Lockheed Martin Supply Chain	This attack targeted a supplier to Lockheed Martin, a major defense contractor, emphasizing the importance of securing the entire supply chain for OT systems. Vulnerabilities in any part of the chain can be exploited to gain access to core systems.
2020	SolarWinds Supply Chain	Widespread attack targeting SolarWinds, a software company whose Orion platform was widely used, including in CI sectors. Hackers infiltrated the platform and delivered malicious updates, granting access to victim networks. This incident underscored the dangers of supply chain attacks and the need to secure all aspects of the software development and deployment process.
2021	Colonial Pipeline Ransomware	This ransomware attack forced the shutdown of the largest U.S. fuel pipeline for several days, leading to fuel shortages and emphasizing how IT system breaches can cascade into OT operations.

2021	Oldsmar Water Facility (Investigation Concluded)	Attackers remotely accessed a water treatment system and attempted to alter chemical dosing levels, initially raising concerns about unsecured remote access in critical infrastructure. However, subsequent investigations into the Oldsmar Water Treatment Plant incident suggested that the event was more likely the result of human error rather than a confirmed cybersecurity breach.
2023	Danish Energy Sector Intrusions	Coordinated cyberattacks targeted 22 energy companies in Denmark, exploiting third-party vendor systems and revealing the continued vulnerability of European critical infrastructure.
2025	Asahi Group Ransomware Attack	Disrupted production systems across multiple global plants, halting operations and exposing the fragility of interconnected industrial networks.
2025	Chinese-Linked Volt Typhoon Campaign (Ongoing)	Cyber-espionage campaign targeting U.S. critical infrastructure operators, maintaining persistent access within OT environments through compromised routers and network devices.

Table 4.4 – Historical cyberattacks directly or indirectly targeting OT systems

While some of the attacks listed in the table may not be traditionally classified as OT security breaches or attacks, the increasing interconnectedness of industrial control systems and the broader network landscape means that they can still have significant implications for OT security. For instance, the SolarWinds supply chain attack targeted a software company widely used in CI sectors, demonstrating how vulnerabilities in seemingly unrelated systems can lead to cascading effects on OT environments.

As the boundaries between IT and OT continue to blur, the need for structured, layered, and resilient network security strategies has never been greater. These strategies form the backbone of modern OT defense, protecting critical assets, ensuring safe communication, and enabling organizations to maintain control even during sophisticated cyber or process incidents. They are discussed next.

Network security and segmentation in OT environments

Network security in an OT context is about creating controlled, monitored, and well-defined communication boundaries that reduce the potential attack surface. This involves more than deploying firewalls or **intrusion detection systems (IDS)**. It's about designing the network in layers, separating functions, and enforcing controls so that if one system is compromised, the rest remain protected.

This principle is implemented through network segmentation, the process of dividing the OT network into smaller, manageable zones based on their function, sensitivity, and risk. Each zone can then be protected and monitored independently. For instance, a process control zone containing PLCs and HMIs should be isolated from the enterprise IT zone, allowing only necessary and approved communication. If a breach occurs in the IT network, segmentation prevents it from moving laterally into the control environment.

Industry standards such as ISA/IEC 62443 and the ISA-99 framework provide structured approaches for designing these secure architectures. They define how to identify assets, group them into security zones, establish conduits for communication, and assign SLs based on the potential impact of compromise. This risk-based approach ensures that security controls align with operational importance and process safety.

The Purdue model as a foundation for OT network security

The **Purdue Enterprise Reference Architecture (PERA)**, commonly known as the **Purdue model**, has been one of the most practical and enduring frameworks used across industrial environments. Initially created to map data flow and functional hierarchy, the model organizes systems into distinct levels from Level 0 (field devices) to Level 5 (enterprise IT).

While the Purdue model was never originally intended as a security framework, its structure naturally supports the concept of defense-in-depth and network segmentation. Each level can be treated as an independent security zone, with controlled conduits and access rules between them:

- **Levels 0–1 (Sensors, Actuators, PLCs)**: These should be protected from direct IT access and isolated with industrial firewalls or VLANs
- **Level 2 (Control and Monitoring)**: Typically houses HMIs and control servers; requires strict control over data exchanges and authentication
- **Level 3 (Operations / Site Network)**: Should interface with IT only through a DMZ, using firewalls and one-way data transfers where possible
- **Levels 4–5 (Enterprise IT and Cloud)**: Must be segregated from OT zones with tightly controlled communication and monitored connections

By treating each level as a separate domain with defined responsibilities and protections, the Purdue model remains a complementary architecture for network security, not just a process hierarchy. It ensures that failures or compromises at higher levels do not cascade into the control layer.

The introduction of **Industrial Internet of Things (IIoT)**, cloud connectivity, and edge analytics has blurred the lines that the traditional Purdue model once clearly defined. Many new devices, sensors, gateways, and even safety controllers now communicate directly across multiple layers, sometimes even bypassing traditional firewalls to send data to cloud-based systems.

This shift has introduced both new capabilities and new risks. The rigid hierarchy of the original Purdue model can no longer accommodate every communication pattern seen in modern industrial environments. Instead, organizations are adopting adaptive segmentation approaches, extending the Purdue model's logic with more granular, dynamic control mechanisms.

One such approach is **micro-segmentation**. Rather than segmenting entire network layers, micro-segmentation focuses on isolating individual devices, applications, or data flows. It applies policy-based controls to determine which specific entities can communicate, under what conditions, and through which protocols. This method limits an attacker's ability to move laterally within even a single zone and provides deeper visibility into network activity.

When used alongside the Purdue model, micro-segmentation can transform traditional architectures into hybrid network designs, combining the predictability of hierarchical structure with the flexibility of modern security controls. The importance of these layered and micro-segmented defenses becomes clear when looking at real-world incidents. The Ukrainian power grid cyberattacks showed how adversaries took advantage of weak segmentation and limited visibility within industrial control networks to disrupt essential services. Studying this case helps us see how architectural gaps, particularly between IT and OT environments, can be exploited to cause widespread operational impact. It also reinforces that concepts such as the Purdue model and micro-segmentation are not just theoretical best practices but essential safeguards for protecting critical infrastructure.

Case study of an OT security incident

We will pick one of the most sophisticated cyberattacks – the Ukraine power grid cyberattack targeting CI, which involved the manipulation of OT systems. Our focus will be on dissecting the incident's progression, detailing the timeline of events, conducting an in-depth analysis of attack methods, and extracting valuable lessons learned. The objective of this comprehensive case study is to shed light on how organizations can prepare for such attacks on their CI. Also, this case study consolidates the knowledge acquired in earlier chapters of this book, bringing together key concepts and strategies.

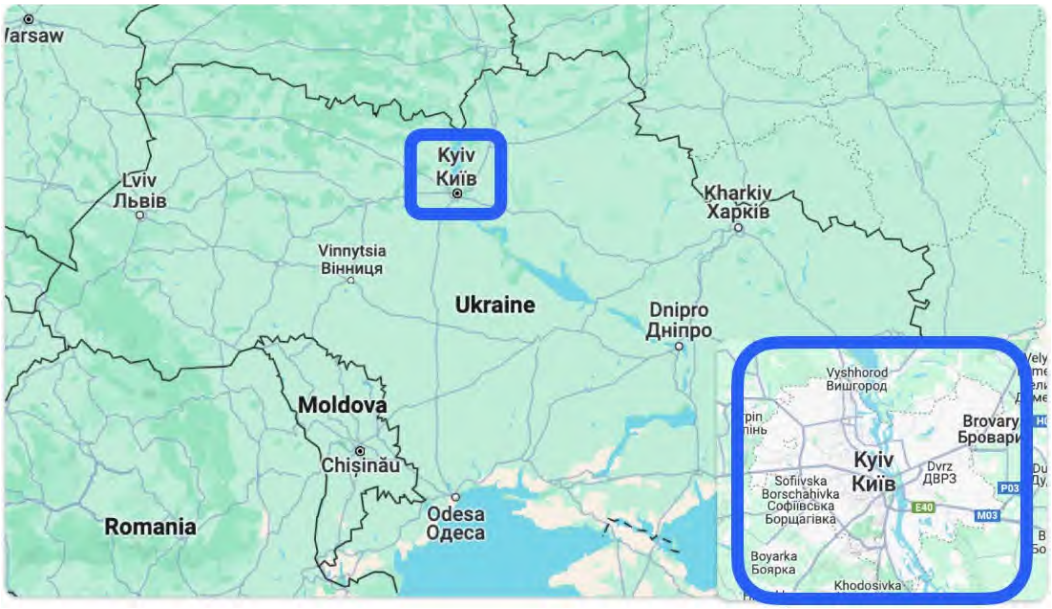


Figure 4.8 – Location of the city of Kyiv in Ukraine

We will also analyze the cyberattack targeting the Ukrainian power grid by examining the events that occurred on *December 23, 2015*. Between 15:35 and 16:30 local time, Kievoblenergo, a Ukrainian utility, experienced an intrusion into their IACS infrastructure by external parties. This breach resulted in the disconnection of seven 110 kV substations and twenty-three 35 kV substations, causing power outages affecting approximately 80,000 customers across various categories. Kyivoblenergo officially disclosed this breach through a public update posted on its website, as shown in *Figure 4.9*:

Figure 4.9 – Kyivoblenergo's public announcement regarding the breach

Additional attacks were associated with a coordinated series of cyber assaults directed at state-owned energy and utility firms, notably targeting entities such as Chernivtsioblenergo and Prikarpatyeoblenergo. *Table 4.5* illustrates further incidents. These attacks were integral components of a broader cyber campaign strategically aimed at disrupting CI within Ukraine.

Date	**Event**
May 2014	Cyberattack targeting the Central Election Commission website during Ukraine's presidential election.
October 2015	Large-scale cyberattack against multiple Ukrainian television networks.
December 23, 2015	Coordinated cyberattack on Ukraine's energy sector, impacting Kyivoblenergo, Chernivtsioblenergo, and Prykarpattyaoblenergo.
February 2016	Cyberattack disrupting operations at Boryspil International Airport.
December 6, 2016	Cyberattack on internal telecommunications networks of the Ministry of Finance, State Treasury, and Pension Fund.
December 15, 2016	**Distributed Denial of Service (DDoS)** attack on the Ukrzaliznytsia (Ukrainian Railways) website.
December 17, 2016	Cyberattack on the Severnaya substation operated by Ukrenergo.

Table 4.5 – Timeline of cyberattacks on Ukrainian infrastructure (2014-2017)

Based on publicly available documents and reports, it is apparent that the attack targeted four areas:

- Firstly, business/enterprise IT workstations fell victim to a phishing attack, compromising their security.
- Secondly, a variety of malware was deployed with diverse functionalities. These included components aimed at gathering information, establishing remote access to victims' **IACS** networks, and causing damage to SCADA systems and other critical components. The objective was to hinder the process of restoration and complicate forensic analysis. Notably, some malware specifically targeted the IACS vendors utilized by the victims.
- Finally, the attackers opened breakers, leading to the outage.
- Additionally, a DDoS attack was executed on company websites to impede customers from reporting the outage effectively.

Understanding how to resolve or prevent incidents like this one is valuable. By studying the actions of the attackers, we can learn how to better manage or prevent such situations in the future. In cybersecurity, there's a concept called the Cyber Kill Chain. This framework outlines the methods used by attackers in terms of steps or stages. Before delving into the case, it's important to familiarize yourself with the Cyber Kill Chain terminology, which will help you understand how cyberattacks progress. This is discussed next.

Cyber Kill Chain

The **Cyber Kill Chain**, developed by **Lockheed Martin**, outlines the stages of a cyberattack, offering a framework for comprehending and thwarting threats; it was initially aimed at combating **advanced persistent threats (APTs)**. Traditionally, it consists of seven stages, although some versions include an eighth.

Attackers typically progress through the following phases:

- **Reconnaissance (Gather Intelligence)**:

  The attacker gathers information about the target organization, its systems, network layout, employees, vendors, and technologies in use. In OT environments, this may involve identifying control system components, communication protocols, remote access points, and safety devices that can be exploited.

- **Weaponization (Create or Acquire Tools)**:

  Based on the gathered intelligence, the attacker creates or acquires the tools needed to exploit specific weaknesses. This could include malware, phishing kits, payloads, or legitimate software modified for malicious purposes. The tools are tailored to penetrate the target's defenses or blend into normal operations.

- **Delivery**:

  The attacker delivers the weaponized payload to the target. Common delivery methods include phishing emails, compromised USB drives, infected software updates, or exploiting vulnerabilities in exposed services or third-party systems.

- **Exploitation**:

  Once the payload reaches its target, the attacker takes advantage of a vulnerability such as a misconfiguration, outdated software, or weak credentials to execute malicious code and gain an initial foothold in the system.

- **Installation**:

  After successful exploitation, the attacker installs additional components or backdoors to maintain access and persistence. In industrial systems, this may include installing remote access tools or manipulating legitimate engineering software to disguise ongoing activity.

- **Command and Control (C2)**:

  The attacker establishes a communication channel back to their infrastructure, allowing remote control of compromised systems. This C2 channel is used to issue commands, exfiltrate data, or coordinate further actions within the environment.

- **Actions on Objectives**:

  With control established, the attacker proceeds to achieve their ultimate goal. This could involve data theft, disruption of operations, manipulation of control logic, or destruction of equipment. In OT networks, this often manifests as operational shutdowns, safety system interference, or the alteration of process parameters.

While some models add data exfiltration as an additional step, grasping the core seven stages is sufficient and pivotal for building robust cyber defenses.

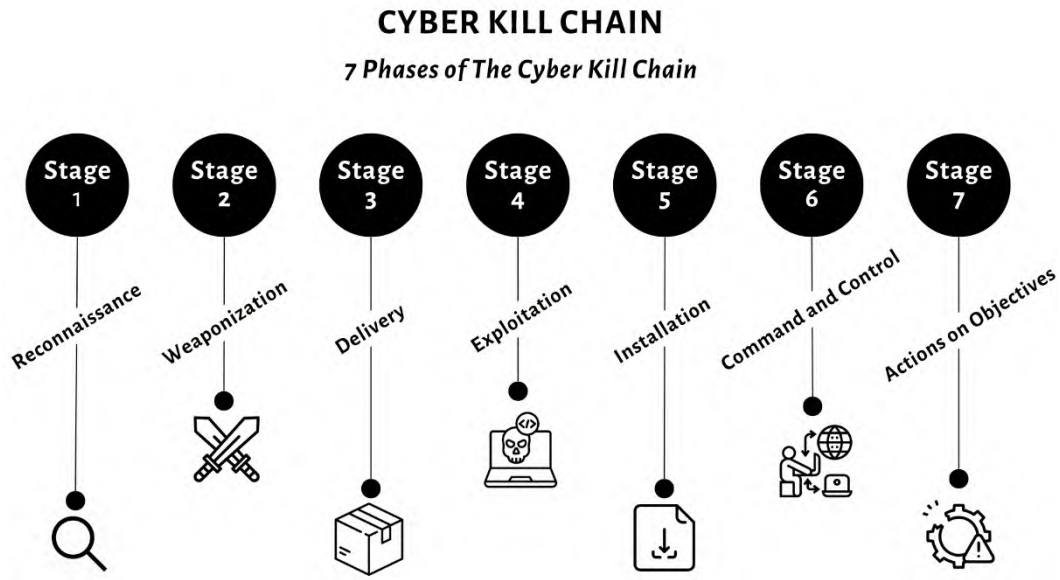


Figure 4.10 – The seven stages of the Cyber Kill Chain

The following presents Ukraine's cyber-induced power outage in the Cyber Kill Chain format. In the initial spear phishing attack, employees were enticed to open an attached Microsoft document containing a macro. Once opened, this macro installed **BlackEnergy 3** (**BE3**) on enterprise workstations:

1. **Reconnaissance (over 6 months)**: Attackers initiated a reconnaissance phase by launching spear phishing campaigns targeting administrative and IT personnel in Ukrainian utilities. These emails were designed to infiltrate networks, gather intelligence, and potentially identify vulnerabilities and harvest credentials.
2. **Weaponization**: Attackers used all of the learning from the reconnaissance to put together custom malware code or identify existing malware that could be used to conduct the cyberattack.
3. **Delivery (Spear-Phishing Emails)**:

   The delivery mechanism employed by the attackers involved sending spear-phishing emails containing hidden malware attachments. By exploiting human trust, they aimed to gain initial access and establish a foothold within the IT network. *Figure 4.10* shows a screenshot of the attachment. Upon opening the document, the user was presented with a dialog recommending the enabling of macros to view the document. Interestingly, the document mentioned *Pravii Sektor* (the Right Sector), a nationalist party in Ukraine. The party was formed in November 2013 and has since played an active role in the country's political scene.

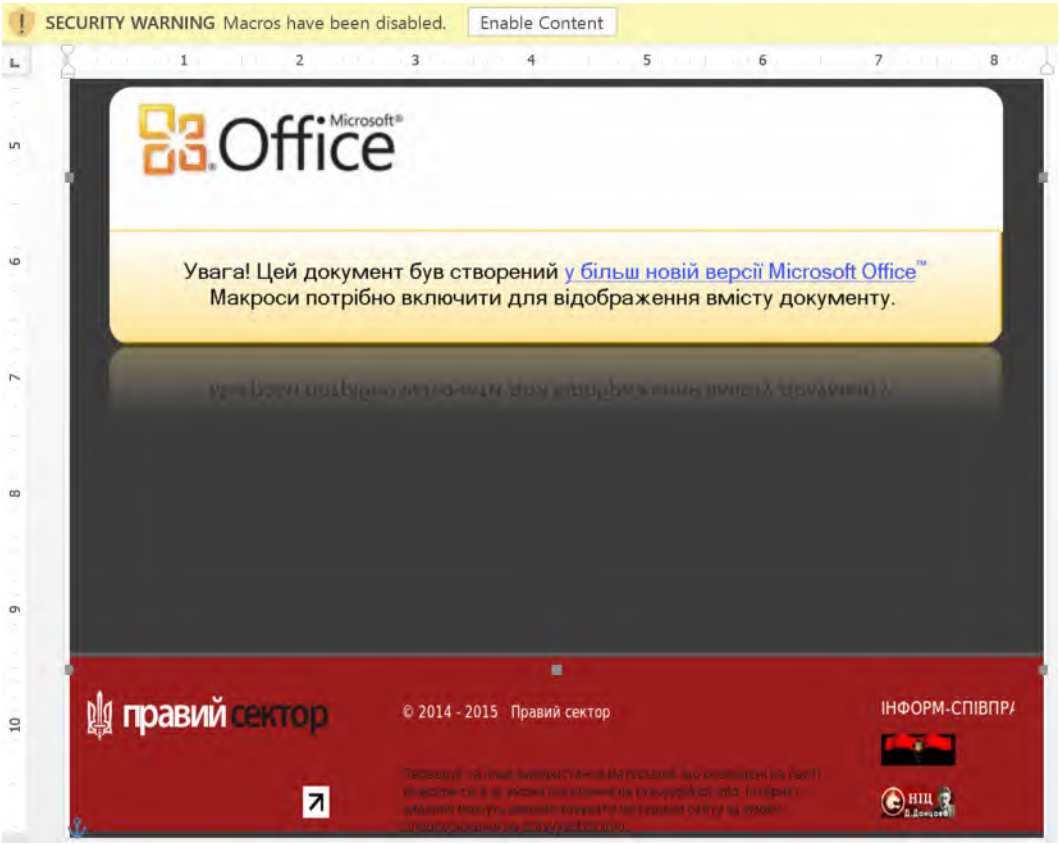


Figure 4.11 – An example of a Microsoft Office document infected with BlackEnergy 3

The attackers managed to discover and access the Microsoft **Active Directory (AD)** servers of the regional power distribution center. These servers store crucial information such as enterprise user accounts and administration credentials.

1. **Exploitation (Credential Harvesting and VPN Tunnels)**:
    - Enabling the macros allowed the malware to exploit Office macro functionality to install BlackEnergy 3 on the victim's system. The malware utilized by the attackers operated on multiple fronts. Initially, it facilitated lateral movement within the IT network, enabling the theft of credentials for further access. Exploiting these credentials and existing VPN tunnels, the attackers breached critical IACS networks.
    - Exploiting the harvested credentials, the attackers created an encrypted pathway from the external network to penetrate the organization's internal networks. This enabled them to establish a foothold within the IACS network, thereby gaining

access to CI. This infiltration's success was facilitated by inadequately configured firewalls that failed to effectively separate the IACS network from the enterprise network.

2. **Installation (Weapon Deployment)**:
    - Within the compromised IACS networks, the attackers executed a multi-pronged assault. They targeted vulnerabilities in specific IACS vendors' systems and even reconfigured a UPS network to disrupt power supply within the utilities. Additionally, they installed malicious firmware for remote communication with substations and deployed data-wiping malware to impede forensic analysis.
    - On December 23, 2015, at approximately 3:30 pm, the attackers initiated their initial assault by infiltrating the operations and SCADA networks via the established tunnels. Subsequently, they compromised the SCADA operator stations, wresting control from the operators. With control in their hands, they proceeded to open the breakers, exacerbating the situation further.
3. **Command and Control (Operator Workstations)**: Having gained control of operator workstations, the attackers effectively neutralized operators by disabling keyboards and mice, thereby securing remote control over CI.
4. **Actions on Objectives**:
    - The attackers' primary objective was to cause a power outage, but to ensure its effectiveness and longevity, they executed several additional attacks. Firstly, they targeted the **UPS** system by gaining access to its management interface, which provided backup power to servers and workstations. By shutting down the UPS system, they disrupted the backup power supply, exacerbating the impact of the power outage.
    - Additionally, the attackers launched **Denial of Service (DoS)** attacks on the call centers, aiming to overwhelm them and hinder the identification of affected individuals. This tactic created a lack of situational awareness by flooding the call centers with excessive traffic, rendering them unable to respond effectively to legitimate inquiries or process critical information about the incident. As a result, operators struggled to assess the scope of the attack and identify affected individuals, leading to confusion and delays in response efforts.

- This situation was further compounded by the operators being blinded by the power outage affecting their operations servers and workstations, which disrupted their ability to access vital systems, communication tools, and real-time data. The combination of these factors severely hampered their situational awareness, making it difficult to coordinate an effective response and implement necessary recovery measures.
- Additionally, DDoS attacks were launched against public-facing utility websites and customer portals, preventing customers from reporting outages or receiving updates about the incident. This further isolated control centers by cutting off external feedback, masking the full scope of the disruption from both operators and the public. By simultaneously disabling visibility, communications, and reporting mechanisms, the attackers ensured that the outage persisted longer and recovery efforts were severely delayed.
- Moreover, the attackers tampered with the firmware of certain serial-to-Ethernet converter devices, corrupting them and rendering them inoperable. These devices serve as communication bridges between legacy serial-connected field equipment and Ethernet-based SCADA systems. By disabling them, the attackers effectively severed communication between the control center and critical field devices, cutting off visibility and control over operational processes. This action disrupted the normal architecture of SCADA monitoring and control, as shown in *Figure 4.11:*

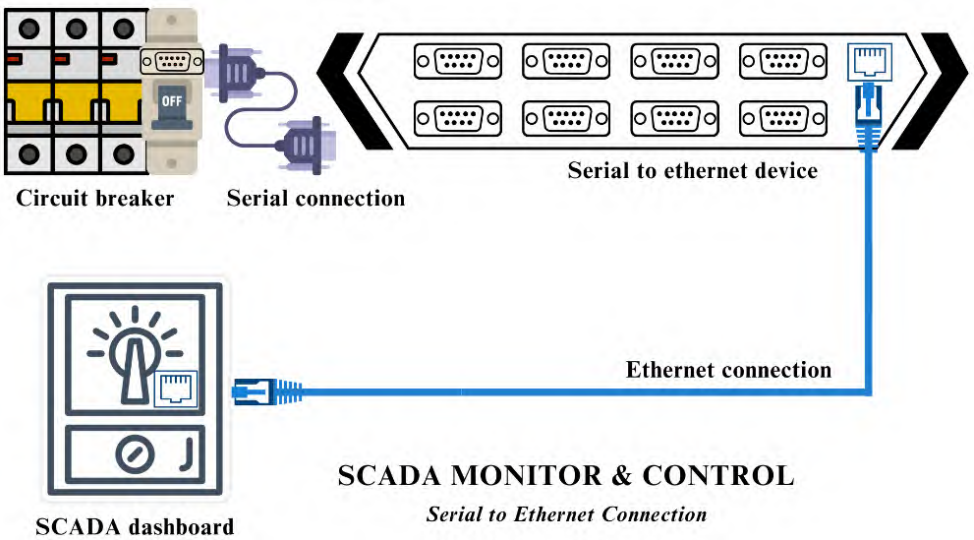


Figure 4.12 – SCADA monitoring and control using a serial-to-Ethernet device

Note

Figure 4.10 shows a typical depiction of the serial-to-Ethernet converter used in the Ukraine power grid cyberattack. These converters served as critical communication bridges between legacy field devices, such as circuit breakers and protection relays, and the SCADA monitoring system at the control center. By corrupting the firmware of these devices, the attackers rendered them inoperable, effectively severing communication between operators and field equipment.

In this setup, the converters translated serial data into Ethernet traffic, enabling centralized control and visibility. Disabling them disrupted this essential communication pathway, isolating substations and blinding operators to real-time system conditions, which prolonged the outage and complicated restoration efforts.

Following this manipulation, the attackers deployed KillDisk malware to wipe several systems, permanently deleting data and corrupting the **Master Boot Record (MBR)**. This rendered many servers and workstations completely unusable. The combination of firmware corruption and targeted data destruction was intentional, designed to amplify operational downtime, erase forensic evidence, and delay system recovery. These coordinated actions demonstrate a calculated effort to not only disrupt power operations but also to obstruct incident response and restoration efforts.

Finding the gaps in security and lessons learned

Various areas for improved recovery efforts can be identified from the cyberattack on the Ukrainian power utility company. By breaking down the attack in terms of security controls, we can pinpoint where improvements could have been made or where controls were lacking.

The initial access to the business or enterprise system was through spearfishing, which is difficult to avoid but can be mitigated through personnel training and robust email security. Vulnerabilities in software programs such as Microsoft and Windows could have been detected through continuous monitoring and the use of IDS and antivirus programs.

Additionally, the use of privileged credentials by the attackers highlights the importance of implementing security methodologies such as zero trust or least privilege, password rotations, and proper implementation of Windows group policies. Inadequate implementation of firewall rules underscores the necessity of periodic firewall audits to remove unnecessary or temporary rules. Proper network segmentation, separating the control network from the enterprise network, could

have prevented the lateral movement of attackers. *Table 4.6* summarizes the cyberattack stages, the systems or processes affected, and the corresponding security controls or strategies:

Cyberattack	**Systems Affected**	**Security Controls or Strategies**
Initial attack on the enterprise network through the email system, using spearfishing	Email system, business/ enterprise network	Personnel training, robust email security, and sandboxing
Lateral movement across networks from business to control	Malware access, tools being deployed	Network segmentation, separation of Active Directory domains, network monitoring
Vulnerabilities in software and firmware	Windows system, Office software, control system software, serial-to-Ethernet devices	Proper maintenance and firmware updates, patching, system upgrades
Loss of data	Hard drives and workstations	Maintaining backups for data and proper recovery procedures

Table 4.6 – Finding gaps in security control/strategies

Significance of the Cyber Kill Chain in incident management

The Cyber Kill Chain serves as more than just a theoretical model—it provides a structured and practical approach to understanding, anticipating, and disrupting an adversary's actions during a cyber incident. By breaking down an attack into its key stages, from reconnaissance to achieving objectives, it enables defenders to visualize the adversary's movement, identify points of detection or containment, and understand where defenses can be strengthened.

In the context of industrial incident management, the Cyber Kill Chain helps security and operations teams connect the dots between isolated alerts, network behavior, and operational impact. It transforms incident response from a reactive firefight into a proactive, intelligence-driven process that can prevent escalation and reduce downtime.

That said, while the framework is highly effective for structured, external attack paths, it has inherent limitations in dealing with insider threats, multi-vector web attacks, or cloud-based intrusions that fall outside traditional perimeters. For this reason, it should be complemented

with behavioral analytics, continuous monitoring, and robust OT-specific controls that reflect the unique architecture of IACS environments:

- **Understanding the attack landscape**: Breaking down a cyberattack into distinct stages, from initial reconnaissance to achieving objectives, enables asset owners to grasp the overall flow of how attackers operate. This framework offers insight into potential weaknesses in defenses at each stage.

  For example, during the Colonial Pipeline attack, the adversaries leveraged stolen credentials in the early access phase. Understanding this within the Cyber Kill Chain model helps teams recognize the importance of strong authentication and network segmentation before an attack escalates.

- **Incident analysis and forensics**: Analyzing incidents through the Cyber Kill Chain helps pinpoint where attackers may have initially breached the system. This focused approach aids forensic investigations by identifying specific vulnerabilities exploited.

  For example, in the 2015 Ukraine power grid attack, investigators traced the intrusion back to the delivery phase—a spear-phishing email containing a malicious attachment. Mapping this to the Cyber Kill Chain clarified the initial compromise, helping responders improve email filtering and awareness training.

- **Targeted response and mitigation:** Understanding the attacker's stage in the Cyber Kill Chain enables organizations to deploy precise countermeasures. Response strategies vary depending on where the threat is detected: reconnaissance, delivery, exploitation, or action on objectives.

  For example, if activity is detected during the reconnaissance phase, proactive measures such as disabling unused network services, reviewing firewall rules, or conducting user awareness refreshers can disrupt adversarial planning before exploitation occurs. Conversely, detecting an attacker in the lateral movement stage might prompt immediate network segmentation or credential resets.

- **Improving future defenses**: Analyzing past incidents with the Cyber Kill Chain reveals weaknesses in security posture at different stages. This insight enables the prioritization of vulnerability patching, detection mechanisms enhancements, or the addition of security controls at specific points in the attack chain.

For example, after a simulated ransomware drill mapped to the Cyber Kill Chain, an organization might find that its intrusion detection system failed to flag command-and-control traffic. The lesson learned leads to enhanced log correlation, better endpoint visibility, and refined rules for early detection in future scenarios.

Integrating the Cyber Kill Chain into incident management processes empowers asset owners to proactively defend critical systems and data against cyber threats. By understanding the stages of an attack and implementing targeted mitigation strategies, organizations can effectively mitigate the impact of cyber incidents and minimize potential damage.

IACS bring significant benefits to critical sectors such as power, manufacturing, and water utilities by enabling automation, remote operations, and improved situational awareness. However, these same features create unique vulnerabilities when targeted by determined adversaries.

The 2015 Ukraine power grid attack remains one of the most instructive examples of how a cyber operation can exploit both technical and procedural weaknesses. Attackers followed the stages of the Cyber Kill Chain, from reconnaissance and phishing to credential theft and remote access, eventually causing a physical power disruption. This event demonstrated that even well-engineered industrial systems are not immune to cyber exploitation. By studying such attacks through the lens of the Cyber Kill Chain, organizations can understand where defenses failed and apply those insights to build stronger response processes.

Now that we have explored how the Cyber Kill Chain strengthens incident management, let us reinforce these concepts through a hands-on exercise. This activity will help you visualize each stage of the Cyber Kill Chain, map it to your organization's environment, and identify where detection or response actions can be improved.

Exercise: Designing simulation exercises with the Cyber Kill Chain

Objective:

By integrating the Cyber Kill Chain into drills, organizations can better prepare their teams to anticipate, recognize, and effectively respond to cyber threats. This exercise is to make you comfortable working on creating scenarios and simulations.

Instructions:

- Develop scenarios for each stage of the Cyber Kill Chain.
- Describe in detail some of the roles and responsibilities of team members, such as attackers, defenders, and observers.

Example:

Here, we are going to divide the teams into three groups: a red team, a blue team, and observers. These will be covered in detail in *Chapter 10*, on running an **Incident Command System (ICS)** exercise. However, to complete this exercise, the red team is the attackers, the blue team is the defenders, and the observers are evaluators who take notes and provide feedback.

Reconnaissance:

The red team will gather information about the ICS network, such as IP addresses, software versions, and Windows credentials, using network tools.

The blue team will monitor for unusual data access patterns, analyze web traffic, and use threat intelligence to identify reconnaissance activities.

Weaponization:

The red team will create a script (malicious payloads) using Batch (BAT), PowerShell, or simply a phishing website to harvest credentials.

The blue team will implement and test endpoint protection systems to detect the creation and execution of the malicious payloads or block the web page.

Delivery:

The red team will attach a malicious payload by compressing it and sending a phishing email to an ICS operator.

The blue team will use email filtering and user training to detect and respond to phishing attempts. (In this case, consider the email as not being filtered or stopped.)

Exploitation:

The red team will then use the credentials obtained from the phishing attack to exploit the vulnerability to gain access to the IACS network or simply remote into the IACS workstation.

The blue team will monitor network and system logs for signs of exploitation attempts and ensure patches are up to date.

Installation:

The red team will install the malware on a compromised IACS device to establish persistence.

The blue team will attempt to use antivirus and **Endpoint Detection and Response (EDR)** tools to detect and remove unauthorized software installations.

Command and Control (C2):

The red team will establish a C2 channel to communicate with the compromised IACS device.

The blue team will continue to monitor network traffic for unusual patterns, such as outbound connections to suspicious IP addresses, and block C2 communications.

Actions on objectives:

The red team will attempt to manipulate the ICS parameters to cause a process disruption, such as altering PLC settings to shut down a critical process.

The blue team will detect and respond to unauthorized changes in the ICS, using incident response protocols to restore normal operations.

Reflection questions

- How did mapping each stage of the Cyber Kill Chain help you understand the attacker's perspective and improve your defensive strategies?
- Which stage of the Cyber Kill Chain do you think is most challenging to detect or mitigate within an IACS environment, and why?
- What lessons did your team learn about communication and coordination between the red, blue, and observer teams during the simulation?
- If you were to run this exercise again, what improvements or additional injects would you include to make it more realistic or effective?

This exercise demonstrates how the Cyber Kill Chain can be applied to strengthen incident preparedness and awareness within IACS environments. By simulating attacker and defender actions across each stage, participants gain a clearer understanding of adversary tactics, detection opportunities, and coordinated response measures. The goal is not only to test technical capabilities but also to enhance teamwork, communication, and analytical thinking—key elements in building a resilient cybersecurity culture.

Summary

This chapter provided an extensive overview of the convergence of **Information Technology** (**IT**) and **Operational Technology** (**OT**) within the context of the Industrial Revolution and the advent of Industry 4.0. We compared the distinct roles and security concerns of IT and OT, highlighting the unique challenges in securing OT systems. The chapter detailed security levels based on ISA/IEC 62443 standards, emphasizing the criticality and impact levels of OT systems.

Historical cyber incidents in OT environments were examined, including a case study on the December 23, 2015, cyberattack on the Ukrainian power grid. Utilizing the Cyber Kill Chain framework and lessons from historical incidents will enhance your ability to detect, disrupt, and mitigate cyber threats. This chapter equipped you with the tools and insights necessary to proactively defend critical systems and data against cyber threats. In *Chapter 5*, we are going to explore emergency operations and the **Emergency Operation Center** (**EOC**) in CI and their significance within an organization's incident response plan.

Further reading

- **Official MITRE ATT&CK**:
- A globally recognized framework that catalogues adversary **Tactics, Techniques, and Procedures** (**TTPs**) observed in real-world attacks. It helps organizations strengthen detection, response, and defense strategies: `https://attack.mitre.org/`
- **Cyber Kill Chain by Lockheed Martin**:
- A foundational model outlining the typical stages of a cyberattack—from reconnaissance to actions on objectives—enabling defenders to identify and disrupt threats at each stage: `https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

Part 3

Pillar 3 — Incident Command Systems (ICS) for Industrial Environments

Pillar 3 introduces **Incident Command Systems (ICS)** as the structural pillar that enables coordinated response during incidents. In critical infrastructure environments, ICS provides a common command, control, and communication framework that brings together cybersecurity, operations, safety, and emergency response teams.

This pillar connects technical understanding with organizational execution. It emphasizes role clarity, decision-making under pressure, and scalable command structures that support both cyber and physical incident management in industrial settings.

This part of the book includes the following chapters:

- *Chapter 5, Emergency Operations and Their Significance in an Organization*
- *Chapter 6, Introduction to the Incident Command System (ICS)*
- *Chapter 7, Practical Considerations for Incident Management in IACS*
- *Chapter 8, Introduction to Incident Management Standards and Frameworks for Critical Infrastructure*

5

Emergency Operations and Their Significance in an Organization

Emergency operations can be defined as the branch or department of an organization responsible for executing emergency functions such as communications, resource management, coordination, safety, situational awareness, recovery planning, and more.

In this chapter, we will explore the basic concepts of incident management by examining various methods of planning, including incident plans, business continuity plans, and disaster recovery plans. We will also discuss the significance of establishing an emergency operations center for critical infrastructure. The goal of this chapter is to pave the way for understanding the **Incident Command System (ICS)**, which will be explored in *Chapter 6*. While most knowledge outlets and various books on ICSs cover the ICS and its components in detail, this book focuses on the exploration and availability of emergency operations in an organization in the critical infrastructure space; these topics are key to building incident response capabilities and achieving continuous improvements in ICS adoption.

We will cover the following topics in this chapter:

- What are emergency operations?
- Significance of emergency operations
- Types of incidents
- Industrial incidents in OT versus security incidents in IT
- Safety in the context of OT security incidents
- Emergency operations management

What are emergency operations?

Emergency operations typically consist of leadership positions at the top, followed by specialized and expert team leaders. *Figure 5.1* illustrates a typical organizational structure for emergency operations, though the exact arrangement may vary slightly from one company to another:

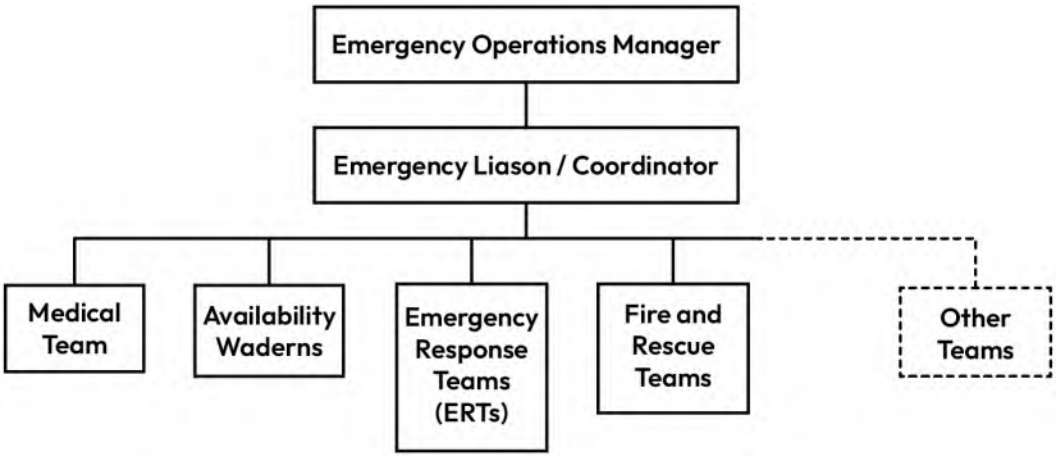


Figure 5.1 – Organizational structure of emergency management

At the top of the organizational chart is the **Emergency Operations Manager (EOM)**, the face of the emergency operations; they are responsible for the overall personnel and resource management for the organization.

For example, in a manufacturing plant, the EOM, sometimes also referred to as the emergency manager or crisis management leader, is responsible for conducting risk assessments, developing and maintaining emergency response plans, and ensuring compliance with safety regulations. They train personnel, conduct drills, coordinate with local emergency services, and lead incident command during emergencies. Their role includes managing emergency resources, conducting post-incident analyses, engaging with the community, and continuously improving safety measures. This ensures that the plant is prepared for emergencies, minimizing risks and protecting personnel and the environment.

In general, emergency operations consist of specialized groups and expert teams such as the following:

- **EOM**: The EOM oversees the entire response operation, sets objectives, and coordinates team activities. They serve as the key decision maker, ensuring effective communication, managing resources, and adapting strategies as the situation evolves. The EOM also liaises with external agencies and maintains situational awareness to support a coordinated recovery.

- In some organizations, this role may also be referred to as the **Incident Commander (IC)** or align with positions such as security officer, facility security officer, or physical security officer, as it often carries multiple duties and functions.
- **Medical team**: The medical team provides immediate first aid and medical care to injured personnel, stabilizes patients, and coordinates with external medical services for evacuation and further treatment.
- **Accountability wardens**: They ensure that all personnel are accounted for during an emergency, conduct roll calls at designated safe areas, and report missing individuals to the EOM.
- **Emergency Response Team (ERT)**: This team is responsible for coordinating the overall emergency response efforts, managing resources, and communicating with internal and external teams to implement the emergency plan effectively.
- **Fire and rescue team**: This team specializes in fire suppression, conducts search and rescue operations, and ensures the safe evacuation routes while working closely with local fire departments.
- **Hazardous Materials (HAZMAT) team**: This team has a very important role, especially in the oil and gas and chemical manufacturing sectors. They are responsible for the identification, containment, and mitigation of hazardous material spills and leaks, decontaminating affected areas, and ensuring compliance with safety regulations and protocols. This team is also sometimes referred to as the chemical spillage control team.
- **Facility security team**: This team's typical role is to maintain the site's security during an emergency, control access to the affected areas, and assist in the safe evacuation of personnel while preventing unauthorized entry. This usually consists of the facility security personnel and guards.
- **Other teams**: Depending on operational needs and emergency protocols, organizations may deploy specialized response teams. For example, the **Nuclear Incident Response Team (NIRT)**—comprising resources from the **Department of Energy (DOE)** and the **Environmental Protection Agency (EPA)**—is activated by FEMA under the Department of Homeland Security to respond to nuclear or radiological emergencies.

Note

Recent regulations, such as those from the U.S. Coast Guard, now also require the inclusion of a cybersecurity team, led by a designated cybersecurity officer, as part of the overall facility security structure. This ensures that cyber threats are addressed alongside physical and operational risks during an incident.

In summary, *emergency operations* refers to the branch or department responsible for overseeing essential functions such as communication, resource management, coordination, safety, situational awareness, and recovery.

Significance of emergency operations in CI organizations

The concept of an emergency can differ slightly between the public and private sectors due to their core functions and priorities. **Public sector emergencies** focus on public safety and well-being, encompassing scenarios such as natural disasters (floods, hurricanes, etc.), pandemics, technological disasters (cyberattacks on critical infrastructure), civil unrest, and large-scale accidents. The response to these emergencies involves evacuation procedures, search and rescue operations, resource mobilization (firefighters, police, medical personnel, etc.), damage assessment, public health measures, and financial aid and recovery programs, often funded by government budgets, federal grants, and emergency relief funds. In contrast, **private sector emergencies** focus on business continuity and minimizing disruption, including events such as IT outages, data breaches, product recalls, workplace accidents, and supply chain disruptions. Responses involve incident management to contain and resolve the issue, communication with stakeholders (customers, investors, employees, and the community), activation of business continuity plans (backup systems and data recovery), and risk assessment and mitigation strategies. Private companies typically rely on their own resources, such as insurance and emergency funds, to manage internal crises, but may have external support through mutual aid and retainers for more specialized resources.

Regardless of the public or private sector, the main goal of emergency operations is to effectively manage and coordinate responses to emergencies and disasters to protect lives, property, and the environment. This involves ensuring public safety, minimizing the impact of the emergency, and facilitating recovery and return to normal operations. In private sector settings, such as chemical manufacturing or processing facilities, minimizing community impact is often placed among the highest priorities, even ahead of financial considerations, reflecting the organization's commitment to safety and social responsibility.

To effectively manage and coordinate responses to emergencies, understanding the nature of various incidents is crucial. In the next section, we will explore different types of incidents, distinguishing between industrial and IT-related events, to better prepare and tailor emergency operations strategies.

Types of incidents

Emergencies happen because of an accident or an incident. The National Safety Council defines an **accident** as an undesired event that results in personal injury or property damage. The **Occupational Safety and Health Administration** (**OSHA**) defines an **incident** as an unplanned, undesired event that adversely affects the completion of a task.

In certain sectors, such as transportation and maritime operations, the term *incident* carries additional significance. For example, within the **Transportation Systems Sector** (**TSS**), a **Transportation Security Incident** (**TSI**) is defined by four key impacts: significant loss of life, environmental damage, transportation disruption, or major economic impact. While rooted in the maritime domain, this definition extends to all transportation modes, including aviation, rail, highways, pipelines, and ports. A cyberattack on a freight rail system, for instance, could meet the TSI definition, even if the facility is not **Maritime Transportation Security Act (MTSA)**-regulated.

Similarly, various organizations define incidents based on their specific contexts and priorities, encompassing factors such as the nature of the disruption, the potential for harm, and the required response to manage the situation. This is why an organization needs to come together and define what an incident is for them, ensuring a clear and consistent understanding that guides their emergency response and risk management strategies.

Building on the risk management foundation of threats and vulnerabilities (which we explored in *Chapter 2*), incident response considers the broader impact on operations, safety, finances, reputation, and the environment. Effective response requires swift action, leveraging available resources, and coordinated communication across internal teams and with external agencies. Compliance with legal, regulatory, and industry requirements is crucial, as is implementing business continuity plans to maintain vital functions.

For incidents originating from a cyberattack, the first step is detecting that an incident has occurred. This type of detection is typically provided by the organization's threat detection systems, **Security Information and Event Management** (**SIEM**), and safety monitoring systems. Much like the maturity of an organization in other areas, such as physical security and process safety, quickly identifying incidents is also linked to continuous improvement in its processes.

Note

While detecting an event is a critical factor, the scope of this book focuses on the management of such incidents.

However, it is important to note that an event or a series of events can lead to an incident. Furthermore, small events can escalate into major incidents. For instance, a minor power fluctuation may initially seem harmless but could lead to a widespread outage if it causes cascading failures in the electrical grid. Another common example is an anomaly in network traffic that might indicate a minor security issue, but could turn out to be a precursor to a larger cyberattack, which can escalate into a major breach affecting sensitive data. This is very much evident in the concept of the incident pyramid, as shown in *Figure 5.2*:

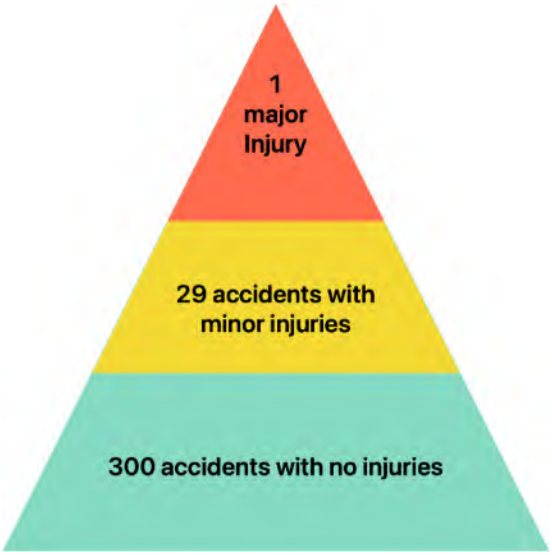


Figure 5.2 – Heinrich's Pyramid, or the incident pyramid, showing industrial accident prevention theory

The concept of the incident pyramid was first introduced by Herbert William Heinrich, an American industrial safety pioneer, in his 1931 book *Industrial Accident Prevention: A Scientific Approach*. Often called Heinrich's Pyramid or the Heinrich Triangle, it illustrates the relationship between different levels of incidents: for every major injury, there are 29 minor injuries and 300 near misses, which are incidents or accidents with no injuries, as shown in *Figure 5.2*.

Before we apply this concept to OT and cybersecurity, it's important to define the terms in the safety context:

- **Major accident**: A serious event causing significant harm or damage
- **Minor accident**: An incident causing limited harm or damage
- **Near miss**: An event that could have caused harm or damage but did not, due to timely intervention or luck

The principle still applies to OT and cybersecurity, as shown next; addressing low-level indicators can prevent major breaches (*Figure 5.3*):

- **Major security breach**: This is the most significant incident that causes severe operational, financial, or reputational damage
- **Minor security incidents**: These are smaller incidents that cause limited disruption or damage but could escalate if not addressed
- **Near misses**: These are events that could have led to a security incident but were identified and mitigated in time
- **Unexpected activities**: These are unusual network activities or behaviors that do not immediately lead to a security incident but indicate potential vulnerabilities

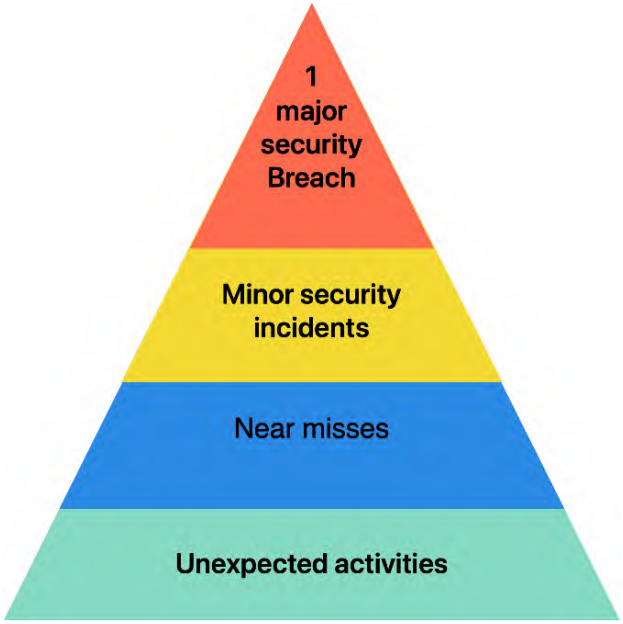


Figure 5.3 – Heinrich's Pyramid applied to OT security

Safety and security address different challenges; **safety** aims to prevent accidents and safeguard people and systems from harm, while **security** protects systems and data from malicious threats. Both share common principles that can enrich our approach to incident management.

By actively detecting and addressing near misses and unexpected activities, organizations can greatly reduce the chances of major breaches—just as in the safety world. In the next section, we'll examine a case study to see how the incident pyramid applies in practice, identifying the different types of incidents in both OT security and safety contexts.

Case study: The Colonial Pipeline cyberattack

Colonial Pipeline, an American oil pipeline system originating in Houston, Texas, experienced a ransomware cyberattack on May 7, 2021. This attack significantly disrupted operations, highlighting vulnerabilities in the computerized equipment managing the pipeline. You can read about it here: `https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years`.

While the Colonial Pipeline incident is well documented, we will analyze it from a specific perspective, emphasizing the various layers that make up a security incident. In real-world situations, the terms *complications* or *contingencies* refer to unexpected or unforeseen issues that arise and demand immediate attention. In the following table, we will break down these complications, which represent different types of security incidents, and correlate them with their potential impacts:

Type of security event	**Event description**	**Security impact**
Unexpected activities	Unexpected activities included abnormal network traffic patterns, which indicated possible probing by attackers or the initial stages of a cyberattack. While we may not know for sure, typically, in the case of a ransomware attack, attackers usually use stolen credentials and try to access systems to test their capabilities. Additionally, strange system behaviors, such as unexplained reboots or software crashes, suggested potential but unconfirmed security issues. These activities served as early warning signs of underlying security problems that required attention.	None
Near misses	Near misses were also present, such as phishing attempts that were successfully thwarted, which could have compromised systems if not identified and mitigated in time. Moreover, the detection and neutralization of unusual login activities prevented them from escalating into significant security incidents. These near misses highlighted the importance of vigilance and quick response in cybersecurity practice.	Low
Minor security incidents	Minor security incidents included unpatched vulnerabilities in their **virtual private network** (**VPN**) systems, which made the network more susceptible to attacks. Additionally, there was unauthorized access that may not have been detected and blocked, showcasing ongoing threats and highlighting the importance of maintaining strong access controls.	Medium

Major security breach	The major security breach was the ransomware attack that caused a complete operational shutdown at Colonial Pipeline. This led to a severe disruption in the fuel supply across the Southeastern U.S., resulting in financial losses and significant damage to their reputation. The attack underscored the critical need for robust cybersecurity measures in protecting vital infrastructure.	High

Table 5.1 – Incident management breakdown of the Colonial Pipeline incident

Minor security incidents, such as unpatched VPN vulnerabilities and unauthorized access, exposed the network to ongoing threats, underscoring the importance of strong access controls. Near misses, such as thwarted phishing attempts and unusual login activities, demonstrated the value of vigilance and swift response in mitigating potential threats. Additionally, unexpected activities, such as abnormal network traffic patterns and unexplained system behaviors, served as early warning signs of vulnerabilities, signaling potential probing by attackers or the onset of cyberattacks. Together, these incidents emphasized the necessity for proactive security measures and constant monitoring in safeguarding critical assets.

Note

The Colonial Pipeline incident, a publicly disclosed cyberattack against critical infrastructure in the U.S., involved multiple stages targeting the company's IT systems, though the operational technology systems moving oil were not directly compromised. Despite the hackers' demands being initially met with a ransom payment of 75 Bitcoin (approximately $4.4 million), federal authorities recovered nearly half of this amount. This disproved the notion that ransoms paid in Bitcoin are irrecoverable due to the cryptocurrency's perceived opaqueness and transaction anonymity.

It is essential to understand the key differences between security incidents in **Operational Technology (OT)** and **Information Technology (IT)**. For example, in IT, a ransomware attack may primarily affect data access, while in OT, the same attack could halt physical operations and impact safety. This distinction is critical because it determines whether the appropriate incident response procedure should focus on safe system recovery or controlled shutdown to protect people, assets, and the environment.

In the next section, we will examine these OT/IT differences in detail to ensure that response strategies are applied effectively.

Industrial incidents in OT versus security incidents in IT

The timeline for an IT security incident begins with normal operations, where systems are continuously monitored and maintained. When a disruption, such as a cyberattack or system failure, occurs, IT and security experts promptly identify and isolate the issue to prevent further impact. This may necessitate a controlled shutdown of affected systems. Detailed analysis follows to pinpoint the root cause and implement remediation actions to fix vulnerabilities. Once secure, systems are gradually rebooted and restored to ensure stability. Normal operations resume after thorough testing, and a post-incident review is conducted to document the incident, extract lessons learned, and update security protocols. Effective IT incident management hinges on the collaboration of IT professionals, security specialists, and operational staff to maintain system integrity and resilience.

Similarly, the timeline for an OT security incident starts with normal operations, where OT systems and ICSs function smoothly under routine monitoring. Upon detecting a disruption, likely due to cyberattacks or hardware failures, ICS experts and security personnel swiftly identify and contain the issue. A controlled shutdown of affected OT systems follows to prevent further damage. Analysis and remediation are conducted to address vulnerabilities, leading to a secure system reboot and gradual restoration. After resuming normal operations, a post-incident review is performed to document actions, learn lessons, and update protocols, ensuring enhanced preparedness for future incidents. Effective OT incident management relies on the collaboration of ICS experts, security and network professionals, and operations personnel.

However, incidents in OT and IT systems differ greatly in nature, impact, and response. OT incidents, such as malfunctions in industrial control systems, can lead to real-world dangers such as equipment failures, chemical spills, fires, or explosions. These pose immediate threats to people, the environment, and critical infrastructure, requiring swift emergency responses, safety protocols, and physical containment measures. In contrast, IT incidents typically involve digital threats such as outages, data breaches, or cyberattacks, impacting data integrity, business operations, and digital infrastructure. Here, the focus is on data recovery, cybersecurity measures, and minimizing downtime through technical interventions.

Despite these differences, both IT and OT systems can rely on some of the same hardware components, but with varying priorities. For instance, both might utilize hard drives for data storage. However, an IT system prioritizing data security might emphasize features such as data mirroring or **Redundant Array of Independent Disks (RAID)** configurations for quick data recovery in case of drive failure. In contrast, an OT system focused on real-time process control might prioritize using a single, high-performance drive for faster data access, even if it comes at the cost of some redundancy for recovery purposes. This difference in priorities can significantly impact recovery procedures. An IT system administrator might prioritize recovering lost data from a mirrored drive during an outage, even if it means some downtime. On the other hand, an OT engineer might prioritize quickly replacing the failed drive with a new one to get critical industrial processes back online as soon as possible, potentially sacrificing some data recovery efforts if they are not essential for immediate operations.

Figure 5.4 presents a timeline of an IT incident at a high level. *Event 1* in the timeline highlights the occurrence of an incident, followed by the escalation of an IT incident:

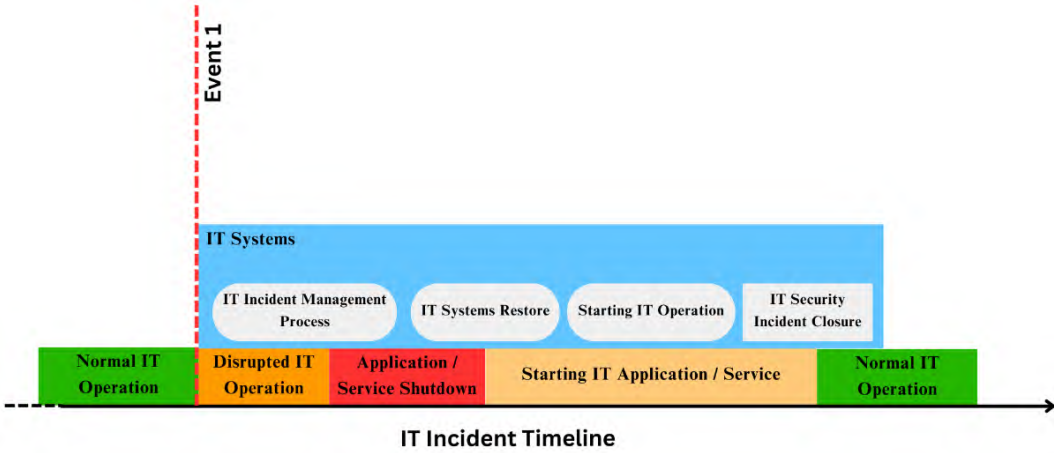


Figure 5.4 – A high-level timeline of an incident in IT

The focus is on swiftly restoring normal IT operations, whether it pertains to an application, a web server, or any other service provided by the organization. Once systems are fully restored and operations have returned to their standard state, the incident is formally closed.

Figure 5.5 shows a high-level timeline for OT incidents. The timeline for an OT security incident begins with normal operations:

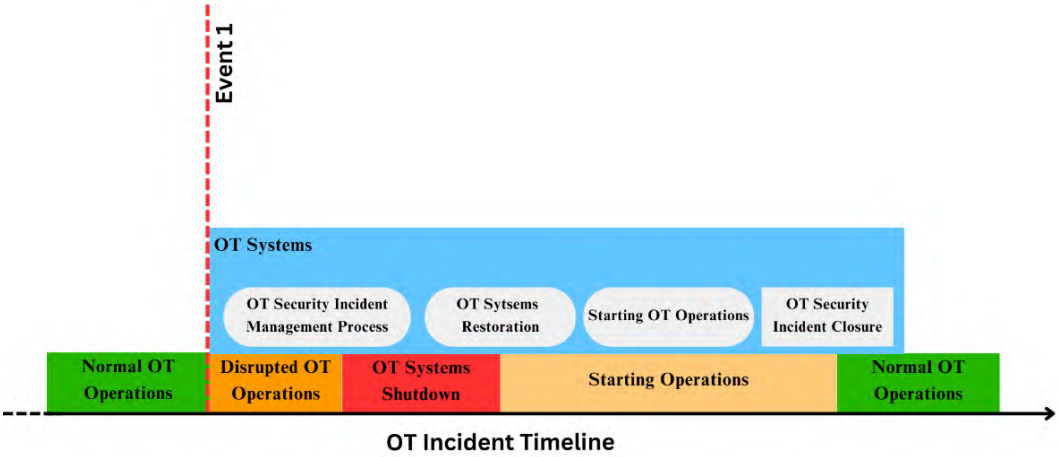


Figure 5.5 – A high-level timeline of an incident in OT

The focus is on understanding how an incident unfolds across the OT environment. This figure illustrates an incident originating within OT systems, showing how operations transition from normal functioning to disruption, controlled shutdown, restoration, and finally, back to a stable operational state. It highlights the sequence of response activities, such as incident management, system restoration, and closure, that bring operations back online safely and securely.

While this example represents an OT-originated incident, it is important to recognize that in real-world scenarios, incidents can also begin in IT networks or even at the business application level. Weak segmentation, remote connectivity, or shared authentication paths can allow an IT compromise to spill over into OT, potentially disrupting critical industrial processes.

Figure 5.5 is significant because it visualizes the structured response flow in OT environments and reinforces the importance of defense in depth, coordinated response, and clear recovery steps. Whether an event begins in OT or IT, effective detection, containment, and restoration are what determine the resilience of an organization's operations.

Incidents in CI

Figure 5.6 shows a typical scenario that we may come across for incidents in CI. Here, the initial entry point, *Event 1*, of a cyberattack originates from an IT-related breach, such as a phishing attack, marking the start of the IT security incident. Despite the IT breach, manufacturing operations might still be normal at this stage.

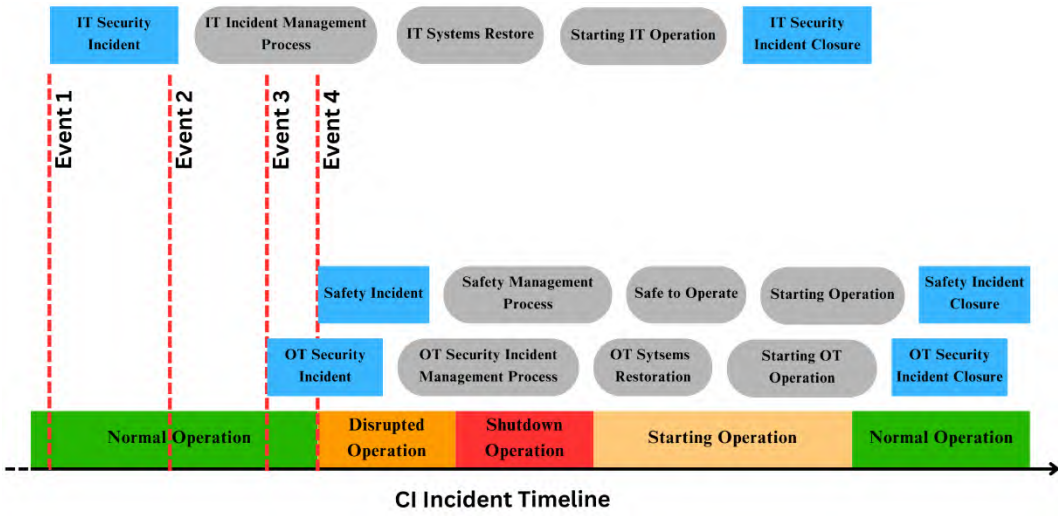


Figure 5.6 – Comparison of IT incident vs. CI incident with ICSs

Event 2 could involve network proliferation, such as a ransomware attack or a worm spreading through business systems. This escalation leads to *Event 3*, where the attack reaches OT networks, initiating the OT security incident and disrupting industrial floor operations.

Event 4 indicates the disruption that can lead to a full-blown OT security incident, which often has the potential to escalate into a safety incident. Each component—IT, OT, and safety—follows its own incident management life cycle. The ultimate goal of managing an OT security incident through the emergency operations center is to maintain safety during the incident and restore normal operations.

Note

In the context of cybersecurity and incident response, **injects** are planned events or pieces of information introduced into a training exercise or simulation to simulate real-world scenarios. Injects are designed to test and evaluate the responses, decision-making, and procedures of participants under realistic conditions. The term *event* is used while managing an actual incident. By incorporating injects into exercises, organizations can better prepare their teams for actual cyber incidents, ensuring that they can effectively respond to and mitigate threats.

We analyzed the incidents and their timeline concerning IT, OT, and CI, recognizing that these incidents can be highly complex, requiring collaboration between IT and OT stakeholders. A critical aspect that often gets overlooked in IT or OT incident management discussions is the safety context. We will delve into safety within the framework of OT security incidents to highlight its importance.

Safety in the context of OT security incidents

In the CI and incident management context, *safety* refers to protecting individuals, operations, the environment, and the public from danger, risk, or injury. This includes ensuring the health and well-being of personnel, maintaining secure and reliable system functions, preventing environmental harm, and safeguarding communities from potential hazards.

Shutting down systems during an industrial incident and starting up systems during the recovery stages of incident management is a critical process that requires substantial consideration. The personnel involved must thoroughly understand these considerations to ensure safety and efficiency.

Understanding the specific phases of operation, particularly in CI and process industries, is crucial. The terms *startup* and *shutdown* refer to these phases. **Startup** is when a plant or system is brought into operation from a non-operational state, while **shutdown** is when the system is taken out of operation. The startup and shutdown phases, more than regular operations, are hazardous. The **Center for Chemical Process Safety** (**CCPS**) has found that most process safety incidents occur during plant startup, despite this phase constituting only a small portion of a plant's operating life. According to CCPS, process safety incidents are five times more likely to happen during startup than regular operations.

Similarly, many safety incidents also occur just before or after a shift change. These periods often involve high activity, incomplete handovers, and simultaneous maintenance or operational adjustments. Critical information about equipment status, alarms, or ongoing process deviations may not be communicated clearly between outgoing and incoming personnel. As a result, gaps in situational awareness or misunderstanding of current operating conditions can increase the likelihood of human error, leading to process upsets or safety events.

Consider the example of a nuclear power plant. The startup and shutdown processes in a nuclear power plant are critical operations that must be conducted safely. This involves more than simply turning equipment on or off; it requires precise control and monitoring to prevent hazardous conditions.

During startup, nuclear reactors must be brought to a critical state where nuclear fission becomes self-sustaining. This process involves gradually increasing the reactor power while carefully monitoring and controlling reactor parameters to avoid a rapid power increase, which could lead to an uncontrolled reaction or even a meltdown.

Similarly, during shutdown, the reactor must be carefully brought to a subcritical state, ensuring that fission reactions cease in a controlled manner. This involves gradually inserting control rods to absorb neutrons and slow the fission process. Rapid or improper shutdown can result in thermal stress on reactor components, potential radiation release, and other safety hazards.

In the chemical manufacturing sector, maintaining a specific temperature during chemical processes is essential for ensuring safety. Temperature directly affects reaction rates, product stability, and the overall safety of the operation.

Figure 5.7 illustrates a conventional batch reactor surrounded by an outer jacket, through which heat transfer occurs during circulation:

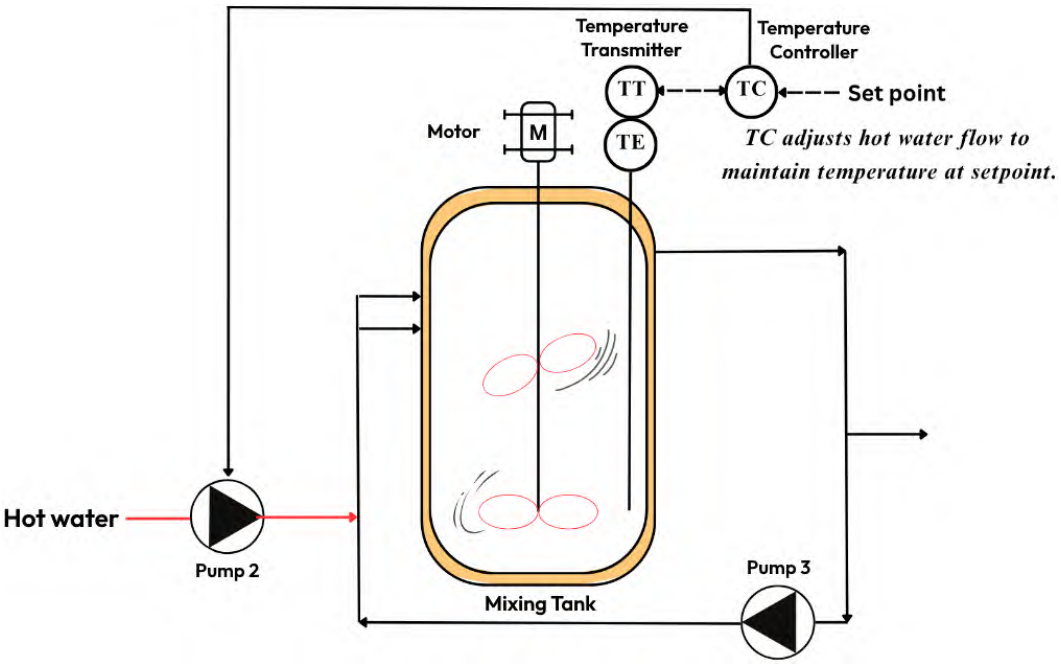


Figure 5.7 – A conventional batch reactor in a chemical manufacturing process

A steam-heated jacket envelops the reactor vessel, transferring heat from the steam into the chemical solution inside. The jacketed design allows for precise heating or cooling of the reactor contents, maintaining the desired reaction temperature.

This temperature control is vital during normal operations and becomes even more critical during process upsets. Precise temperature management prevents dangerous situations such as runaway reactions, equipment damage, or even explosions. In the event of a process upset, such as a sudden change in reactant concentration or an unexpected exothermic reaction, it becomes crucial to manage the temperature effectively. Failure to do so can lead to catastrophic outcomes, putting both personnel and equipment at risk.

The complexity and risks associated with these operations underscore the necessity of following stringent safety protocols to protect the plant personnel and the surrounding environment. The consequences of improper startup or shutdown can be catastrophic, as evidenced by historical incidents such as the **Three Mile Island** accident, where a partial meltdown occurred due to operator errors during the shutdown process.

Note

The Three Mile Island accident was a partial nuclear meltdown of the Unit 2 reactor (TMI-2) at the Three Mile Island nuclear generating station on the Susquehanna River in Londonderry Township, near Harrisburg, Pennsylvania. The incident began at 4:00 a.m. on March 28, 1979, releasing radioactive gases and iodine into the environment. It stands as the worst accident in the history of U.S. commercial nuclear power plants. The TMI-2 reactor accident is rated Level 5, an *accident with wider consequences*, on the 7-point logarithmic International Nuclear Event Scale.

Another crucial aspect of incident response is effective emergency operations management. The upcoming section will delve into the significance of this topic, as the entire incident response hinges on the principles of well-executed emergency management. In this next part, we'll explore how these principles play a vital role in managing incidents effectively.

Emergency operations management

Emergency Operations Management encompasses the systematic organization and application of resources and processes to prepare for, respond to, and recover from emergencies, aiming to minimize their impact and ensure operational continuity. This involves preparedness through planning, training, and risk assessment; effective response through resource deployment and coordination; recovery efforts to restore normal operations; and mitigation strategies to reduce

future risks. In this context, we will explore key topics such as incident management, various incident management frameworks, the critical importance of clear communication channels, and the development of comprehensive emergency planning. This comprehensive approach ensures that organizations are well-equipped to handle emergencies efficiently and maintain resilience.

Incident management

Incident management is the process of identifying, assessing, and addressing incidents that disrupt normal operations or pose threats to an organization's systems, processes, or assets. It involves a series of coordinated actions to quickly restore normal operations and prevent future occurrences, and also encompasses all activities and strategies to manage and respond to incidents.

Effective incident management follows a structured approach that includes identifying, containing, responding to, remediating, and closing incidents. *Identification* involves detecting and confirming that an incident has occurred; *containment* focuses on limiting its spread or impact; *response* refers to immediate corrective actions to stabilize operations; *remediation* involves implementing longer-term fixes and recovery steps; and *closing* an incident means verifying that all corrective actions are complete, lessons learned are documented, and approval is obtained from relevant stakeholders to formally conclude the case.

Different frameworks and standards may refer to these phases using varying terminologies, but the core principles remain the same. Let's learn about the phases of incident management.

Phases of incident management

A *phase* in incident management represents a distinct stage in the life cycle of managing an incident, from initial detection to final resolution. Each phase comprises specific activities and objectives designed to systematically handle and mitigate the incident's impact. This structured approach ensures comprehensive and effective management of incidents. We can define these phases as identification, containment, response, remediation, and closure, as shown in *Figure 5.8*:

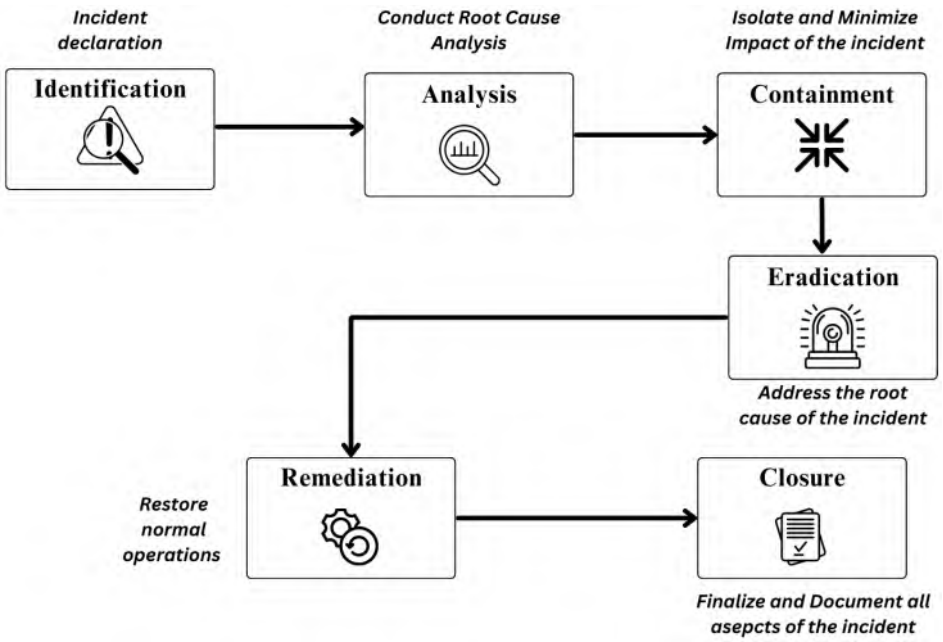


Figure 5.8 – Phases of incident management

Let's go through each phase:

1. **Incident identification**: This is the critical first step in any incident response process. It involves recognizing that something unexpected has happened that disrupts or has the potential to disrupt normal operations. *Not all disruptions are classified as incidents*. Incidents can be identified through various channels: user reports via email, phone, or service desks, automated alerts from monitoring tools, and proactive discovery during maintenance or routine system checks. Advanced systems such as **Intrusion Detection Systems (IDSs)**, SIEM platforms, network monitoring tools, and anomaly detection algorithms help detect abnormal behavior or potential breaches in real time, prompting further investigation.

Note

In the 2015 Ukrainian power grid cyberattack, which was covered in *Chapter 4* as a case study, operators at Prykarpattyaoblenergo power distribution didn't just see a single red flag. They witnessed multiple suspicious activities: substations disconnecting unexpectedly and unauthorized access to control systems. These combined signs left no doubt that a significant cyber incident was unfolding.

2. **Incident analysis**: Also referred to as **Root Cause Analysis (RCA)**, this phase involves verifying that the event is a true incident, assessing its impact, and determining its underlying cause. The analysis often includes reviewing system logs, network traffic, and forensic data to understand what happened, how it happened, and which systems or data were affected. This step guides decision-making for containment and remediation.

Note

In practice, initial containment actions often occur concurrently with early analysis, especially if the incident poses an immediate risk. Full RCA typically follows once the situation is stabilized.

3. **Incident containment**: Containment involves taking immediate and strategic actions to halt damage and prevent further spread of the incident. Short-term containment may include isolating affected systems, disabling compromised accounts, or blocking malicious IP addresses. Long-term containment focuses on maintaining essential operations while preparing for eradication and recovery. Techniques such as network segmentation, system isolation, and implementing temporary firewall rules are commonly used. The goal is to stabilize the environment without disrupting critical services.

Note

In cybersecurity, containment typically occurs after the incident analysis phase, once the threat has been verified and its scope understood. The goal is to isolate affected systems, limit spread, and prevent further compromise.

In contrast, during a physical incident such as a chemical spill, containment is an immediate safety action taken right after the event to stop the spread of hazardous material. This distinction highlights how the timing and intent of containment differ between cyber and physical domains. One focuses on technical isolation after assessment, while the other prioritizes immediate physical control to protect people and the environment.

4. **Incident eradication**: Eradication focuses on completely removing the root cause of the incident and any residual threats from the environment. This may involve deleting malware or malicious code, removing unauthorized user accounts, patching exploited vulnerabilities, restoring corrupted configurations, and strengthening access controls.

In OT environments, this could also mean resetting PLCs, validating firmware integrity, or restoring logic from trusted backups. The objective is to ensure the threat cannot re-emerge once systems are restored.

5. **Incident remediation**: Remediation involves restoring normal operations, validating that systems are secure, and ensuring business continuity. This includes recovering data from clean backups, validating restored systems against known baselines, and implementing security improvements identified during analysis. Remediation bridges the transition from response to recovery.
6. **Incident closure**: Closure marks the formal conclusion of the incident management process. It involves documenting all actions taken, summarizing findings, preparing reports, and conducting a post-incident review to capture lessons learned. This phase also includes verifying that corrective actions were successful and ensuring all systems are fully operational. Closing an incident means the organization has confirmed containment, eradication, and remediation are complete, stakeholders have approved closure, and insights are integrated into training or procedural updates to strengthen future resilience.

These phases are supported and guided by incident management frameworks, which provide structured approaches and best practices for handling incidents effectively.

Incident management frameworks

Incident management frameworks provide guidelines, best practices, and processes for effectively handling and responding to security incidents, ensuring efficient resolution and continuous improvement.

In recent years, numerous frameworks have emerged from both industrial and business IT sectors, each addressing specific needs in incident management and cybersecurity. One such pivotal framework is the ICS, which was developed by FEMA in the 1970s following devastating wildfires in California (`https://training.fema.gov/is/coursematerials.aspx?code=IS-100.c`).

Initially, it was aimed at enhancing the coordination and management of emergency responses across multiple agencies. Now, ICS has evolved into a comprehensive system adopted widely in public and private emergency response sectors. Formally adopted by various public and private organizations, its flexibility and scalability have proven effective in managing incidents ranging from natural disasters to industrial accidents, solidifying its status as the standard incident management system in the U.S. under **Homeland Security Presidential Directive 5 (HSPD-5)** since 2003. Continuously refined based on lessons learned, ICS remains a cornerstone of global emergency management, ensuring efficient incident response and interoperability among diverse response organizations.

Another critical framework is the NIST **Cybersecurity Framework (CSF)**, which addresses incident management and cybersecurity across critical infrastructure sectors. Developed by the **National Institute of Standards and Technology (NIST)** in response to *Executive Order 13636*, the NIST CSF integrates established cybersecurity standards and practices into a structured approach featuring *Core*, *Implementation Tiers*, and *Profiles* components. It is adopted across the globe, particularly in finance, healthcare, and government, and has become integral to regulatory frameworks and organizational cybersecurity strategies. Its significance in incident response lies in providing systematic methods for identifying, protecting, detecting, responding to, and recovering from cybersecurity incidents. In *Chapter 9*, we will explore additional frameworks.

Incident response life cycle

To fully grasp the phases and stages of incident management, it's essential to differentiate between incident management and the incident response life cycle. While these terms are sometimes used interchangeably, they refer to different aspects of handling emergencies. Incident management encompasses the overall strategy, processes, and resources deployed to manage incidents effectively. It involves planning, coordination, and decision-making to mitigate the impact of disruptions. On the other hand, the incident response life cycle outlines the sequential stages that an incident progresses through, from detection and containment to eradication, recovery, and post-incident analysis. Understanding this distinction is critical for implementing comprehensive incident management strategies and ensuring a structured approach to handling incidents from start to finish.

Note

While frameworks may define different numbers of stages, one common and essential element is the preparation stage. It is the proactive phase where organizations build readiness by developing plans, defining roles, testing tools, and ensuring coordination so that when an incident occurs, the response is organized and effective.

According to NIST, the incident response life cycle is structured into three primary stages (`https://csrc.nist.gov/projects/incident-response`):

- **Detect**: This entails identifying the occurrence of an incident through monitoring, alert systems, or anomaly detection
- **Respond**: This entails implementing immediate actions to contain and mitigate the incident, limiting its scope and impact
- **Recover**: This entails restoring normal operations and services to resume regular business functions

Figure 5.9 depicts the incident response life cycle model from **Special Publication (SP)** 800-61 Revision 3, released by NIST for public comments:

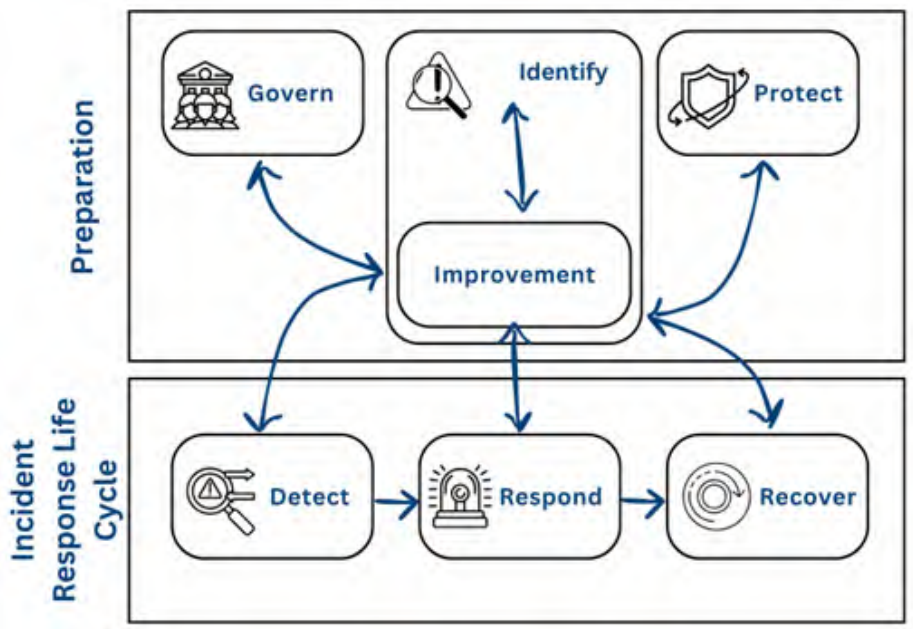


Figure 5.9 – The incident response life cycle model in SP 800-61 Revision 3

The incident response life cycle itself is shown in the bottom half of the figure and includes three stages: *Detect*, *Respond*, and *Recover*. The top half reflects broader cybersecurity risk management activities (*Govern*, *Identify*, and *Protect*) that support but are not part of the incident response life cycle. Continuous improvement is emphasized through the *Improvement* category within the *Identify* function, with lessons learned from all activities feeding into and enhancing all functions.

This revision aims to help organizations integrate cybersecurity incident response into their overall risk management as outlined by the NIST CSF 2.0. The structured approach enhances preparation for incident responses, reduces the occurrence and impact of incidents, and improves the efficiency and effectiveness of detection, response, and recovery efforts. Upon finalization, it will replace SP 800-61 Revision 2.

The entire model comprises several key stages. The preparation stage, as defined by NIST, precedes the incident response life cycle and involves proactive measures such as developing incident response plans, establishing communication protocols, conducting training and drills, and ensuring readiness of resources and personnel. This preparatory phase is crucial as it lays the foundation for an effective and coordinated response when incidents occur.

The NIST incident response life cycle is an important framework because it bridges the gap between cybersecurity theory and real-world operational readiness. It demonstrates how structured response processes can be integrated into daily operations to strengthen resilience. I have included it in this book because it provides a clear and practical foundation for understanding how detection, response, and recovery fit together within a larger organizational strategy.

This integrated approach aligns incident response with enterprise risk management and the broader NIST CSF 2.0 framework. It enhances readiness, reduces incident impact, and supports sustained operational resilience across both IT and OT environments.

Importance of clear communication channels

The establishment of clear communication channels is crucial for effective emergency management, especially within an **Emergency Operations Center** (**EOC**), which serves as the nerve center during crises. These channels ensure seamless communication among key stakeholders such as **Crisis Management Teams** (**CMTs**), **Public Relations** (**PR**), IT, OT, physical security, safety officers from operational units, as well as external agencies, including emergency responders, mutual aid groups, police, fire departments, and **emergency medical technicians** (**EMTs**).

Before an incident occurs, it is imperative to establish and validate these communication pathways through regular practice and exercises. This proactive approach enhances coordination and collaboration during emergencies, enabling timely decision-making and resource allocation.

The command center serves as the focal point where these communication efforts converge, facilitating the coordination of response activities across various departments and external entities. A structured communication framework ensures that critical information flows efficiently, enabling organizations to effectively manage crises, maintain operational continuity, and safeguard personnel and assets.

Emergency planning

Emergency planning involves collaboration among diverse stakeholders across multiple agencies and departments within an organization. This collaborative effort is essential for developing specific plans that can be activated swiftly and effectively during incidents. Each stakeholder brings unique expertise and responsibilities to collectively build comprehensive emergency plans, ensuring preparedness and facilitating an efficient response to crises.

For example, in August 2012, a corroded pipe in the crude unit at Chevron's Richmond refinery ruptured and released a vapor cloud that ignited (`https://www.csb.gov/chevron-richmond-refinery-fire/`). Plant operations detected the leak, the onsite fire brigade executed suppres-

sion and unit isolation, OT and control engineers supported a controlled shutdown, safety and environmental teams coordinated air monitoring and a community shelter in place, security managed site access, and public affairs and legal coordinated notifications with county health and regulators. This multi-department response, together with follow-on investigations and upgrades, shows how coordinated planning enables rapid activation when an incident occurs.

The following are the key types of plans that stakeholders commonly collaborate on:

- **Incident Response Plan (IRP)**: The IRP outlines procedures and guidelines for responding to and managing incidents to minimize their impact on operations and information assets. An IRP may include steps such as incident detection and identification, containment measures, eradication of threats, recovery of systems, and post-incident analysis. It specifies the roles and responsibilities of incident response team members and communication protocols during incidents.
- **Disaster Recovery Plan (DRP)**: The DRP primarily focuses on restoring IT infrastructure and data to ensure business continuity following a disaster or disruptive event. Given that OT systems increasingly incorporate IT components, a comprehensive DRP will also include provisions for restoring OT assets alongside traditional IT assets. A DRP may detail backup and restoration procedures, **recovery time objectives (RTOs)**, **recovery point objectives (RPOs)**, alternative work locations, and the sequence of steps to resume critical IT systems and services after a disaster such as a cyberattack or natural disaster.
- **Business Continuity Plan (BCP)**: As the name suggests, the BCP outlines strategies and processes to maintain essential business functions during and after disruptions to minimize financial loss and ensure continuity of operations. A BCP includes risk assessments, **BIAs**, recovery strategies for critical business functions, succession plans for key personnel, communication plans, and testing and maintenance procedures.
- **Facility Security Plan (FSP)**: The FSP details security measures and protocols to safeguard physical facilities, assets, and personnel from threats such as unauthorized access, theft, vandalism, and terrorism. An FSP may cover access control measures, surveillance systems, security patrols, emergency response procedures, visitor management, and incident reporting protocols tailored to the specific facility's needs. Recently, some federal agencies, including those overseeing maritime facilities, have incorporated cybersecurity considerations into FSPs. This recognizes the growing threat of cyberattacks that can disrupt operations, damage equipment, and compromise sensitive data.

- **Emergency Response Plan (ERP)**: The ERP outlines actions and protocols to respond to various emergencies, such as fires, natural disasters, chemical spills, or medical emergencies, to protect life, property, and the environment. An ERP includes evacuation procedures, emergency notification systems, assembly points, roles and responsibilities of emergency response teams, medical response plans, and coordination with external emergency services.
- **OT-specific plans**: These are plans tailored for OT systems to ensure their security, safety, and operational continuity. Here are a few examples:
- **ICS security plan**: This focuses on securing and protecting ICS from cyber threats to maintain operational reliability and safety. An ICS security plan may include risk assessments for ICS assets, network segmentation strategies, security controls for ICS components (e.g., DCS, PLCs, and SCADA systems), incident detection and response procedures, and continuous monitoring of ICS networks and devices.
- **Process Safety Management (PSM) plan**: A PSM plan addresses risks associated with hazardous processes in industrial settings to ensure that safety measures are in place to protect personnel, facilities, and the environment. A PSM plan includes **process hazard analyses (PHA)**, operating procedures for hazardous processes, maintenance procedures, emergency shutdown procedures, training requirements for personnel working with hazardous materials, and compliance with regulatory requirements such as OSHA's PSM standard.

Note

These plans, such as those for incident response, communication, and continuity, all align under an organization's broader **Business Continuity and Disaster Recovery (BCDR)** framework.

BCDR brings these plans together into one coordinated strategy to maintain and restore essential operations during and after a disruption. Each plan serves a unique purpose; incident response manages the immediate technical actions, communication ensures stakeholders are informed, and continuity focuses on keeping critical functions running—but together, they form a unified approach to organizational resilience.

Think of BCDR as a strategy rather than a single plan. It connects all these components into one cohesive structure that strengthens both preparedness and recovery.

The emergency planning outcomes are summarized in *Table 5.2*, which outlines the various plans, the responsible departments, and key stakeholders involved. Additionally, the table identifies the custodians of these plans, the department in charge, which is crucial since these plans require regular review and updates. Assigning custodians ensures ongoing maintenance, accountability, and the ability to effectively address evolving risks and operational needs.

Type of plan	**Description**	**Stakeholders**	**Department in charge**
IRP	Defines procedures for handling and mitigating incidents to minimize impact and restore operations	IT, security, operations, and management	IT security team (business)
DRP	Specifies steps to recover IT infrastructure and data following a disaster or disruptive event	IT, operations, and management	IT infrastructure team
BCP	Ensures that critical business functions continue during and after a disaster or disruption	Executives, operations, HR, and finance	Upper management
FSP	Details security measures to protect physical facilities, assets, and personnel from threats	Security, facilities management, and HR	Facility security management
ERP	Outlines actions to respond to emergencies such as fires, natural disasters, or accidents	Safety, emergency response teams, and management	Safety manager
OT-specific plans	Plans tailored for OT systems, ensuring their security and resilience	OT engineers, IT, operations, engineers, safety officers, and operations	OT manager

Table 5.2 – Emergency plans and stakeholders

IRPs, though often developed by specific departments within an organization, typically overlap and involve multiple stakeholders across various areas. *Figure 5.10* illustrates these overlaps, showing how different departments can be interconnected through shared responsibilities:

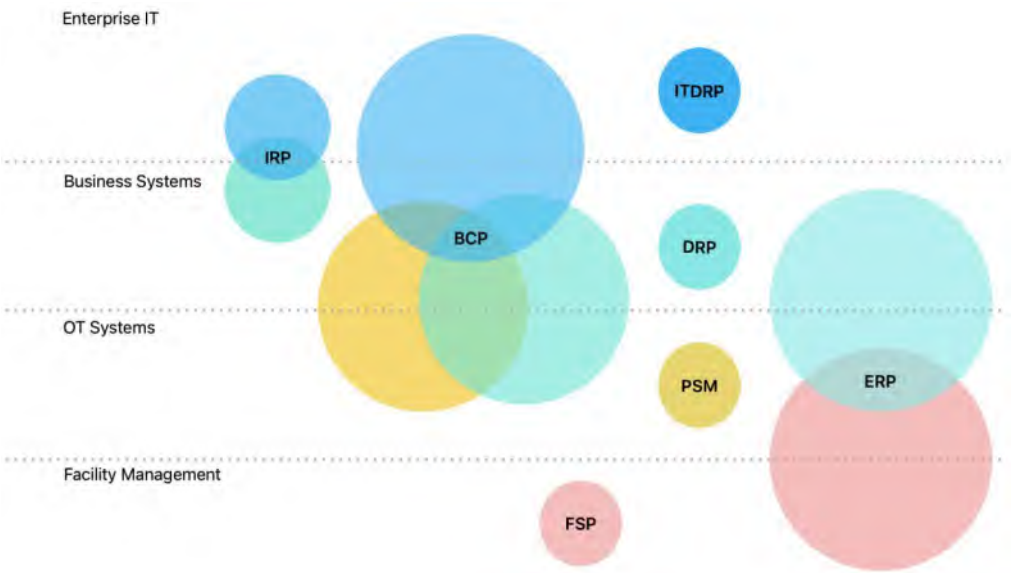


Figure 5.10 – Emergency plans that may have overlapping goals or inputs from multiple stakeholders

For instance, a BCP might include aspects of OT systems, business systems, and enterprise IT systems. Similarly, an emergency response plan could involve facility management, OT systems, and business systems.

In many organizations, stakeholders responsible for these plans come from diverse areas, as shown in *Table 5.2*. It's important to note that this distribution of responsibilities may vary depending on the organization's structure.

By involving multiple departments, these plans become more robust and comprehensive, ensuring that all relevant areas are covered. This integration enhances the organization's overall resilience and ability to respond effectively and cohesively during incidents, thereby maintaining operational continuity.

Note

These plans are developed in advance in preparation for an incident. They are ideally identified during exercises and drills, with other methods including meetings and brainstorming sessions. Another important aspect of these plans is that they are evergreen documents, requiring regular updates and periodic reviews to ensure they remain effective and relevant.

EOM is a crucial topic that we covered extensively. This section emphasized the fundamental phases common to most frameworks, providing a standard approach to managing emergencies. Additionally, we explored various emergency response plans, which help organizations ensure comprehensive coverage and address all critical aspects during incidents.

Next, let us look at how these concepts play out in a real incident. We have explored how IRPs, DRPs, BCPs, and other plans create structure and clarity during a disruption. To reinforce that, the following case study walks you through a real-world event where those plans were put to the test and shaped the city's response at every stage.

Case study: City of St. Paul, Minnesota, ransomware cyberattack

In late July 2025, the city of St. Paul, Minnesota, suffered a major ransomware attack that disrupted municipal operations, paralyzed IT systems, and forced an unprecedented deployment of the Minnesota National Guard's cyber unit (`https://gisgeography.com/st-paul-map-minnesota/`).

Saint Paul, often called St. Paul, is the state capital of Minnesota and is nestled in Ramsey County. *Figure 5.11* shows a map of the city. It's the second-most populous city in the state, with a 2024 population estimate of around 307,500 residents—holding steady from its 2020 Census count of 311,527:

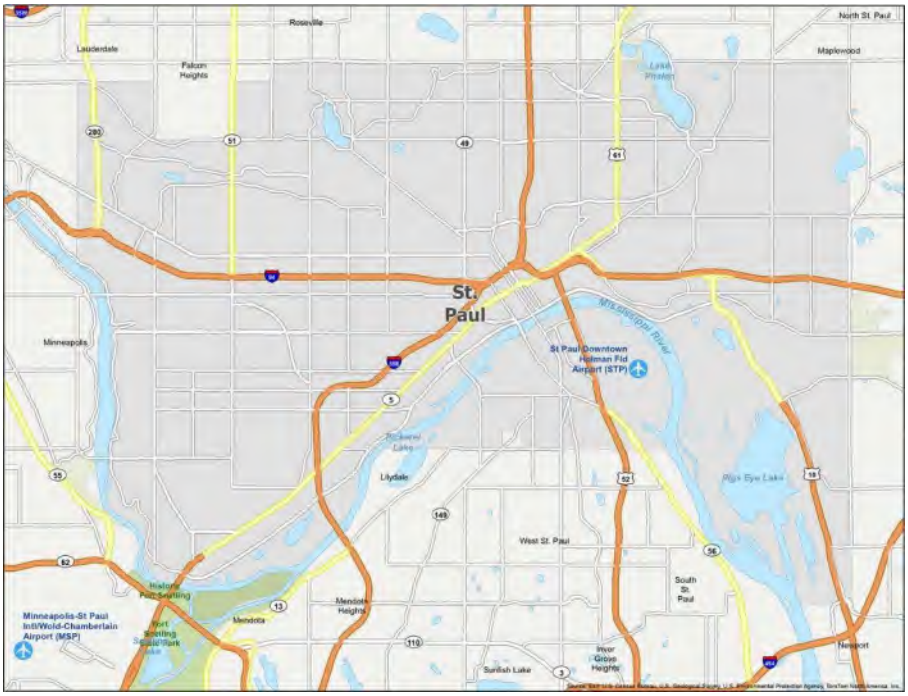


Figure 5.11 – Map showing St. Paul, MN

St. Paul is home to nearly 300,000 residents and serves as Minnesota's state capital, positioned at the heart of a much larger metropolitan region. Keeping that in mind helps put the incident into perspective; this was not a minor disruption, but one that touched on the emergency operations and essential services of a major city.

The response to this incident highlights how emergency operations navigated the crisis through the phases of preparedness, response, impact, and recovery. *Figure 5.12* shows the message posted on St. Paul's website during the incident, a clear example of effective communication (from `https://www.stpaul.gov/`):

Figure 5.12 – The warning message on St. Paul's website

The city kept its residents informed with timely updates on the response efforts, reinforcing trust and transparency during a period of uncertainty.

In this case study, we will examine the incident through the lens of the incident management life cycle, as introduced earlier in the section on management phases (see *Figure 5.8*). While, in practice, these phases often overlap and unfold simultaneously, here they are presented in a structured, staged format to make the sequence of actions and the overall flow of the response easier to understand.

The first indication came between July 25 and 27, when abnormal activity appeared across the city's IT systems. Officials saw multiple internal applications suddenly go offline, leaving staff unable to access their usual tools and files. The disruption spread quickly through departments, impacting services from online payments and licensing to public Wi-Fi. The pattern pointed to ransomware, and by July 27, the city confirmed that it was facing a coordinated, targeted attack. At that point, the EOC was activated, and all non-essential systems were shut down to contain the spread. Several mission-critical services were also isolated. *Figure 5.13* shows *Stage 1*, which covers the identification and preparedness phases:

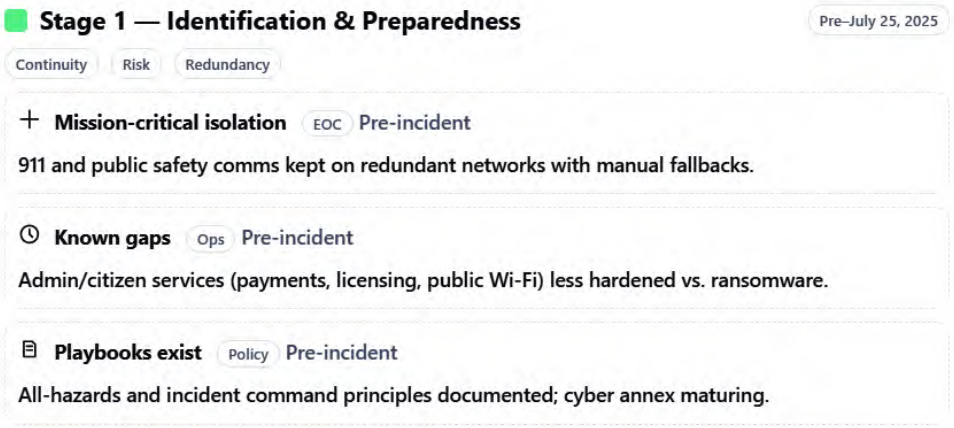


Figure 5.13 – Stage 1, covering identification and preparedness

In *Stage 1*, mission-critical emergency services were isolated from vulnerable IT systems, which is a win in this situation and highlights the key strength of their IRP. While the hardening of their IT systems and applications does not necessarily fall under the IRP, it does highlight the gaps that existed in their broader IT and administrative networks, such as licensing, billing, and vehicle laptops, leaving room for ransomware intrusion and spreading of the infection.

During *Stage 2*, the analysis and containment stage (see *Figure 5.14*), the EOC led a swift and coordinated response to the ransomware attack.

Figure 5.14 – Stage 2, covering analysis and containment

In *Stage 2*, all non-essential IT systems were immediately shut down to prevent further spread of the malware and safeguard critical networks. On July 29, guided by the EOC, the Mayor declared a local state of emergency, enabling rapid mobilization of resources and bypassing procedural delays. The Minnesota National Guard's Cyber Protection Team was then deployed to provide specialized expertise in forensic analysis, threat containment, and system recovery. At the same time, federal partners, including the FBI and DHS/CISA, integrated into the city's emergency operations framework, facilitating real-time intelligence sharing, advanced cyber threat hunting, and a unified command approach to managing the crisis.

As the incident moved from containment into the impact phase, the EOC maintained its central role in managing the crisis and sustaining operational continuity. The criminal group *Interlock* claimed responsibility for the attack and, following the city's refusal to pay the ransom, released 43 GB of stolen data online. *Figure 5.15* shows *Stage 3* of the EOC's response actions:

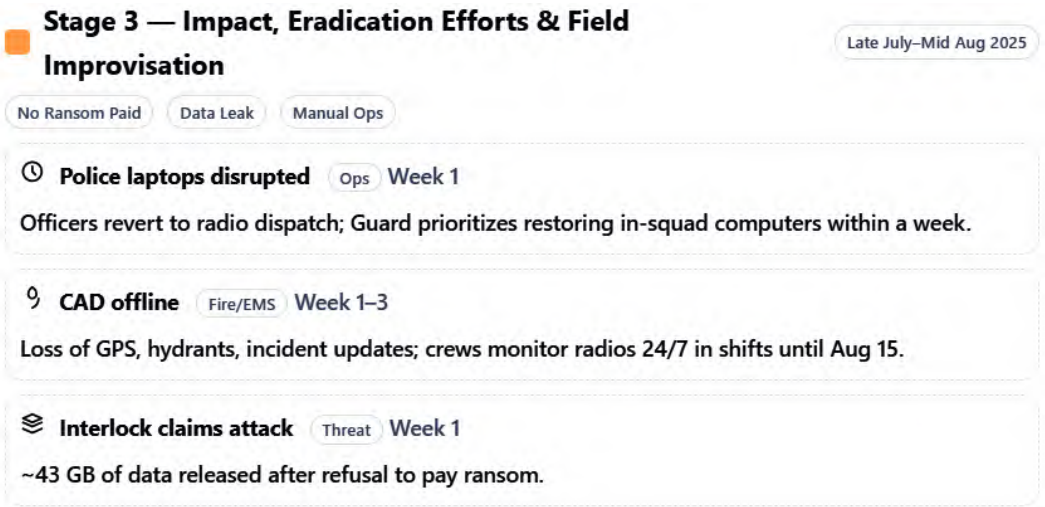


Figure 5.15 – Stage 3, covering the impact and eradication efforts

In *Stage 3*, the EOC quickly shifted its focus to managing both operational stability and public confidence. While routine city services such as bill payments and public Wi-Fi were disrupted, the systems supporting emergency services remained fully functional—a clear outcome of the EOC's prioritization of mission-critical infrastructure during the initial response phase. Departments adapted by reverting to manual workflows, ensuring that critical city functions continued despite significant IT limitations. At the same time, the EOC coordinated consistent, clear communication with the public, balancing transparency with legal and operational considerations, and reinforcing trust while managing the reputational challenges created by the data breach.

As the incident transitioned into the recovery and restoration phase, *Stage 4*, the EOC maintained a deliberate and methodical approach, recognizing that resilience is built through careful, phased restoration rather than rushed fixes. Under *Operation Secure Saint Paul*, every city employee was required to reset credentials, verify their identities, and install advanced cybersecurity tools on their devices before any systems were allowed back online. *Figure 5.16* highlights some of the key moments in this stage:

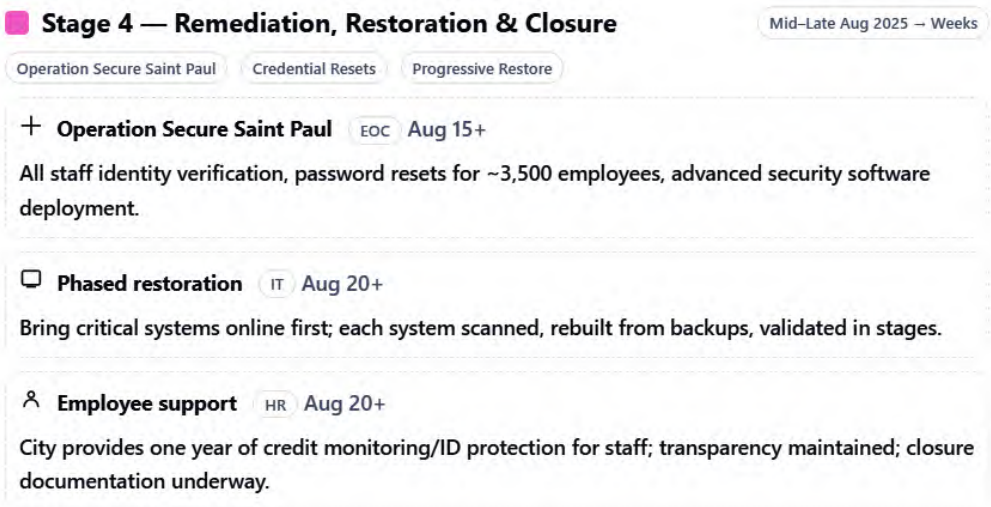


Figure 5.16 – Stage 4, covering the final phases of remediation and restoration

In *Stage 4*, guided by the EOC's prioritization framework, public safety systems, particularly police and fire laptops, were restored first to ensure uninterrupted emergency response, while other municipal platforms were gradually reintroduced after thorough testing and validation. In parallel, the EOC coordinated employee support initiatives, including a year of credit monitoring and identity theft protection for all staff whose information might have been exposed. Throughout this stage, city leadership maintained clear and transparent communication, reinforcing public trust by emphasizing that no ransom had been paid and that recovery actions were focused on building long-term security and operational resilience. As of the time of writing this book, the recovery process remains ongoing, with the city continuing to implement security enhancements and lessons learned from the incident.

The St. Paul cyberattack stands out as a strong example of how modern emergency operations frameworks adapt to evolving threats. I chose this case because it demonstrates, in real time, how an incident can escalate from an IT disruption to a full-scale emergency requiring coordinated response, clear leadership, and multi-agency collaboration.

This case study underscores that cyber incidents in critical services demand the same structured, phased response as natural disasters or physical emergencies. From this case, we learn the importance of preparedness, prioritization of life-safety systems, transparent communication, and the integration of federal, state, and local partners, which are all critical elements for building resilient operations in any CI organization.

Note

All of the sources for the St. Paul cyberattack case study were derived from the following:

Wikipedia contributors. *2025 St. Paul cyberattack*. Wikipedia. August 20, 2025: `https://en.wikipedia.org/wiki/2025_St._Paul_cyberattack`

Reuters. *FBI warns of Russian hacks targeting US critical infrastructure*. August 20, 2025: `https://www.reuters.com/world/us/fbi-warns-russian-hacks-targeting-us-critical-infrastructure-2025-08-20`

KSTP News. Richard Reeve. *St. Paul still working on a fix after July 25 cyberattack*. August 20, 2025: `https://kstp.com/kstp-news/top-news/st-paul-still-working-on-a-fix-after-july-25-cyberattack`

Exercise 1: Developing an emergency plan for your organization/facility

Question 1: What are the primary types of emergencies or crises that your facility is most susceptible to, and why?

Sample answer: Our chemical manufacturing facility is particularly vulnerable to incidents such as cyberattacks orchestrated by nation-state actors. These attacks could target our ICS, disrupting production processes and potentially leading to hazardous chemical releases or accidents. Nation-state attackers possess sophisticated capabilities to infiltrate CI, manipulate control systems, and cause physical harm or environmental damage. This makes cybersecurity incidents a top priority in our emergency plan, ensuring that we can quickly detect, contain, and recover from such threats to minimize operational disruptions and mitigate risks to public safety and environmental impact.

Question 2: How would you go about developing communication protocols within your emergency plan to ensure effective coordination and dissemination of information during an emergency?

Hint: Use *Table 5.2* to identify the stakeholders to bring to the table. While there is no communications plan in the table, you will have to develop one, which will be a subset or a section of the main emergency plan.

Sample answer: To build strong communication protocols, I would start by identifying all key internal and external stakeholders using *Table 5.2*. This includes executives, the EOC, IT and OT teams, safety officers, security, operations, vendors, local responders, and regulatory partners. From there, I would map out who needs to receive information, who provides updates, and the channels used for each stage of the incident.

The communications plan would then be drafted as a dedicated section within the main emergency plan. It would define notification procedures, escalation paths, approval workflows, and backup communication methods if primary systems fail. This includes everything from internal alerts and conference bridges to public messaging, coordination with emergency responders, and updates for leadership. The goal is to ensure that accurate information moves quickly, roles are clear, and communication remains steady and structured even when systems or personnel are under pressure.

Question 3. Identify the types of plans that your organization will need.

Hint: Use the Appendix and the template at the back to get started.

Sample answer: After reviewing our operations, critical systems, and regulatory requirements, our organization will need a combination of technical, operational, and emergency-focused plans. Together, these plans provide a full spectrum of preparedness and response capabilities. Please refer to *Table 5.2* for a summary of the plans needed, along with the purpose and responsible departments:

Exercise 2: Running a tabletop exercise/discussion to develop an emergency response plan

Objective: Guide participants through developing a tailored emergency plan for their facility—emphasizing coordination, communication, and readiness for diverse emergencies (cyber, physical, natural, or manmade).

Scenario: A Category 4 hurricane is projected to make landfall within 36 hours near your facility. Local authorities have advised voluntary evacuation. Meanwhile, your OT cybersecurity team has detected anomalies in remote sensor data, possibly due to a cyberattack exploiting weather-related network disruptions.

Note

The Saffir–Simpson Scale classifies hurricanes based on sustained wind speeds and potential damage. Understanding these categories helps emergency planners determine when to activate certain procedures, such as partial shutdowns, evacuations, or remote. Refer to *Chapter 12*, *Table 12.1*, *Categories of hurricanes - Saffir–Simpson Hurricane Wind Scale*.

Question 1: What are the primary types of emergencies your facility is most susceptible to, and why?

Action items:

- Brainstorm threats by category: cyber, physical, environmental, supply-chain, and so on
- Rank them by likelihood and impact
- Identify interdependencies

Hint: Encourage discussion on cascading effects (e.g., a power outage → loss of communications → safety systems offline).

Question 2: How would you develop communication protocols to ensure effective coordination during an emergency?

- Who must be informed (internal + external)? Reference *Table 5.2*.
- What tools will you use (phones, radios, Teams, email, emergency hotline)?
- Who communicates first and to whom?
- If primary systems fail, what's the backup (satellite, handhelds, printed contact lists)?
- Create sample notifications: *Cyber Incident Notification*, *Evacuation Order*, and so on.

Action item: Draw a quick communication flow diagram showing arrows between teams (OT, IT, ERT, HR, public affairs, etc.).

Question 3: Identify the types of plans your organization needs.

Final wrap-up: In the final stage of the exercise, participants consolidate their findings and translate discussion points into actionable improvements. The goal is to capture key insights, assign accountability, and set a timeline for follow-up activities that strengthen the organization's overall emergency readiness.

During this wrap-up session, do the following:

- Identify three key gaps discovered during the exercise, such as a lack of redundancy in communication systems, unclear procedures for ICS restoration, or missing contractor contact lists.
- Assign action owners to each identified gap to ensure accountability and progress tracking. Each responsible team member should define the next steps and report updates during future review meetings.
- Schedule a follow-up drill within the next 60 days to test communication channels, coordination flow, and the effectiveness of corrective actions implemented after this exercise.

Exercise 3: Micro tabletop exercise

This tabletop exercise has been modeled on the case of the Chevron fire (`https://www.csb.gov/chevron-richmond-refinery-fire/`).

Objective: Practice rapid, coordinated activation across departments for a refinery process leak and fire.

Example scenario: Leak detected on a crude unit line with elevated H_2S (Hydrogen Sulfide) risk, visible vapor cloud near a hot surface, and ignition within minutes.

Participants: Operations, OT and control systems, fire brigade and safety, environmental and health, security and logistics, communications and legal, and the incident commander.

This is what each group does:

- Operations declare the incident, start unit isolation and depressurization, and confirm safe states with the control room
- OT and control engineers place affected loops in manual or safe mode as needed, validate alarms and data integrity, and support isolation steps
- Fire brigade and safety deploy suppression and vapor control, establish hot, warm, and cold zones, and check PPE and gas readings
- Environmental and health begin air monitoring on and off-site, advise on shelter-in-place, and notifications
- Security and logistics control gates, guide emergency vehicles, and account for personnel
- Communications and legal coordinate internal updates, regulator notifications, and public messaging with local health authorities
- Incident command maintains a common operating picture, sets operational periods, and plans for transition to recovery

Hot wash: Capture what worked, gaps in handoffs, and action items to roll into updates of procedures, training, and mechanical integrity checks. Repeat with timed drills to build proficiency and shorten decision cycles over time. Lessons from the Richmond fire underscore corrosion management rigor, stronger process safety oversight, and clearer interagency coordination.

Summary

This chapter explored the EOC for CI organizations, emphasizing the importance of emergency management and providing insights into the organizational structure required for effective response. We discussed the roles of leadership and key experts essential to the organization. The chapter also examined several foundational plans, including the BCP, DRP, and IRP, and discussed how these documents function as evergreen documents, also referred to as a living document, that must evolve through continuous improvement.

Additionally, we analyzed the Colonial Pipeline incident to understand how incidents can progress, highlighting the distinctions between IT and OT incidents. We observed that an IT incident can sometimes impact OT systems or ICS operations, potentially leading to an OT incident. This chapter provided a comprehensive understanding of the complexities and interdependencies involved in managing cybersecurity incidents.

In *Chapter 6*, we will introduce the importance of emergency operations in organizations and cover key topics in ICS, such as roles and responsibilities, ICS functions, and the basic structure of ICS. You will gain an understanding of the significance of emergency operations and learn how to apply the ICS.

6

Introduction to the Incident Command System (ICS)

Ensuring the safety and continuity of **CI** is essential for the functioning of societies. This chapter will explore the vital role of incident response in protecting CI from disruptions, outlining foundational strategies and structures that enable organizations to manage and mitigate incidents effectively. The third pillar for CI, as shown in *Figure 6.1*, is devoted to enhancing your expertise in **Incident Command Systems (ICSs)** specifically designed for CI.

Figure 6.1 – ICS highlighted as the third pillar of incident management for CI

This segment ensures thorough preparation for implementing the FEMA-developed ICS framework and responding effectively to incidents in ICS environments. **ICS** is a key framework for managing emergencies and ensuring structured responses. We will introduce the key principles of ICS, providing an overview of its basic structure and core functions, which are essential for maintaining coordination and control during incident responses. These functions enable teams to manage resources, communication, and strategic decisions efficiently.

A significant element of ICS is the concept of **unified command** (**UC**), which allows seamless collaboration across multiple agencies and teams, ensuring a coordinated response when incidents involve different stakeholders. The chapter will also delve into the *incident facilities and locations* ICS planning process, which highlights the various locations critical to an organized response during an emergency, such as command posts, staging areas, and medical facilities.

Additionally, this chapter will offer a detailed exploration of the ICS structure, highlighting its framework and critical role in effective incident management. Gaining a solid understanding of these concepts will empower organizations to enhance their preparedness, ensuring a more resilient and coordinated response to incidents. This, in turn, helps to minimize disruptions to CI and safeguard public safety.

In this chapter, the following topics will be covered:

- The importance of incident response for CI
- Key principles of the ICS and basic ICS structure
- ICS functions
- The ICS structure
- Incident facilities and locations
- The ICS planning process – the Planning P process

The importance of incident response for CI

An incident management framework should effectively support the various phases of incident response outlined in *Chapter 5*, including identification, containment, and recovery. It serves as a structured outline defining the roles and responsibilities of key personnel, establishing a hierarchical structure for responsibilities, and organizing effective communication channels within the organization.

An effective incident management framework prevents people from being in a *"deer caught in the headlights"* situation where decision-making is paralyzed due to a lack of direction or preparedness. It serves as a blueprint that enables organizations to respond promptly to incidents, minimize their impact, and facilitate a swift return to normal operations.

A well-defined framework includes mechanisms for documenting incidents and maintaining records, which are critical for immediate use during an incident and for conducting thorough post-incident analysis and learning. It supports the execution of an organization's incident response plans, ensuring that responses are coordinated and effective across all levels of the organization.

In terms of maturity, organizations that adopt and consistently use an incident management framework tend to develop greater resilience over time. They become adept at identifying potential risks, responding proactively to incidents, and continuously improving their response strategies based on lessons learned. This iterative process enhances overall organizational readiness and strengthens their ability to manage future incidents with confidence.

In this section, you will explore the basic structure of the ICS and become familiar with the key principles of the ICS framework.

Key principles of the ICS and basic ICS structure

The ICS utilizes several core principles to guarantee its effectiveness across various incidents. These principles include standardization, flexibility, scalability, and common terminology.

Figure 6.2 highlights the four key principles of the ICS.

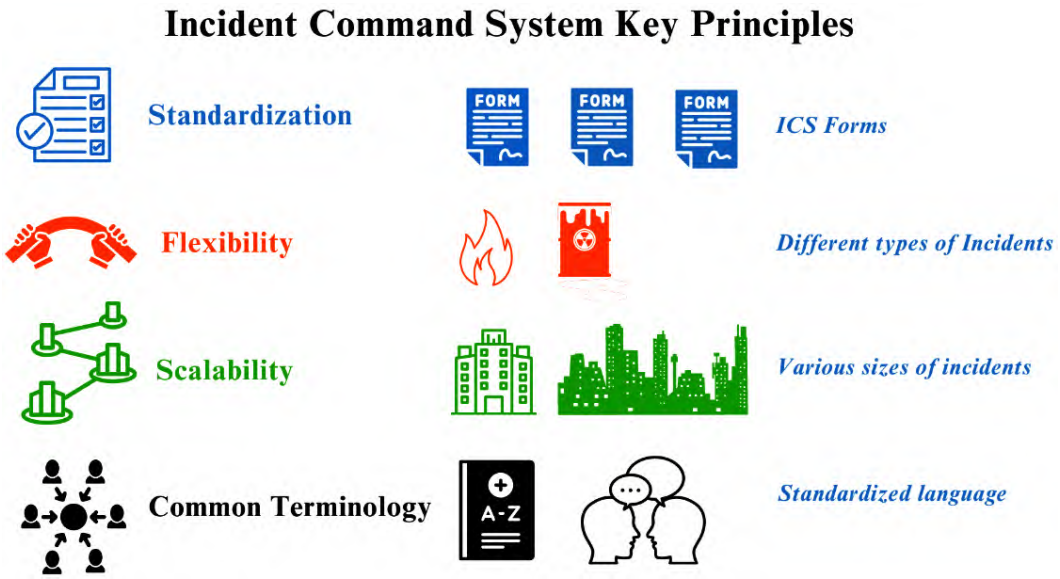


Figure 6.2 – Key principles of the ICS framework

These principles are fundamental to the successful application of an ICS in diverse emergency situations:

- **Standardization** ensures consistency in roles, responsibilities, and procedures across agencies, allowing the smooth integration of personnel and resources from different jurisdictions. This eliminates confusion and establishes a uniform approach to incident management. One of the key features is the various types of ICS forms, which are standardized templates developed by FEMA to help responders document incident objectives, actions, and resources. They create a common structure and make it easier for teams from different agencies or organizations to work together. During an incident, these forms guide communication, decision-making, and documentation in a consistent way. See the *ICS forms* section in *Chapter 12* for examples and more details.
- **Flexibility** allows the ICS to be adapted to the unique characteristics of each incident. Whether dealing with wildfires, chemical spills, or mass casualty events, the system can be tailored to meet the specific needs of the situation, ensuring optimal efficiency and response effectiveness.
- **Scalability** enables the ICS to expand or contract based on the size and complexity of the incident. This ensures that resources are neither overcommitted nor underutilized, providing the right level of support at every stage of the response.
- **Common terminology** is critical for fostering clear communication between all parties involved, from first responders to leadership teams. By using standardized language, the ICS reduces the risk of misunderstandings and errors that could compromise the response effort.

Together, these principles ensure that the ICS can be applied effectively across a wide range of incidents, promoting coordinated, efficient, and organized management, regardless of the type or scale of the emergency.

Apart from these key principles, ICS also has additional features that significantly enhance effective incident management. They are as follows:

- **Modular and scalable structure**: The ICS operates with a modular structure comprising functional sections (command, operations, planning, logistics, and finance) that can be activated or deactivated for specific incidents. This modular approach allows for a customized response that scales efficiently, deploying only necessary resources.
- **Manageable span of control**: The ICS follows the principle of a manageable span of control, where supervisors oversee a limited number of personnel (typically 3–5 subordinates). This ensures clear communication, efficient task delegation, and heightened situational awareness.

- **Unity of command**: Central to the ICS, unity of command establishes a clear chain of authority. This eliminates confusion by ensuring that a single **Incident Commander (IC)** makes critical decisions and directs the overall response effort.
- **Effective time management**: Efficient incident response hinges on effective time management. The ICS incorporates a structured approach to time management, including defined operational periods and clear task timelines within the **Incident Action Plan (IAP)**. This structure enables timely decision-making and a cohesive response.
- **Comprehensive resource management**: The ICS ensures that people, equipment, and supplies are organized and assigned in a structured way so the incident can be handled without delays or shortages. This gives teams clarity on what resources are available, who is responsible for them, and how they will be used during the response.

  Let's take a simple example. A pump seal fails at a chemical plant, causing a small leak. The IC identifies the required resources: one maintenance technician, proper PPE, a replacement seal, and spill-control materials. Logistics checks availability and assigns everything immediately. Because the resources are tracked and deployed systematically, the leak is contained quickly with minimal disruption. This demonstrates how a structured resource approach keeps the response efficient and reduces unnecessary downtime.

The ICS empowers organizations managing CI with **Industrial Automation and Control Systems (IACSs)** to effectively respond to emergencies.

To summarize, the ICS offers a consistent and adaptable structure that supports clear command, coordination, and communication during any type of incident. Now that we have covered the foundational concepts, we can shift our focus to how the ICS actually operates in practice. The next section breaks down the core ICS functions and explains how each one contributes to effective incident management.

ICS functions

In a CI organization, the ICS plays a crucial role by organizing response efforts through its key functional areas. Each section within the ICS manages different aspects of an incident, as we explored in the previous chapter regarding various stages in incident response. This section will specifically focus on operations, planning, and logistics management related to incidents:

- **Command functions**: This establishes overall objectives and priorities. For instance, during a cyberattack on a power grid, the CI organization's CEO or designated leader would take the command role, which sets goals for IT security teams and operational recovery.

- **Operations functions**: These are responsible for executing tactical response actions. In a CI organization, operations could involve teams directly managing critical systems to restore functionality. For example, during a hazardous material spill in a chemical plant, operations would oversee containment and cleanup efforts to mitigate environmental impact.
- **Planning functions**: They gather and evaluate information to develop strategic plans. In a CI organization facing a physical security breach, the planning section would analyze security camera footage, assess vulnerabilities, and formulate strategies to enhance facility protection.
- **Logistics functions**: These provide necessary resources such as equipment and personnel. They also ensure that **Emergency Response Teams (ERTs)** have access to vehicles, fuel, and communication tools needed to clear debris and restore operations in a transportation network affected by a natural disaster such as a hurricane.
- **Finance/administration functions**: These manage financial and administrative aspects. For instance, in a telecommunications company responding to a widespread service outage, finance/administration handles cost tracking for repair materials, coordinates insurance claims, and ensures regulatory compliance.

Apart from ICS functions, learning about the types of incidents is also crucial because it helps emergency management personnel understand the scale, complexity, and resources required to handle different situations effectively. This is discussed next.

Types of incidents and incident classification

Effective incident management begins with understanding how incidents are categorized and how these categories shape the response. Industrial facilities and CI organizations face a wide range of events, from small technical disruptions to complex multi-agency emergencies. Classifying incidents helps responders quickly determine severity, scale resources appropriately, and maintain control during high-pressure situations.

This section introduces the core concepts used across emergency management and industrial environments. We begin with the FEMA Incident Command System model, which defines incident complexity from Type 5 to Type 1. This model is widely used across CI sectors because it focuses on resource requirements, coordination needs, and operational impact. Following this, we introduce cybersecurity severity ratings and threat classification systems that complement the FEMA model and support cyber-physical incident response.

FEMA ICS incident types (Type 5 to Type 1)

The FEMA ICS framework categorizes incidents based on their complexity, resource demands, and the extent of coordination required. These incident types provide a common language for emergency management teams and help ensure that the response is neither over-scaled nor under-scaled.

Table 6.1 summarizes the five FEMA ICS incident types used across industrial operations and emergency response organizations; these categories help responders understand the operational scale and resource needs for managing an event:

Incident Type	Description	Example(s)
Type 5	• Handled with one or two single resources and up to six personnel. • Only the IC position is activated. • No written IAP is required. • Incident is typically contained within the first operational period, often within an hour to a few hours. • Minimal or no command and general staff positions are needed.	Minor water main break, isolated IT network outage in a single office.
Type 4	• Command staff and general staff functions are activated as needed. • Requires several resources, including a task force or strike team. • Typically limited to one operational period. • The agency administrator conducts briefings and updates the complexity analysis and delegation of authority. • No written IAP is required, but an operational briefing is documented for all incoming resources. • Operational plans with objectives and priorities are established.	Localized power outage affecting a neighbourhood, gas leak in a residential area, cyberattack on a small municipal system

Type 3	• ICS positions added to match complexity. • Some or all command and general staff positions may be activated. • May involve division/group supervisor and/or unit leader positions. • Managed by a Type 3 **Incident Management Team (IMT)**. • The incident may extend into multiple operational periods. • A written IAP may be required for each operational period.	Regional water contamination affecting multiple communities, cyberattack on a medium-sized hospital network, fire at a critical manufacturing plant impacting regional supply
Type 2	• Extends beyond local control capabilities and spans multiple operational periods. • May require regional or national resources. • Most or all command and general staff positions are filled. • Written IAP required for each operational period. • Functional units are needed and staffed. • Operations personnel usually do not exceed 200 per period; total personnel typically do not exceed 500.	Major power grid failure affecting several states, prolonged disruption of a major transportation hub, widespread flooding impacting CI in multiple regions
Type 1	• Most complex, requiring national resources. • All command and general staff positions activated. • Operations personnel often exceed 500 per period; total personnel usually exceed 1,000. Branches are established. • Agency administrator conducts briefings, updates the complexity analysis, and delegates authority. • High impact on the local jurisdiction, requiring additional administrative and support staff.	Large-scale cyberattack on national financial institutions, catastrophic earthquake affecting CI across multiple states, coordinated terrorist attacks targeting multiple CI sectors

Table 6.1 – Types of incidents

Classifying incidents from Type 5 to Type 1 helps ensure that resources are deployed at the correct scale. A Type 5 event may require a single responder, while a Type 2 or Type 1 event may demand multi-agency coordination, specialized capabilities, and extended operations. Understanding these levels prevents under-response, which may allow the incident to escalate, and avoids over-response, which diverts resources unnecessarily.

Cybersecurity severity ratings (SEVs) and threat classification

Cybersecurity incidents also need to be classified by urgency and impact. Severity levels, commonly referred to as SEVs, provide a structured way to determine how quickly an incident must be addressed and how many resources may be required. SEV ratings are widely used in security operations environments and can be applied effectively in industrial settings when aligned with operational risk.

SEV0 – critical (immediate response required)

These incidents pose an immediate threat to safety, operations, or national security. They require the highest level of response and full organizational attention.

Examples include the following:

- Ransomware affecting SCADA systems in a power grid
- Physical or cyber sabotage of refinery control networks
- Widespread disruption of water treatment operations
- Unauthorized remote access to nuclear facility safety systems

The response at this level involves immediate escalation to executive leadership and the relevant government agencies so that the situation is recognized as a high-priority threat. Containment becomes the primary focus, and all other activities are temporarily set aside to prevent further impact on safety, operations, or CI. During this stage, threat intelligence is also shared with federal partners when appropriate to support coordinated awareness and broader protective measures.

SEV1 – high priority (urgent response needed)

This refers to serious incidents that are not yet crippling but could escalate rapidly if not contained.

Examples include the following:

- Unauthorized access detected on a gas pipeline control network
- Malware on industrial control system workstations
- Denial-of-service attacks against transportation network components
- Persistent probing on substation networks

The response at this level focuses on rapid containment led by experienced cybersecurity teams who can quickly assess and control the situation. During this process, communication with regulators or sector partners may be necessary to maintain transparency and meet reporting expectations. The incident is formally logged, and analysts closely monitor the environment for any signs of escalation or additional activity that may indicate a broader threat.

SEV2 – medium priority

This refers to incidents that may pose a risk but currently have a limited operational impact.

Examples include the following:

- Phishing targeting utility staff without credential compromise
- Unusual traffic patterns inside an ICS network
- Failed brute-force attempts on refinery PLCs
- Non-disruptive malware found on an isolated system

The response at this level is assigned to analysts who carry out a focused investigation to understand the nature of the activity. Monitoring is increased to identify any signs of escalation or changes in behavior that may indicate a developing threat. Internal reporting is maintained throughout the process to ensure that key stakeholders remain aware of the situation and can respond promptly if conditions change.

SEV3 – low priority

This refers to minor security events with minimal impact.

Examples include the following:

- Repeated login failures on non-critical IT systems
- Routine vulnerability scan findings
- Low-level IDS alerts with no immediate relevance

The response at this level involves logging the event and monitoring it for any changes that might indicate an emerging issue. No immediate action is required, but the activity is still observed periodically to ensure that patterns do not shift in a way that would require additional attention or escalation.

SEV4 – informational

This refers to events with no direct security impact. It is useful only for documentation or trend analysis.

Examples include the following:

- Routine system logs
- Scheduled patch notifications
- Non-malicious configuration changes in SCADA

The response at this level is limited to logging the event for reference and reviewing it periodically to identify any trends or recurring patterns. Since these events do not pose a direct threat, no further action is required unless future analysis indicates a change in behavior or frequency.

While FEMA Incident Command System focuses on the operational scale of an incident, cybersecurity incidents also need to be classified by urgency, potential impact, and threat behavior. SEVs are widely used in SOC environments to differentiate between informational events and critical emergencies. The MITRE ATT&CK framework further supports this by mapping adversary tactics, techniques, and procedures across the attack life cycle.

The following is an explanation of how SEVs and MITRE ATT&CK complement FEMA types:

- FEMA types indicate how large or complex the response must be
- SEV ratings indicate how urgent or dangerous a cybersecurity event is
- MITRE ATT&CK describes how the attacker is operating and what stage the intrusion is in

For a unified view of how these frameworks align, including OT-specific examples, see *Table 7.1* in *Chapter 7*. This combined table maps FEMA complexity levels to SEV ratings and MITRE ATT&CK categories, creating a comprehensive classification model for cyber-physical incidents.

In industrial environments, all three perspectives are valuable. A seemingly small cyber event may still qualify as a Type 3 or Type 2 operational incident if it affects control systems, safety instrumented systems, or process stability.

With the incident types and classification models established, we can now explore the structure of the ICS itself. The following section explains the ICS roles and functions that support coordinated response and helps you identify the individuals within your organization who are best suited to take on these responsibilities during an incident.

The ICS structure

The ICS structure is designed to be flexible and scalable, adapting to incidents of any type and size, as described in *Table 6.1*. *Figure 6.3* shows the hierarchical structure of the ICS:

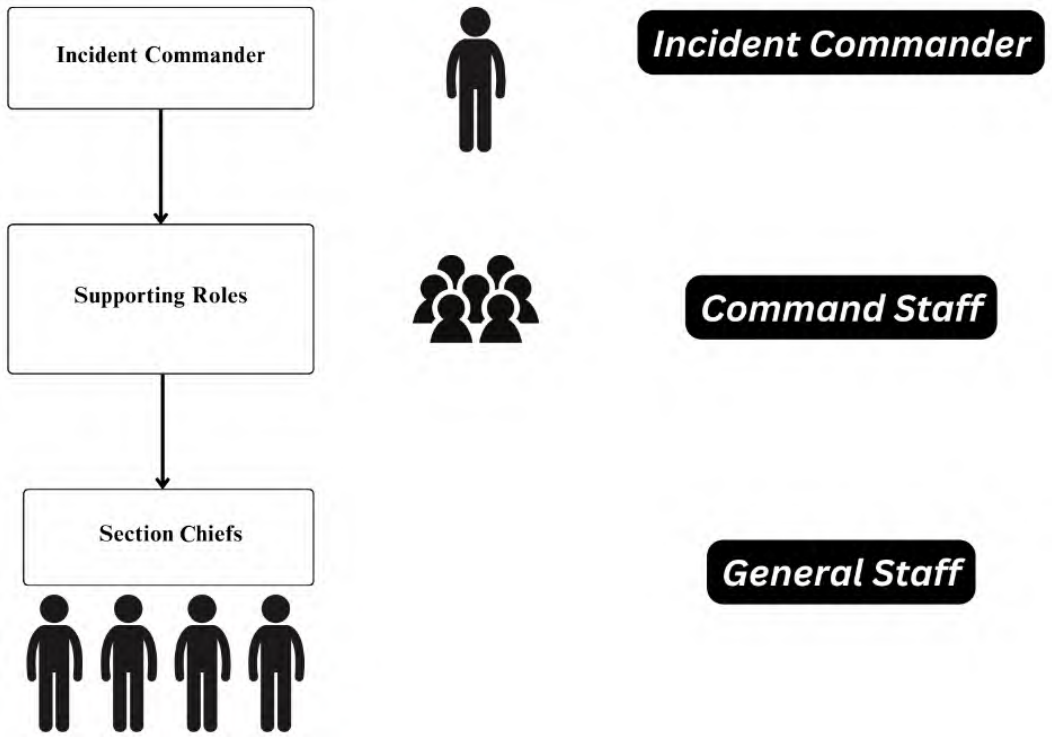


Figure 6.3 – Key positions in the ICS organizational structure

The IC oversees the entire incident management, acting as the highest authority on the scene. Supporting the IC, the **command staff** holds key positions that offer crucial support and guidance. The **general staff** consists of section chiefs responsible for managing major functional areas.

Such an ICS structure ensures clear, accurate, and timely communication across all levels of the response organization. The command function can be organized in two primary forms: a single IC and a UC. Each form has its own specific structure and application, depending on the nature and scope of the incident. Both forms are discussed in detail in the upcoming subsections, starting with the single IC.

ICS roles/responsibilities

The IC is responsible for receiving information from the command and general staff. They disseminate strategic decisions and objectives, ensuring a consistent and smooth flow of information down the chain of command, as shown in *Figure 6.4*:

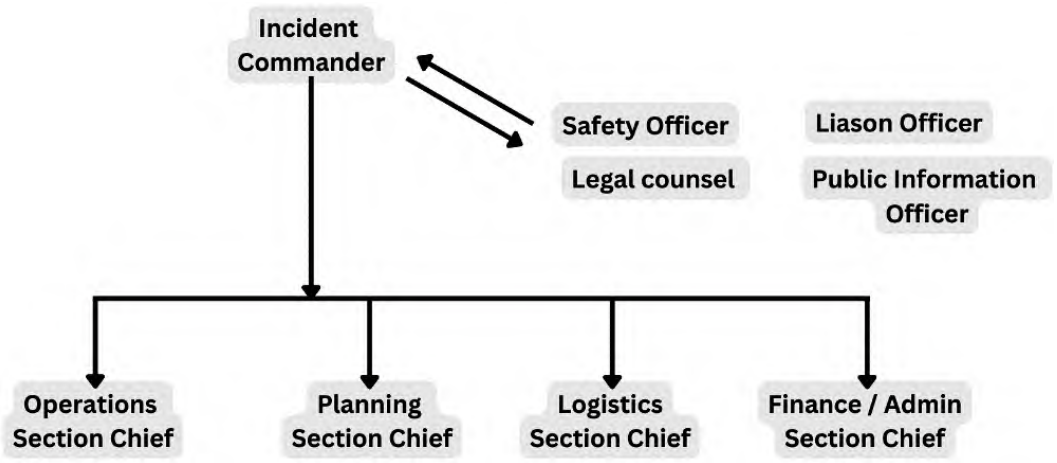


Figure 6.4 – Communication flow within the ICS structure

Smaller organizations can often manage emergencies with a single IC. This works well when incidents are limited to one site or a single operational area. As organizations grow, however, their operations become more interconnected, and incidents can quickly affect multiple domains at the same time. When this happens, the response requires deeper subject-matter expertise. This is where specialized ICs become essential. Let's take a closer look at why these specialized roles are needed and how they enhance the overall response.

Specialized incident commanders in large and complex organizations

Emergencies in large organizations often span multiple sites, departments, or even geographic regions, creating a level of complexity that goes far beyond what a single coordinator can manage. This is where specialized ICs become essential. These ICs bring domain-specific knowledge and skills to handle events such as IT outages, cybersecurity issues, supply chain disruptions, environmental incidents, or regulatory challenges. Their involvement ensures that each incident receives the right level of technical and operational attention.

Larger organizations typically have more extensive infrastructure, technology systems, and operational processes. Each of these components may require a dedicated IC who understands the specific nuances and vulnerabilities within that domain. For instance, an IT IC would focus on cybersecurity incidents, data breaches, and network disruptions, whereas an operations IC might handle production halts, equipment failures, or logistical challenges.

Regulatory compliance and legal considerations often mandate specialized expertise in managing incidents. ICs may need to ensure that response actions align with industry standards, government regulations, and organizational policies. For example, in sectors such as healthcare or finance, compliance with data protection laws or financial regulations could necessitate the involvement of specialized ICs who understand these requirements.

Additionally, larger organizations typically have more stakeholders involved in incident response. This includes executives, department heads, external partners, regulatory bodies, and possibly public relations teams. Specialized ICs are equipped to effectively communicate with these diverse stakeholders, ensuring transparency, managing expectations, and maintaining organizational reputation during crisis situations.

In summary, while smaller organizations can operate effectively with a single IC and a backup, larger organizations benefit from specialized IC roles that reflect the scale, complexity, and regulatory demands of their operations.

With the role of ICs established, we can now look at the next layer of support within the ICS structure. This is where the command staff comes in. The command staff, which includes the legal counsel, **public information officer** (**PIO**), safety officer, and liaison officer, reports directly to the IC and provides essential guidance in key functional areas.

Command staff

The PIO manages the information released to the public and media. The **legal counsel** provides legal advice and support to the IC and the command staff. The **safety officer** monitors safety information and addresses safety concerns, while the **liaison officer** facilitates the exchange of information between the IC and external agencies.

For example, during a chemical leak at an industrial facility, the PIO prepares accurate public updates, the safety officer reviews air-monitoring data to guide protective actions, the liaison officer coordinates with local fire and emergency teams, and the legal counsel advises on reporting obligations. Together, they help the IC manage the incident with clarity and compliance.

General staff

In the ICS, the **general staff** plays a critical role in managing incidents. These key individuals are responsible for overseeing essential functional areas such as operations and logistics and ensuring that response efforts are well coordinated and effective. As shown in *Figure 6.5*, the general staff comprises roles such as operations, planning, logistics, and finance/administration.

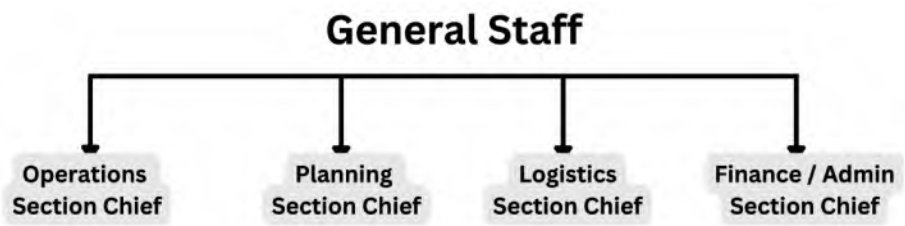


Figure 6.5 – The various roles in general staff

The general staff, composed of the operations, planning, logistics, and finance/administration section chiefs, reports directly to the IC. Each section (operations, planning, logistics, and finance/administration) is led by a section chief, as shown in *Figure 6.5*.

It's important to note that, depending on the organization's size and structure, the EOC's composition and staffing can vary significantly. In smaller organizations, the process of filling the general staff roles for all sections with dedicated individuals might be lengthy and time-consuming, depending on the organization's maturity regarding its **Emergency Operations Center (EOC)**. Therefore, existing employees may take on ICS roles in addition to their regular duties, showcasing the system's flexibility and adaptability.

In contrast, in larger organizations, the EOC may have full-time dedicated employees. Some of these employees might have prior ICS experience and be specifically recruited to be part of the EOC or the ERT. The responsibility for building an incident response team generally falls on leaders within the safety, health, and environmental departments. Consequently, many ICS roles are often filled by personnel from these departments.

Let us take a close look at each section role, identifying the main responsibilities for that role.

Operations section

The operations section provides tactical information and resource status. The operations section in the ICS is led by the **operations section chief**, who oversees all tactical operations related to managing the incident. The operations section chief ensures that strategic objectives are met by effectively utilizing available resources and coordinating with other sections.

The following table provides an overview of key roles within the operations section, outlining their responsibilities and common job titles associated with each position, helping you identify the right personnel within your organization who can take on these responsibilities:

Role	Responsibilities	Typical job titles
Operations section chief	• Oversees all operations directly applicable to the primary mission • Develops and implements tactical strategies • Directs all tactical resources • Coordinates with other section chiefs • Ensures execution of the IAP	Senior operations manager or incident manager
Division/group supervisor	• Manages a specific geographic area (division) or functional group of resources • Directs operations within their assigned area • Coordinates with the branch director	Plant supervisor or unit manager
Strike team/task force leader	• Directs a team of similar resources (strike team) or a mix of resources (task force) • Ensures resources are used effectively to accomplish assigned tasks	Team lead or shift supervisor
Single resource	• Individual personnel or equipment assigned to perform specific tasks • Mostly carries out specific assignments as directed by supervisors	Individual technicians or operators
Staging area manager	• Manages all activities within the staging area	Logistics coordinator

Malware expert	• Identifies, analyzes, and mitigates malware threats • Protects IT and OT infrastructure	Cybersecurity expert, external service provider
ICS security specialist	• Provides security for ICS infrastructure and network systems	OT security officer, OT security network expert, OT security engineer
ICS experts	• Provides specialized knowledge and expertise on the industrial control systems, SCADA and DCS, and PLC systems.	SCADA specialist, DCS engineer, process control systems engineer
Asset engineers	• Assesses, repairs, and maintains CI and assets. • Ensures functionality and safety of infrastructure.	Maintenance engineers or reliability engineers

Table 6.2 – Typical roles and positions in the operations section

Planning section

The planning section handles incident data, situation reports, and resource tracking and is a critical component of the ICS. This section develops the IAP and maintains the resource status and documentation, ensuring the comprehensive and efficient management of all planning activities. The following table outlines key roles within the planning section of the ICS, detailing their responsibilities and common job titles associated with each position. These roles are crucial for gathering and managing the information needed to plan and track the response to an incident:

Role	Responsibilities	Typical job titles
Planning section chief	• Oversees all planning activities, including the collection and analysis of incident information. • Develops and disseminates the IAP. Maintains the resource status, incident documentation, and situation status reports. • Coordinates with other section chiefs to ensure unified incident management.	Senior planner or planning manager

Resources unit leader	• Tracks all resources assigned to the incident and maintains their status. • Ensures that resource information is up to date and available for the IAP.	Resource manager or HR specialist
Situation unit leader	• Collects and analyzes incident information to develop situation status reports. • Provides a clear picture of the current incident status for planning purposes.	Operations analyst or situation analyst
Documentation unit leader	• Manages all incident-related documentation, including maintaining accurate records. • Ensures that all documents are properly filed and accessible for future reference.	Document controller or administrative officer

Table 6.3 – Typical roles and positions in the planning section

Logistics section

The logistics section in the ICS is responsible for providing facilities, services, and materials in support of the incident. The following table outlines the roles within the logistics section, their respective responsibilities, and typical personnel who play these roles in a CI organization:

Role	Responsibilities	Typical job titles
Logistics section chief	• Oversees all logistics operations, including the provision of facilities, services, and materials. • Develops and implements the logistics plan. • Coordinates with other section chiefs to ensure unified incident management.	Logistics manager or supply chain director
Communications unit leader	• Develops and implements the communications plan. • Ensures reliable communications systems and equipment. • Manages communications support for the incident.	IT manager or communications specialist
Medical unit leader	• Develops and implements medical plans. • Provides medical care and support for incident personnel. Manages medical supplies and resources.	Medical officer or occupational health specialist

Supply unit leader	• Manages the ordering, receiving, and distribution of supplies and equipment. • Ensures adequate inventory levels. • Coordinates with procurement for resource acquisition.	Supply chain manager or inventory control specialist
Facilities unit leader	• Provides and maintains incident facilities, including base camps and staging areas. • Ensures facilities are safe and operational. • Manages facility-related support services.	Facilities manager or site manager
Ground support unit leader	• Manages the transportation of personnel, supplies, and equipment. • Maintains and repairs vehicles and equipment. • Ensures safe and efficient transportation operations.	Transportation manager or fleet manager

Table 6.4 – Typical roles and positions in the logistics section

Finance/administration section

The finance/administration section in the ICS is responsible for financial management, cost analysis, and administrative support for incident management. The following table outlines the roles within the finance/administration section, their respective responsibilities, and typical personnel who play these roles in the CI organization:

Role	Responsibilities	Typical job titles
Finance/administration section chief	• Oversees all financial and administrative aspects of the incident. • Manages financial records, cost analysis, and administrative documentation. • Ensures compliance with financial policies and procedures. • Coordinates with other section chiefs to ensure unified incident management.	**Chief financial officer (CFO)** or senior finance manager
Time unit leader	• Tracks hours worked by personnel involved in the incident. • Ensures accurate timekeeping and payroll records. • Manages time records for all personnel.	Payroll manager or timekeeping specialist

Procurement unit leader	• Manages all procurement activities, including contracts and purchase orders. • Ensures compliance with procurement policies and procedures. • Coordinates the acquisition of goods and services required for the incident.	Procurement manager or supply chain manager
Compensation/ claims unit leader	• Manages claims related to personal injury and property damage. • Processes compensation claims and ensures timely resolution. • Maintains records of all claims and compensation payments.	Claims manager or compensation specialist
Cost unit leader	• Tracks and analyzes costs associated with the incident. • Develops cost estimates and projections. Ensures accurate and timely cost reporting.	Cost analyst, budget manager or an accountant
Administrative support	• Provides general administrative support to the finance/administration section. • Manages correspondence, documentation, and record keeping. • Ensures efficient administrative operations.	Administrative assistant or office manager

Table 6.5 – Typical roles and positions in the finance/administration section

Ensuring that roles are assigned early and that backups are identified is not just a precaution but a core requirement in ICS. A good example is the logistics section chief. This role oversees resource procurement, distribution, and all support services during an incident. If this position is unfilled or activated too late, the entire response can slow down. By having the logistics section chief identified in advance, along with a trained alternate, organizations ensure that equipment, supplies, personnel, and vendor support can be mobilized without delay. This level of readiness demonstrates why role clarity and depth of staffing are essential before moving into the operational functions of ICS.

We have already focused on the concept of a single IC. However, in certain situations, incidents may require the involvement of multiple ICs, which is addressed under the UC structure. In the next section, we will explore UC, an essential concept to understand as the complexity of incidents increases, especially when multiple entities or agencies are involved.

Unified command

In many organizations, especially those dealing with complex operations, the role of the IC is vital in effectively managing emergencies and ensuring a coordinated response. Traditionally, organizations designate an IC and a backup to handle site-level emergencies.

However, as organizations grow in size and complexity, more specialized personnel and tailored IC roles become necessary to address unique challenges, especially in industries such as manufacturing and other CI sectors. UC is a collaborative process that enables multiple agencies, or departments within an organization, to come together under a unified structure to manage an incident. This approach ensures that all entities involved in the incident agree upon shared objectives and strategies, fostering a coordinated and efficient response. In this structure, an IC is appointed from each responsible agency or department, and together they form a unified leadership team. The IC serves as the primary point of contact and a central source of information, ensuring streamlined communication and decision-making throughout the incident.

Unified command and incident complexity

Figure 6.6 illustrates the correlation between the complexity of an incident and the nature of the command structure.

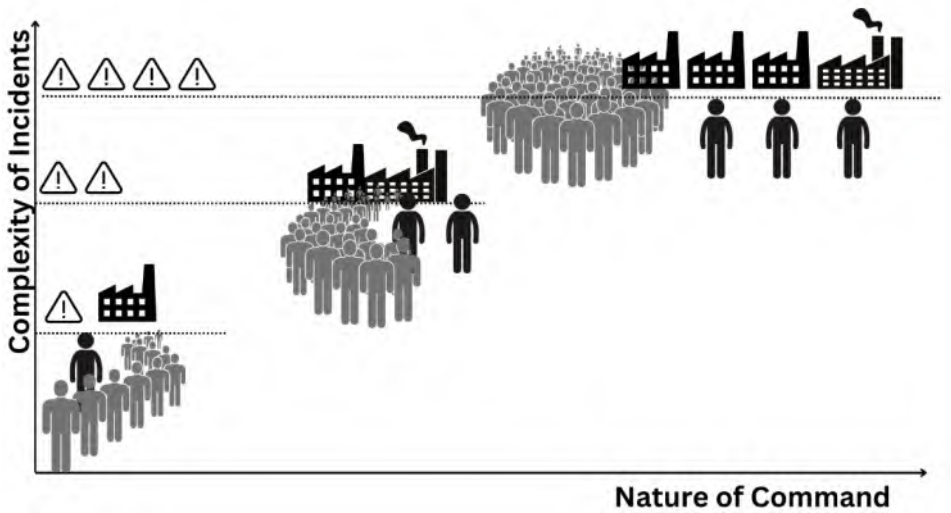


Figure 6.6 – Relationship between complexity of incident versus nature of the command

As incidents become more complex—whether due to the organization's size, the number of affected sites, or the diverse agencies involved—the need for a UC increases. Complexity may also arise from incidents involving different domains, such as environmental hazards, public safety,

or IT security. In these situations, a single IC might not have the capacity or expertise to manage every aspect, necessitating a unified structure where each IC brings their specialized knowledge to the table.

Figures 6.7 and *6.8* highlight two different approaches to incident management based on the involvement of agencies and the role of the IC.

In *Figure 6.7*, we see an incident managed by a single agency, where a single IC takes full responsibility for coordinating the response.

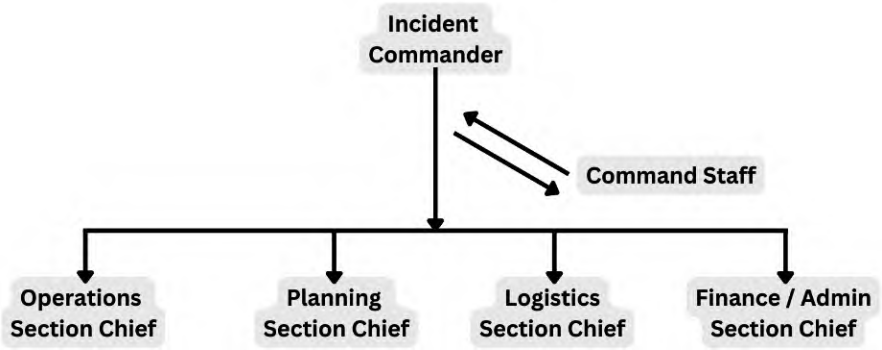


Figure 6.7 – An incident managed by a single agency, with one IC

The IC, supported by command staff (such as safety officers, PIOs, and liaison officers), ensures that all operations, logistics, and planning efforts are effectively executed within that agency's jurisdiction. The command staff provides vital support to the IC by managing specific functions, allowing the IC to focus on overall incident strategy and decision-making.

In *Figure 6.8*, the complexity increases as multiple agencies are involved in the incident response. Each agency appoints its own IC, and together they form a UC.

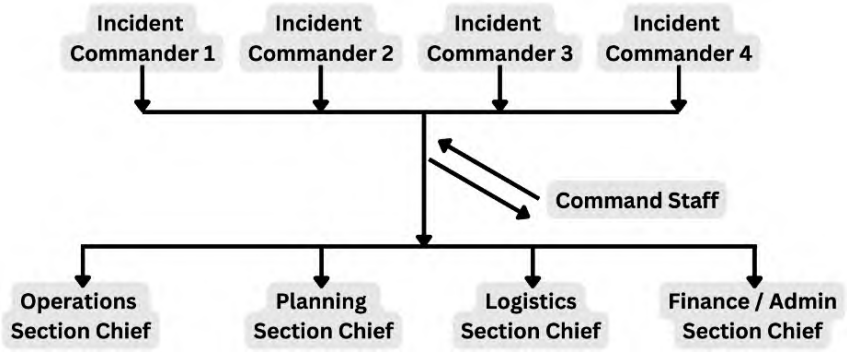


Figure 6.8 – Incident managed by multiple agencies with each of the ICs

In this structure, each IC retains authority over their respective agency's resources while collaborating with other ICs to establish shared objectives and strategies. The command staff in a UC supports not just one IC but the collective decision-making process, ensuring consistency across agencies. This allows for a more coordinated, multi-agency response, where diverse expertise and resources are effectively utilized while maintaining unified leadership.

The role of agencies in incident management

In incident management, an agency refers to any governmental body, private sector organization, or **non-governmental organization** (**NGO**) that has legal or functional responsibilities during an incident. Agencies are involved based on their jurisdiction, expertise, or available resources. Examples include local fire departments, police departments, environmental agencies, or health services, all of which may respond to different aspects of an incident.

There can be multiple agencies involved when an incident crosses various domains or jurisdictions, requiring different skill sets and resources. For example, a chemical spill at a manufacturing plant might involve the local fire department for suppression and evacuation, the environmental agency to handle hazardous materials, and the health department to manage public health concerns.

A natural disaster, such as a hurricane, might involve federal agencies such as FEMA for coordination, state agencies for resource distribution, and local agencies for on-the-ground response.

In such scenarios, each agency contributes its expertise, authority, and resources to manage the incident effectively. UC plays a key role in facilitating collaboration, ensuring that decisions are made collectively and objectives are aligned.

Unified command in the manufacturing sector

In manufacturing sectors, UC is particularly crucial when incidents affect multiple sites or involve various departments with distinct responsibilities. Incidents such as chemical spills, fires, or cyberattacks can impact several production facilities simultaneously, requiring coordination across geographically dispersed locations or between different functional departments (e.g., production, storage, or distribution).

For example, a chemical spill in a manufacturing plant that uses hazardous chemicals might require collaboration between the following:

- Facility managers from both the affected plant and nearby facilities to coordinate evacuation and shutdown procedures
- Environmental response teams to manage hazardous material containment and cleanup

- Local fire departments to oversee fire suppression and rescue operations
- IT teams to protect critical data and ensure continuity of operations

In such cases, each site or department would assign an IC to the UC structure, ensuring that all stakeholders work together under a shared framework. This allows the UC to prioritize response strategies—whether containing the chemical spill, securing nearby facilities, or minimizing production downtime—while addressing each site's unique needs in a coordinated manner.

Unified command in other CI sectors

UC is equally important in other CI sectors, such as energy, transportation, healthcare, and telecommunications, where incidents often span multiple locations or involve several organizations. Examples include the following:

- **Energy sector**: In the event of a widespread power outage or cyberattack affecting the power grid, collaboration between utility companies, government regulators, local emergency services, and cybersecurity teams is essential. UC allows these entities to work together, prioritize restoration efforts, and protect critical systems.
- **Transportation sector**: During a severe weather event affecting airports, railways, and seaports, UC ensures coordination between airport authorities, rail operators, port authorities, and national emergency services. Each entity manages its own operations, but through UC, they work toward shared goals such as ensuring passenger safety, minimizing disruptions, and restoring services.
- **Healthcare sector**: In the case of a pandemic or mass casualty event, UC may include hospital management teams, public health agencies, **emergency medical services (EMSs)**, and government authorities. They work together to allocate medical resources effectively, manage patient care across multiple sites, and implement public health measures.

In each of these CI sectors, UC prevents siloed responses by uniting stakeholders from multiple sites or agencies under a shared command structure.

Incident facilities and locations

When planning emergency responses in CI sectors, including chemical manufacturing, specific physical locations are designated to ensure safety, coordination, and effective incident management. These areas vary based on the organization's size, the materials handled, and the nature

of the facility. The following are examples of key areas, their purposes, and how they apply to various sectors, such as chemical manufacturing, energy, and healthcare:

- **Incident Command Post (ICP)**: The ICP serves as the central hub for managing incident response operations. In a chemical manufacturing plant, it should be located at a safe distance from production areas and equipped with monitoring systems to oversee all parts of the facility. In the energy sector, the ICP may be situated near power substations or control centers to manage blackouts or grid failures.
- **Staging areas**: Staging areas are critical for assembling personnel, equipment, and emergency teams. For example, in the event of a chemical spill, staging areas should be positioned upwind from the spill and away from hazardous materials. In transportation (such as airports or rail systems), staging areas might be located near hangars or depots where teams can gather and prepare for large-scale incidents such as fuel leaks or crashes.
- **Control rooms**: Control rooms are the nerve centers where operators monitor and control processes. In a chemical plant, these rooms ensure that automated systems remain operational during incidents. Similarly, in the energy sector, control rooms help manage grid stability and ensure power systems function smoothly in emergencies such as cyberattacks or blackouts.
- **Hazmat operations area**: This is a designated area specifically for handling hazardous materials. In a chemical plant, this area includes decontamination stations and waste storage for toxic chemicals. In the transportation sector, hazmat areas may be located near ports or rail yards where hazardous materials are frequently shipped or stored.
- **Camps/rest areas**: These areas provide rest spaces for personnel during prolonged incidents. In energy sectors, camps may be set up for emergency workers who need extended breaks during infrastructure repairs. In chemical facilities, these areas must be equipped with proper ventilation and PPE to ensure the safety of personnel resting between shifts.
- **Helibase and helispots**: Areas used for helicopter operations, such as transporting injured personnel or collecting hazardous samples. In a chemical plant, helispots should be located in non-contaminated zones. In healthcare facilities, helibases are often used for airlifting critical patients during emergencies like natural disasters.
- **Medical and decontamination unit**: These units provide medical assistance and decontamination for those exposed to hazardous substances. In chemical manufacturing, these units must be equipped with eyewash stations, PPE, and neutralizers for chemical exposure. In hospitals, decontamination areas are critical for dealing with patients exposed to infectious diseases or hazardous materials.

- **Safety zones/assembly points**: Designated areas where personnel and responders can safely gather during emergencies. In chemical plants, these zones are positioned away from blast or contamination zones. Similarly, in energy facilities, safety zones may be established away from electrical hazards or potential explosions at power plants.
- **Chemical storage and handling areas**: Specific areas designed for the safe storage and handling of hazardous chemicals. These areas must have containment systems to prevent leaks or spills. In transportation hubs, similar zones exist for managing dangerous cargo, such as flammable or toxic substances being shipped by air or sea.
- **Evacuation routes and muster points**: Pre-designated evacuation routes and meeting points are critical for ensuring orderly evacuation. In chemical plants, these routes must avoid high-risk areas such as reactors or chemical storage zones. In healthcare, evacuation routes must ensure patient safety and efficient movement of critical care equipment.
- **Fire suppression equipment storage**: Fire suppression systems, such as foam, dry chemicals, and water-based equipment, are stored in strategic locations. In chemical plants, this equipment is vital for controlling fires involving flammable substances. Similarly, in energy sectors, suppression systems are essential for dealing with electrical fires.
- **Incident communications center**: This center manages communication during an incident. In a chemical facility, it coordinates responses with local hazmat teams and emergency services. In energy sectors, the communications center ensures coordination between regional grids, power companies, and ERTs.
- **Containment zones/isolation areas**: These areas are set up to contain leaks or spills of hazardous substances. In chemical plants, containment zones have barriers to prevent the spread of toxic chemicals. In energy sectors, such zones can isolate oil spills or leaks in pipelines.
- **Explosion-proof zones**: These are areas designed to minimize the risk of explosions in locations where volatile chemicals or gases are used. These zones are critical in chemical plants where explosions can lead to catastrophic damage. In energy facilities, explosion-proof zones are necessary around gas turbines and storage tanks.
- Explosion-proof zones are typically installed around equipment or processes that handle volatile materials, for example, storage tanks for flammable liquids or gases or loading and unloading stations for hazardous materials. These zones help ensure that electrical devices, lighting, controls, and instrumentation in those areas are designed and installed to prevent sparks, arcs, or heat that could ignite an explosive atmosphere.

- **Air quality monitoring stations**: These stations continuously monitor air quality to detect toxic or flammable gases. In a chemical plant, monitoring stations are placed near areas where hazardous materials are processed. In transportation hubs, such stations help detect leaks from fuel storage tanks or dangerous cargo.
- **Ventilation control areas**: Ventilation control zones regulate airflow to prevent the buildup of harmful gases. In chemical manufacturing, these areas are essential to prevent vapors from accumulating in confined spaces. In healthcare facilities, ventilation controls are critical for isolating airborne pathogens.

Key considerations for maintaining emergency response areas

When designing and maintaining emergency response areas in CI sectors such as chemical manufacturing, energy, and healthcare, several important considerations must be addressed to ensure effective communication, accessibility, and upkeep. The following are some key considerations for these areas:

- **Communication**: Effective communication is essential during an emergency response, as it ensures that responders can coordinate and make informed decisions in real time.

  Each emergency area, such as the ICP, staging areas, and medical units, must be equipped with reliable communication systems such as radios or satellite phones. These devices should be compatible with other agencies or departments that might be involved, such as local fire departments or environmental agencies. In certain high-risk areas, radio frequency shielding or repeaters may be required to ensure coverage.

  In sectors such as chemical manufacturing, it is critical to have a dedicated communication line between control rooms and staging areas to ensure swift updates on any changing conditions, such as a chemical leak or fire.

  Redundant communication systems, such as backup radios or satellite phones, are important in case of power or network failures. This is especially crucial in isolated areas such as oil rigs, remote power plants, or large healthcare facilities during natural disasters.

- **Access**: Quick and safe access to key emergency response areas is vital for both personnel and equipment. Well-planned accessibility can significantly impact the efficiency of the emergency response.

ICPs, staging areas, and hazmat zones should have clear and well-maintained access roads. These roads must accommodate not only emergency vehicles, such as fire trucks, ambulances, and hazmat units, but also heavy equipment such as cranes or decontamination units. In chemical plants, it's important to establish upwind access routes to avoid contamination in the event of a chemical release.

All areas should have clearly marked pathways and signage, especially in high-risk zones such as chemical storage areas or explosion-proof zones. This ensures that personnel can quickly navigate to safety zones or assembly points. In energy facilities (e.g., power stations), having direct routes to CI, such as switchyards and transformers, is essential.

For security and safety reasons, certain areas (e.g., hazmat operations or containment zones) should have restricted access to authorized personnel only. This prevents untrained individuals from entering hazardous areas, reducing the risk of accidents. Keycard access or digital locks may be used in sectors such as healthcare and chemical manufacturing.

The ICS planning process – the Planning P process

The planning in the incident management process of ICS is a key function that sets the direction and expectations for the incident responders.

The Planning P was created to organize and structure repetitive incident management processes. It provides guidance to individuals involved in incident management for successful communication, faster incident response, and proper documentation of incident activities. It serves as a visual tool to ensure all necessary steps are followed during incident response. The **Planning P** process begins with everyone gathering together in a room. There are two main parts of the Planning P: the **stem** and the **circle**.

The stem phase involves gathering information, assessing the situation, and setting objectives for the incident, ensuring a prompt and organized response to prevent confusion. The circle represents the continuous cycle of planning, execution, and evaluation, emphasizing the need for constant assessment, feedback loops, and adjustments to ensure ongoing success and efficiency.

Both the stem and the circle are critical because they enable incident managers to move from a clear and organized initial response to an adaptable and ongoing management cycle. This structure reduces risks, promotes better communication, and ensures all aspects of the incident are addressed in real time.

By adhering to the Planning P, incident managers can ensure a thorough and organized approach to managing incidents, ultimately leading to better outcomes and enhanced safety.

Figure 6.9 shows the sequential steps of the Planning P.

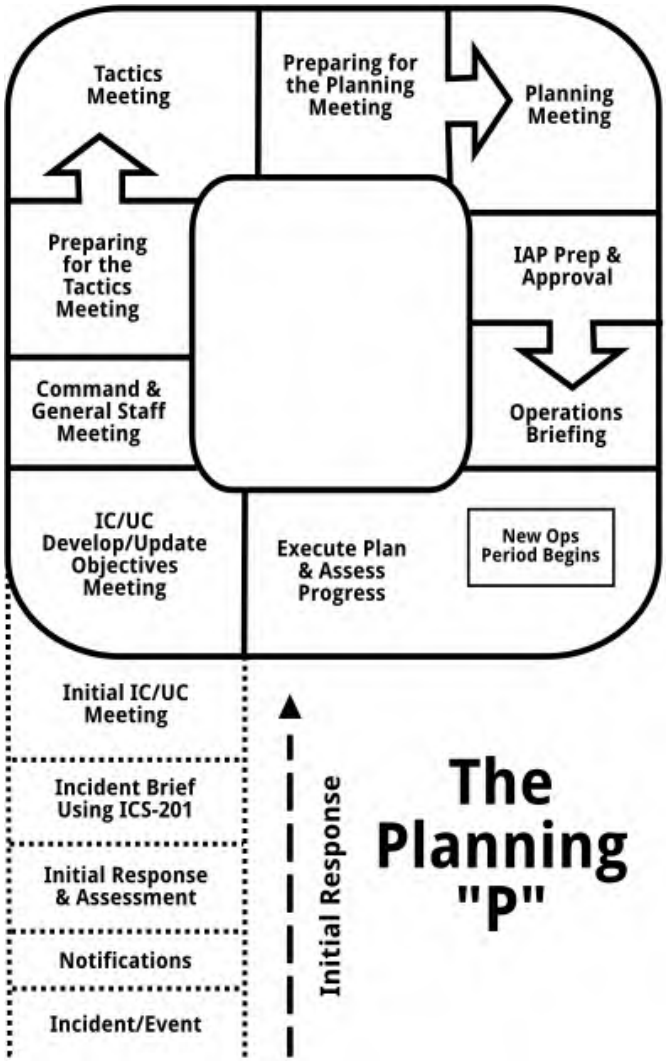


Figure 6.9 – The Planning "P" in ICS, outlining the step-by-step process for effective incident planning and management

The stem of the P consists of steps that are required at the beginning stages of an incident, while the circular part of the P shows the steps that repeat themselves until the end of an incident.

The process begins with the event that triggers the incident. As discussed in earlier chapters, an incident is any unexpected event that disrupts normal operations, requiring immediate attention. Once an incident is declared, the next phase is initiated: the notification phase.

The notification phase involves alerting relevant stakeholders, both internal and external. Depending on industry guidelines and regulatory requirements, this could include internal teams, municipal authorities, government entities, or other critical responders. The scope and timing of these notifications are dictated by pre-established protocols and sector-specific guidelines to ensure proper escalation.

Following the notifications, the initial response and assessment phase begins. This stage involves mobilizing ERTs, such as medical assistance, ambulances, firefighting units, or specialized ERTs, depending on the nature of the incident. These immediate actions are generally outlined in the organization's incident response plan, ensuring that all personnel involved are familiar with the steps to be taken.

While the initial response is underway, an incident briefing is conducted. During this briefing, operational personnel provide an overview of the current conditions, including the status of the incident, the impacted areas, and any personnel involved. This step is crucial for ensuring that everyone is on the same page and has up-to-date information before the next phase begins.

The final phase of the stem occurs when the IC assumes control of the incident management process. At this point, the situation may require coordination with multiple entities or agencies. If this is the case, a UC meeting may be convened to ensure cohesive decision-making across all involved parties. Alternatively, if the response remains within one organization, an IC meeting is held to plan the next steps. This meeting feeds into the broader cycle of the Planning P, which guides the continued response and resolution of the incident.

Ensuring an effective Planning P involves following a strict schedule, ensuring punctuality at meetings, and adhering to the agenda established by the planning section chief.

Scenario analysis — initial steps for containing a chemical spill

Consider a scenario involving a chemical spill at a small specialty chemical company that manufactures resin-based products. On a routine weekday morning, an operator working in the blending area notices a strong chemical odor and sees liquid spreading under a storage drum. At the same time, a fixed gas detector in that zone triggers an alarm that confirms that a spill has occurred. The operator steps away from the area, avoids the vapors, and pulls the nearest emergency alarm to notify the control room. This marks the beginning of the incident.

Immediately after the alarm, notifications go out through the plant's alerting system. Text messages, emails, and overhead announcements inform supervisors, responders, and the ICS team that a chemical spill has been detected in the west processing bay. Personnel begin moving into their roles and the first layer of response starts.

Figure 6.10 presents the details of the initial actions taken.

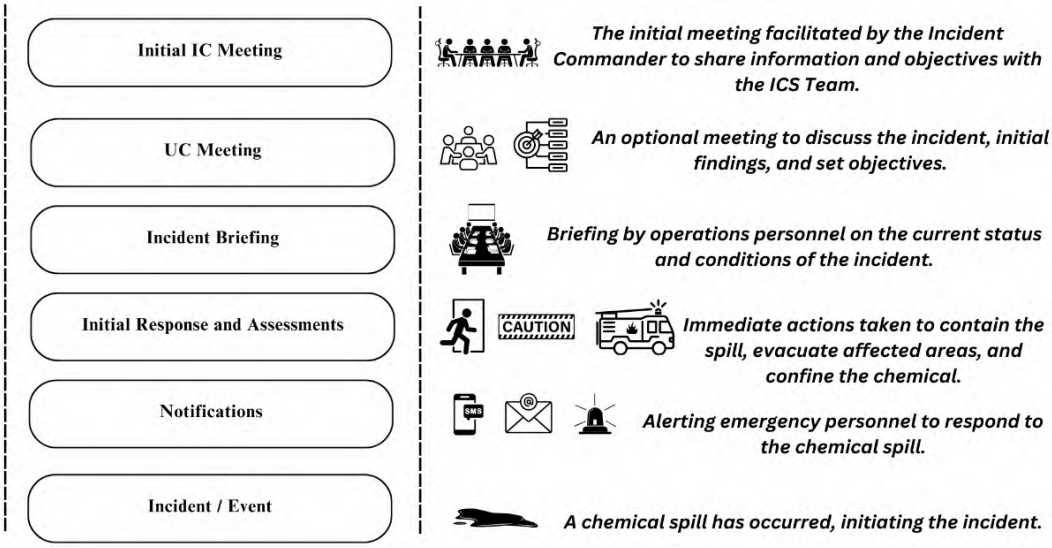


Figure 6.10 – Details of the initial steps, the stem, for a chemical spill

Initial response and on-scene actions

Before the IC begins formal coordination, the first responders on shift perform the usual early actions that take place in most chemical spill situations. They secure the affected area and stop nearby operations. Responders put on the appropriate personal protective equipment based on the safety data sheet for the chemical. This usually includes gloves, goggles, and protective coveralls, along with respiratory protection if required.

Responders then try to stop the source if it is safe to do so. They may upright the drum, close a leaking valve, or place the container into an overpack. Spill kits that are staged in the processing bays are quickly opened. Absorbent socks are placed around the spill to keep the chemical from reaching drains or walkways. Absorbent pads, sand, or vermiculite are used to keep the material from spreading. Once the spill is contained, responders gather the soaked absorbents, place them into proper waste containers, and label the waste. The area is then decontaminated using the cleaning method recommended for that specific chemical.

Progression through the Planning P stem

As the situation becomes more stable, operations personnel who work directly with the chemical provide an initial briefing to the IC. This briefing includes the type of chemical involved, the

approximate quantity released, the status of the source, any potential exposures, and any impact on surrounding equipment or personnel. This initial briefing helps the IC understand what has happened and what risks may still be present.

A UC meeting may then take place if the facility uses this structure. This meeting can involve safety, environmental, facilities engineering, and, if needed, local fire and rescue teams. The goal is to ensure that everyone has the same understanding of the event, the hazards, and the immediate objectives.

The final step in the stem of the Planning P is the initial IC meeting with the ICS team, the command staff, and the general staff. The IC brings together all the information gathered so far, confirms assignments, outlines priorities, and prepares the team to move into the main part of the Planning P cycle. This begins the development of the IAP and the operational response for the remainder of the incident.

Note

In general, chemical spill response focuses on life safety first, followed by source control and containment. Securing the area, using proper personal protective equipment, stopping the leak when safe, placing barriers to keep the chemical away from drains, cleaning and decontaminating the affected area, and properly disposing of all waste are the core actions that most organizations follow. These steps are supported by trained personnel, accessible spill kits, and a clear spill response plan, which together ensure a safe and effective response.

Operational periods

An **operational period** is a defined timeframe within which specific incident management actions and objectives are planned and executed. The duration of an operational period can vary, but it is typically 12 to 24 hours long. The operational period is crucial for structuring the response efforts, ensuring that all team members are working toward clear and achievable objectives within a set timeframe. It also allows for regular assessment and adaptation of the IAP based on changing conditions and new information.

Figure 6.11 illustrates a representation of the four operational periods for the chemical spill incident from the previous example, each lasting 14 hours.

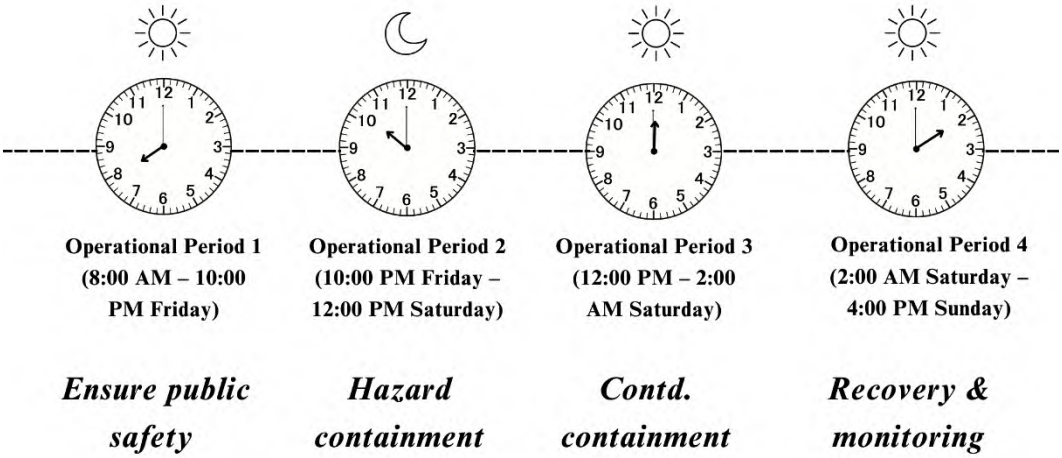


Figure 6.11 – Breakdown of the four operational periods in the ICS for a chemical spill

The first operational period begins at 8:00 A.M. on Friday, with the primary objective of ensuring public safety. During this phase, the focus is on notifying stakeholders, evacuating personnel, securing the affected area, and communicating safety measures to the public.

In the second operational period, starting at 10:00 P.M. on Friday, the focus shifts to hazard containment. The incident response team works to fully control and contain the leak, while specialists conduct environmental monitoring to assess the impact. Public updates continue to be issued as the containment efforts progress.

The third operational period, beginning at 12:00 P.M. on Saturday, concentrates on continued cleanup, medical support for exposed personnel, and a reassessment of containment measures. During this phase, the response team ensures that any hazardous materials are properly removed and that medical care is provided to anyone affected.

Finally, the fourth operational period, starting at 2:00 A.M. on Sunday, focuses on final containment, debriefing, demobilization of resources, and the beginning of recovery and monitoring efforts. By the end of this phase, the situation is fully under control, and the recovery process is initiated, ensuring long-term safety and environmental stability.

The circular process

The Planning P circle outlines the ongoing processes in incident management until the incident is resolved; it emphasizes the key processes of planning, execution, and reassessment.

Preparation meetings are held at various stages to ensure readiness and coordination among internal teams, external agencies, and other stakeholders. These meetings serve to plan, organize, and strategize before key operational periods or critical decision points during an incident. The IC leads these meetings, with the aim of ensuring that the response teams are fully prepared to execute the next phase of operations.

During the various sessions, the IC and key personnel review the current status of the incident, analyze available data, and plan for upcoming operational periods. These meetings are not only a time for decision-making but also for refining the IAP based on evolving needs and challenges by continuously revisiting the objectives and adjusting strategies. The following are the main meetings that take place in the circle part of the Planning P:

- **Tactics meeting**: The tactics meeting is a brief, focused session typically lasting 10 to 15 minutes, where the operations section chief presents the draft tactical plan to key IMT members. This meeting ensures alignment on proposed tactics for the upcoming operational period, discussing specific hazards and mitigation strategies. It serves as an informal check to ensure operational feasibility and safety.
- **Planning meeting**: The planning meeting involves the entire IMT and focuses on strategic planning. During this meeting, the IAP is developed or updated based on the latest information and input from various team members. It sets clear objectives, assigns responsibilities, and outlines operational strategies for achieving incident goals.
- **IAP preparation and approval**: Following the planning meeting, the IAP is prepared, detailing operational objectives, tactics, and resource allocations for the next operational period. This document undergoes review and approval by the IC and other command staff to ensure alignment with incident priorities and safety protocols.
- **Operations briefing**: The operations briefing precedes each operational period and involves briefing operational personnel on the finalized IAP. Led by the operations section chief, this briefing ensures that all personnel understand their roles, objectives, and safety considerations before executing their assigned tasks.
- **New operational period begins**: With the IAP approved and briefed, a new operational period begins. Operations are initiated based on the outlined strategies and objectives, with personnel deployed according to their assignments. This marks the start of focused efforts to achieve incident management goals within the defined timeframe.

- **Execution of the IAP and assessment of progress**: Throughout the operational period, the IAP is executed, with teams implementing planned tactics and actions to manage the incident effectively. Continuous monitoring and assessment of progress against established objectives are conducted to gauge effectiveness, adapt strategies as necessary, and ensure safety and operational efficiency.

To put this into perspective, consider the chemical spill example discussed earlier. After the initial stabilization took place during the stem of the Planning P, the circular process carried the response through each operational period. During the tactics meeting, the operations section chief reviewed containment boundaries, changes in the spill area, air monitoring results, and the protective equipment required for entry teams. In the planning meeting that followed, the wider team agreed on the next set of objectives, such as expanding monitoring zones, coordinating with the environmental contractor for product recovery, and adjusting staffing based on updated conditions.

These decisions were formalized in the IAP, and the operations briefing ensured every responder understood their assignments, the expected outcomes, and any safety concerns. As the new operational period began, teams carried out the plan while supervisors monitored the weather, chemical readings, and progress on containment. At the end of the period, the IC reviewed the results, refined the objectives, and set the direction for the next cycle. This example shows how the circular part of the Planning P keeps the response effort organized, informed, and able to adapt until the incident is fully resolved.

As the response progresses, the IC and the ICS team begin organizing information, documenting decisions, and tracking resources. This is where ICS forms become essential. They provide a structured way to record what is happening, what decisions are being made, who is assigned to each task, and what the next operational period will require. In an incident such as the chemical spill described, these forms can help bring clarity, support coordination among different groups, and ensure that every action is captured in a consistent and traceable format.

The next section discusses the ICS forms that are most commonly used during incidents and explains how they support a smooth and well-managed response.

ICS forms

In incident management, ICS forms are indispensable for organizing information, coordinating efforts, and documenting actions from the onset to the resolution of incidents. With a wide array of forms, exceeding as many as 30 options, organizations typically begin by logging incident

particulars in a unified document featuring timelines and timestamps. Subsequently, this data is methodically transferred to specific ICS forms tailored for comprehensive documentation. Essential examples of forms used during incident management are listed here:

ICS 201 – Incident Briefing: This form is used to provide a comprehensive snapshot of the incident status and current actions. It details incident objectives, operational periods, resource assignments, and a summary of the incident situation. This form is essential for briefing ICs and other key personnel, ensuring everyone is informed and aligned with the incident management strategy.

ICS 213 RR – Resource Request: This form is used to request additional resources needed to support incident operations. It includes resource type, quantity, location, and required arrival time. The form facilitates efficient resource management by ensuring the timely and appropriate allocation of resources based on incident needs.

ICS 215 – Operational Planning Worksheet: This form is used to develop and document the IAP. It details operational objectives, tactics, resource assignments, and safety considerations for each operational period. ICS 215 ensures that all aspects of the response are systematically planned and communicated to the IMT.

ICS 203 – Organization Assignment List: This form documents the organizational structure of the IMT, including roles, responsibilities, and reporting relationships. It ensures clarity in command and control, facilitating effective coordination and communication among team members.

Note

For a full collection of all ICS forms and their descriptions, refer to the FEMA resources listed at the end of this chapter. You can also review *Chapter 12* for additional detail on each form and how it is used, along with links to download and use the forms.

The next section looks at how to conduct effective briefings and meetings and why they are essential to the planning process.

Effective briefing and meetings

Briefings and meetings are essential elements of this planning process. However, there are key differences between the goals of a briefing and those of a meeting. The purpose of a briefing is to pass along specific information about the incident. In contrast, meetings are held during the planning cycle to process information and make decisions. Effective briefings and meetings are key to the success of incident management. Without accurate, timely information exchange, it's impossible to manage an incident safely, effectively, and smoothly.

Key features of briefings

Some salient features of briefings are as follows:

- Briefings are designed to pass along specific information about the incident
- Briefings ensure that the information shared is current and relevant
- They communicate clearly and concisely to avoid misunderstandings
- They identify and develop a format and consistently follow it to ensure all necessary information is covered

Conducting an effective briefing

There are a number of things that can be done to ensure that effective briefings are conducted. Before the briefing, gather all relevant information, such as the latest incident reports and resource availability. Encourage questions and provide necessary clarifications, such as explaining specific terminology or procedures, to ensure everyone is on the same page. Additionally, ensure that actions or tasks resulting from the briefing, such as deploying specific teams to critical areas, are tracked and completed for effective incident management. Further, clear identification of the speaker and the context ensures that participants understand the source of the information and their role in addressing the situation.

Let's look at an example script. In this scenario, the person conducting the briefing is likely the IC or a lead operations officer. Their role is to provide a clear update on the situation, explain the challenges, and ensure that every participant is aligned on the next steps to manage the incident. Here is an example script: "*Before we dive into our first incident management meeting, I want to provide a detailed overview of the current situation. As of 0600 hours, we have experienced a significant disruption in our control room workstations. Operators and manufacturing processes are impacted, leading to operational delays and potential safety concerns.*"

Key features of meetings

Some key elements of meetings in an ICS are as follows:

- Meetings are held to process information and make decisions based on that information.
- Meetings are critical for making timely and effective decisions.
- A clear agenda should be followed to keep the meeting focused and efficient.
- It should be ensured that all relevant parties are involved in the meeting.

Recipe for a successful meeting

A successful meeting should have clear goals and objectives, with everyone understanding the purpose of the discussion and what decisions need to be made. Information must be exchanged accurately and comprehensively, and each participant should provide updates that are relevant to their responsibilities. Decisions taken during the meeting should lead to clear, actionable outcomes that guide the next steps in the response. Meetings should also start and end on time so that the response effort maintains momentum and teams can move to their next assignments without unnecessary delays.

For the spill scenario that we discussed in the previous section, this approach becomes very practical. During the meeting, team leads would share updates on containment boundaries, the latest air monitoring results, product behavior, and the readiness of response equipment. The objectives would be clear, such as expanding monitoring zones or determining whether additional protective measures are needed for entry teams. Decisions would translate into specific actions, including task assignments, coordination with the environmental contractor, or adjustments to isolation distances. By keeping the meeting focused, structured, and timely, the response team remains aligned and able to execute the plan effectively.

Exercise 1 – ICS structure and role assignments

1. **Objective**: Identify the command staff and general staff roles within the ICS for a simulated incident in your organization.

   Instructions: Based on the roles described in the chapter, distinguish between command staff and General Staff positions that would be crucial in managing an incident such as a chemical spill or another relevant scenario in your organization. Provide examples of responsibilities for each role.

   Example: Consider a ransomware attack affecting the business network in a manufacturing facility, with signs that the malware is attempting to move toward OT systems. Who would fill the roles of IC, PIOs, safety officer, and liaison officer? Describe their specific responsibilities in coordinating the response.

Role	Personnel	Responsibilities
Incident commander	Maria S.	Responsible for the overall management of the cyber incident. Oversees containment strategies in the business network, ensures rapid isolation of affected systems, approves the protection of OT assets, and sets clear objectives for the response.

Public information officer	Jamal M.	Manages all internal and external communications, including updates to employees, partners, and the public. Ensures accuracy in all messages, especially concerning service disruptions and potential impacts. Keeps leadership informed of communication needs.
Safety officer	Alejandro R.	Monitors safety considerations related to system shutdowns and manual workarounds. Ensures that any shift to manual operations in OT does not create hazards and verifies that cybersecurity containment actions do not introduce new physical risks.
Liaison officer	Fatima K.	Coordinates with external partners, including the incident response vendor, threat intelligence partners, the FBI, and state cyber teams. Ensures seamless communication across all involved agencies.
Operations section chief (OSC)	Diego L.	Leads the tactical response effort. Oversees IT and OT cyber teams working to isolate the malware, remove infected systems from the network, monitor lateral movement, and protect critical processes.
Planning section chief (PSC)	Emily S.	Collects and analyzes threat indicators, logs, and forensic data. Develops the IAP for each operational period and provides projections on how the incident may evolve. Maintains full documentation of all incident actions.
Logistics section chief (LSC)	Raj P.	Manages resources such as laptops, clean network segments, forensics tools, backup systems, and workspace. Ensures cyber teams have all the support needed to continue operations safely.
Finance/ administration section chief (FSC/ASC)	Mei C.	Tracks incident-related costs, including vendor support, hardware replacements, legal consultation, and employee overtime. Manages contracts with external response partners.

Table 6.6 – Sample staff identification

Exercise 2 – develop objectives for managing an incident

Objective: Develop objectives for managing an incident, tailored to your organization's needs and priorities.

Instructions: Using the principles outlined in *Key Principles of the ICS and Basic ICS Structure* section of the chapter, outline objectives that would guide your organization's response to a ransomware incident that begins in the business network and threatens to spread to OT systems. Focus on objectives that protect people, processes, and CI.

Example: Objectives for managing a ransomware incident include identifying and isolating all infected systems in the business network, rapidly preventing the malware from reaching OT assets, protecting production systems by segmenting vulnerable pathways, restoring essential business functions from verified backups, and conducting continuous monitoring to detect additional threats. Clear priorities also include maintaining safe OT operations, communicating status updates to all employees, and coordinating with external agencies for threat intelligence and investigative support.

Exercise 3 – create an operational plan

Objective: Create an operational period plan for responding to a ransomware attack.

Instructions: Utilizing the structure of operational periods discussed in the chapter, design a plan for the initial operational period of an incident response. Include specific activities, resource allocations, and safety considerations that would be essential for managing the incident effectively.

Example: Operational Period 1 Plan: Initial Response to Ransomware Incident:

1. **Establish command post**: Set up a virtual or physical command post supported by secure communication tools. Confirm the availability of backup communications in case primary systems are affected.
2. **Initial assessment**: Deploy the IT security team to identify compromised systems, trace the entry point, and perform log reviews. Determine the extent of lateral movement within the business network and evaluate any attempted access to OT systems.
3. **Network segmentation and isolation**: Immediately isolate affected systems. Disable VPN access temporarily if required. Validate the integrity of jump servers, firewalls, and data diodes to ensure no unauthorized pathway exists between business and OT networks.
4. **Deploy cyber response teams**: Assign cyber analysts to containment tasks, forensic review, log collection, and malware analysis. Ensure OT engineers review ICS equipment for abnormal traffic or failed authentication attempts.

5. **Coordinate with external authorities**: Establish communication with the organization's incident response vendor and notify relevant agencies, such as the FBI or state cyber units. Share details, seek guidance, and request assistance when needed.
6. **Communication protocols**: Implement structured communication using designated platforms. Confirm that all staff know how to report suspicious activity. Prepare internal updates for leadership and employees.
7. **Incident documentation**: Assign personnel to maintain ICS form 214 –Activity Logs documenting all actions, findings, and decisions. Ensure that system snapshots and forensic images are preserved for later investigation.
8. **Ongoing safety monitoring**: If manual operations are required in the OT environment, verify that alternate procedures are safe and properly supervised. Review risks related to equipment shutdowns, manual overrides, and environmental conditions.

Summary

This chapter provided a comprehensive overview of the ICS, detailing its structure and the management principles crucial for effective response and coordination. It highlighted organizational operations, planning methodologies, and the utilization of standard forms essential for managing incidents of various scales and complexities. Emphasizing clarity in roles and responsibilities, the chapter stressed the importance of systematic communication, resource management, and ongoing evaluation in achieving incident objectives. From initial response through to recovery phases, the ICS framework ensures cohesive efforts, informed decision-making, and adaptable strategies, facilitating a methodical approach to incident management. Additionally, the chapter distinguished between briefings and meetings, preparing you for upcoming chapters focused on setting up, conducting training exercises, and managing organizational readiness, which is essential for facilitating effective incident response in your organization.

In *Chapter 7*, we will explore several common frameworks, examining their strengths and weaknesses in detail. We will also discuss how each framework addresses specific needs and requirements across various industry sectors, providing a deeper understanding of how these tools are applied in real-world scenarios. This will help you assess and choose the right framework for your organization's unique challenges.

Further reading

- ICS forms: `https://training.fema.gov/icsresource/icsforms.aspx`
- Resource center for forms: `https://training.fema.gov/emiweb/is/icsresource/icsforms/`
- *Incident Action Planning Process*: `https://www.fema.gov/sites/default/files/documents/fema_incident-action-planning-process.pdf`
- NIST – *Preparing Your Organization for Ransomware Attacks*: `https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Tips_for_Preparing_for_Ransomware_Attacks.pdf`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

7

Practical Considerations for Incident Management in IACS

Incident management only becomes meaningful when it can be applied to real situations inside an industrial environment. In the previous chapter, we looked at how the **Incident Command System** (**ICS**) depends on the organization's management structure, planning process, resource availability, and the level of expertise within the response teams. In this chapter, we will take that foundation and move it into the world of industrial automation and control systems.

As we have already established, **industrial automation and control systems** (**IACSs**) and **operational technology** (**OT**) do not behave like traditional IT networks. They are built for safety, continuity, and deterministic behavior. When something goes wrong in an IACS environment, the goal is not only to investigate the cyber incident but also to maintain safe operations and protect equipment, people, and the environment. This chapter will focus on the specific considerations that make incident handling in IACSs different and why a tailored approach is necessary.

We will walk you through the complete process of incident handling, from the moment an event is detected to the point where systems are safely restored. You will learn how monitoring tools work in an industrial setting, how **security information and event management** (**SIEM**) systems can be adapted for OT networks, and how to use industrial sensors for vulnerability monitoring. Communication in OT environments is another important topic because response teams must often coordinate through controlled channels, especially when safety or process integrity is at risk.

To help reinforce these concepts, this chapter includes optional exercises. These activities will guide you through simulated industrial environments or sample datasets. They are not required, but they provide a practical way to build confidence in analyzing events, collecting forensic information, and restoring systems in an IACS environment.

In this chapter, we will focus on the following areas:

- Incident response for IACS
- Threat intelligence and monitoring in IACS environments
- IACS-specific incident response planning
- Forensic data collection and incident documentation

Incident response for IACS

Incident response for IACS is fundamentally different from traditional IT incident response. Although an **incident response plan** (**IRP**) is an organization-wide function that involves IT, OT, safety, emergency response, and business continuity, the way incidents unfold inside an IACS environment requires its own set of considerations. Unlike IT systems, industrial systems interact with physical equipment, people, and processes, and any disruption can affect safety, environmental compliance, and production stability. This section focuses on what makes IACS incident response unique and how these environments influence the way incidents are detected, confirmed, and managed.

Understanding the information gaps in industrial networks

One of the first challenges in an industrial environment is the lack of immediate visibility. While many facilities now operate with segmented OT networks, central log collection, and industrial monitoring tools, there are still systems that remain isolated or entirely islanded. These networks are often legacy systems, vendor-maintained equipment, or standalone controllers that were never designed to communicate outside their own boundaries.

An isolated network has extremely limited connectivity. An islanded network has none. This makes detection difficult because alerts do not always reach the **Security Operations Center** (**SOC**) or the monitoring team. When something goes wrong, the first indication may come from an operator noticing strange equipment behavior rather than from an automated alarm. This delay affects the entire response timeline. Therefore, investigators must plan for situations where they may need to physically visit a local PLC panel or access a separate station to understand the situation.

Access and personnel limitations

Another significant factor is access. Industrial facilities often restrict remote access to control systems, and many sites disable it entirely during an active event. Responders, therefore, rely on physical access to equipment. This introduces delays because entry requires badges, safety approvals, or the presence of an escort. Even highly skilled responders may need to wait before they can examine the system that is experiencing the issue.

Safety instrumented systems and their role in response

As we discussed in *Chapter 6*, a **safety instrumented system (SIS)** is a protective system that monitors critical conditions and automatically places equipment in a safe state when something goes wrong. SIS networks are intentionally separated from the main control system. This independence improves safety but adds complexity during a cyber event. When the main OT network is affected, responders must verify that the SIS is functioning as expected and that no safety functions have been triggered or inhibited.

For example, if a distributed control system shows abnormal behavior due to a cyber issue, responders must confirm that the SIS responsible for pressure relief, emergency shutdown, or burner management is still healthy. This verification step is essential because an incorrect assumption about SIS health can escalate a simple cyber incident into a potential safety hazard.

Process stability before cyber response

In industrial operations, the safety and stability of the physical process always come first. Before responders begin collecting logs, isolating traffic, or blocking accounts, they must ensure that the equipment is stable. Operators may need to steady flows, control pressures, or bypass non-critical alarms before incident responders take any cybersecurity action.

This order of operations may feel unusual to IT teams, but it reflects the priority of keeping the industrial process safe. A well-designed IRP for IACS will clearly define how operational stabilization and cybersecurity tasks work together.

Vendor dependencies during response

Many industrial systems rely on vendor-maintained hardware or software. A vibration monitoring system, an analyzer package, or a specialized control module may require the vendor's technician to interpret diagnostic logs or unlock certain functions. During an incident, this can delay containment or remediation because the vendor's support team must be engaged, verified, and aligned with the organization's safety procedures. Planning for these delays is an important part of OT incident management.

Change management and approval requirements

Changes to control systems cannot be made freely during an incident. Even actions that seem simple, such as restarting a controller or isolating a workstation, may require approval from operations, engineering, or safety personnel. This is because industrial processes are tightly coupled, and even a temporary change can affect production, quality, or safety. The IRP must clearly explain how emergency changes are requested and approved during an incident.

OT DMZ and firewall considerations during an incident

The OT DMZ and its firewall rules play a major role during containment. Investigators may need to isolate traffic from a specific segment, block an IP address, or temporarily allow a secure channel to retrieve forensic data. Any change to the DMZ must be handled carefully because an incorrect rule can disrupt historian data, **manufacturing execution system (MES)** traffic, or control system monitoring. Incident response planning should therefore include predefined procedures for who can authorize temporary firewall changes and how those changes are validated.

Finally, the organizational environment sets the tone for decision-making, authority, and coordination during an IACS incident.

Organizational environment

The organizational environment strongly influences how incidents are handled across both IT and OT, and it affects how quickly teams can respond. In an IACS setting, this environment includes plant operations, maintenance, engineering, safety, external vendors, and the cybersecurity team. Each group has specific responsibilities and approval requirements, and these shape how decisions are made when an incident occurs. Knowing who can authorize equipment shutdowns, network isolation, or vendor engagement is essential.

In practice, incident response in OT must align with the existing operational chain of command. A plant manager or operations supervisor may have the final say on actions that affect production or safety. Engineering may need to review any activity that touches controllers or process logic. The cybersecurity team can guide containment and investigation, but operational approval is often required before any changes are made. This shared decision structure is one of the reasons IACS incidents unfold differently from traditional IT incidents.

NIST SP 800 39 provides a helpful way to think about these structures by grouping decisions into three tiers. The *organizational tier* focuses on governance and risk tolerance. The *business process tier* integrates response expectations into daily operations. The *operational tier* handles the technical actions at the system level for both IT and OT assets. All three tiers influence how

an incident escalates and how quickly the organization can act. On the other hand, an IRP must account for production priorities, safety considerations, vendor involvement, and the authority held by plant management.

When the organizational structure is understood and built into the plan, the response process becomes clearer and easier to coordinate.

Note: other considerations

During an incident, responders must also account for the practical constraints of industrial operations. Any emergency change often requires approval from operations or safety teams, even when time is limited, because a single adjustment can affect the stability of the process. Valuable process data is also time-sensitive, since high-resolution trends are quickly overwritten, which means responders need to capture information early before it disappears. Another consideration is staffing. Many sites do not have dedicated cybersecurity personnel on every shift, so incidents that occur at night or on weekends are often first identified by operators who must make the initial assessment before specialized teams arrive.

Now, we will transition into the next topic: how threat intelligence and monitoring guide detection and early analysis in IACS environments.

Threat intelligence and monitoring in IACS environments

Threat intelligence and monitoring play a major role in detecting issues early inside an IACS environment. Monitoring tools must be tailored to the process, the controllers, and the communication patterns that keep industrial systems running. The goal is not only to detect malicious activity, but also to identify unusual behavior that could affect the physical process.

In an IACS environment, normal operations follow a predictable pattern. Controllers talk to HMIs at fixed intervals, historians collect tags on a schedule, and operator actions follow a routine pace. When this rhythm changes, it can be a sign of trouble. For example, if a PLC that normally communicates every 100 milliseconds suddenly begins responding every 5 seconds, that delay may indicate overloaded firmware, unauthorized polling, or a compromised engineering workstation. These are subtle indicators that would be ignored in an IT network but are important in OT.

Threat intelligence supports this effort by helping teams understand which vulnerabilities, malware families, or attack techniques are currently being used against OT environments or industrial vendors. Since many incidents begin at the corporate level or through vendor networks, intelligence helps responders focus their attention on the right alerts and entry points.

Monitoring in OT depends heavily on passive techniques. Active scanning is avoided because it can disrupt sensitive equipment. Instead, the environment uses passive monitoring sensors, network taps, and specialized OT visibility tools that observe traffic without sending probes. These tools identify abnormal commands, changes in firmware versions, shifts in engineering workstation activity, and unusual controller instructions. When combined with the DMZ logs and historian trends, responders get a clear picture of what is happening. *Figure 7.1* shows a typical OT flow:

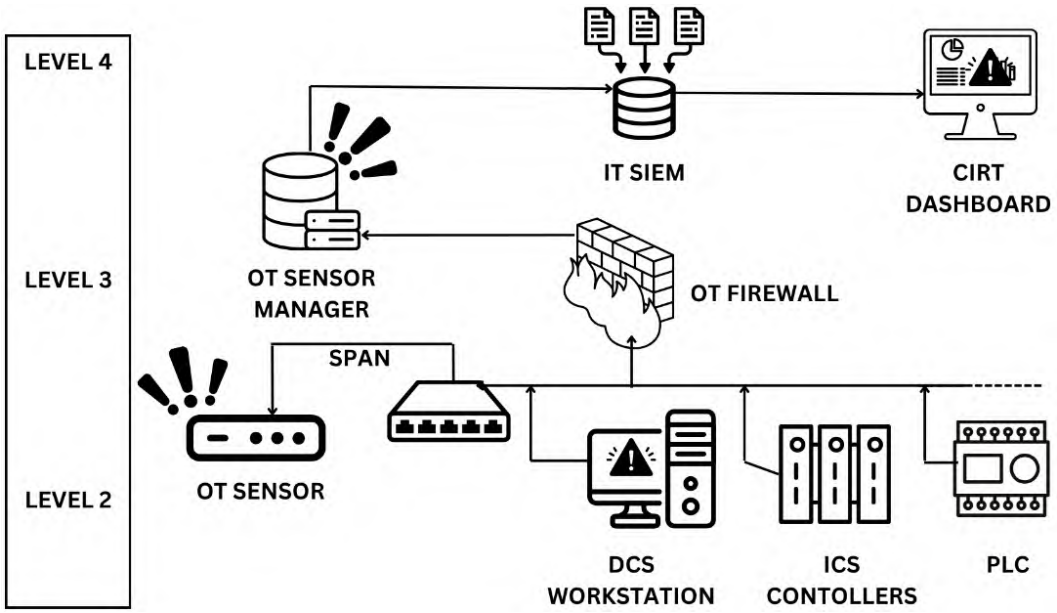


Figure 7.1 – OT visibility flow using passive sensors, SPAN ports, the OT sensor manager, and IT SIEM integration to support early detection in IACS environments

To make this easier to visualize, consider the following simple example. A control room operator notices that several pumps begin cycling more frequently than usual. At the same time, the OT sensor, connected to a SPAN port, as shown in *Figure 7.1*, detects a new engineering workstation attempting to communicate with multiple PLCs on the control network. The OT sensor manager at level 3 begins flagging unusual traffic patterns and forwards these alerts through the OT firewall into the IT SIEM. The analyst reviewing the **Cyber Incident Response Team** (**CIRT**) dashboard also sees a sudden spike in write operations recorded by the historian.

In an OT environment, this combination of events can indicate unauthorized logic changes or manipulation of setpoints. This early visibility allows responders to investigate before the physical process is affected.

Note

A SPAN port, also called port mirroring, is a switch feature that creates a copy of network traffic and sends it to another port for monitoring. In an OT environment, this is the preferred method for connecting an OT sensor because it allows the sensor to observe all traffic flowing between controllers, workstations, and servers without inserting anything into the live process network.

The SPAN port does not interfere with the equipment. It simply mirrors traffic so the sensor can analyze commands, detect unusual behavior, or identify new devices trying to communicate with PLCs. This approach keeps the control network safe while giving responders the visibility they need during an incident.

Active and passive monitoring techniques

Monitoring in an IACS environment can be done using active or passive techniques, and each method brings benefits and limitations. **Passive monitoring** observes traffic without sending any probes or commands into the network. It relies on SPAN ports, mirrored traffic, and sensors that watch controller communications in real time. This makes passive monitoring a safe choice for sensitive or legacy devices, since it does not interfere with the process.

Active monitoring performs scans or device queries to collect information about systems. These methods can reveal missing patches or configuration changes, but they introduce traffic into the control network. Some equipment may respond unpredictably to this activity, which is why active techniques are often restricted to maintenance windows or performed with vendor oversight.

This topic is a point of speculation and often the center of discussion when designing an OT security solution or when engaging external vendors. Some environments prefer a purely passive approach, while others are comfortable with limited active techniques. At the end of the day, the real deciding factor is how well the IACS specialists and OT cybersecurity teams understand their environment. Their knowledge of the process, the network, and the behavior of the equipment guides how security appliances such as firewalls and switches are configured to prevent issues during active scanning. When planned carefully, a combination of passive and active strategies can be used safely to improve visibility without disrupting operations.

Note

Passive monitoring systems work by mirroring traffic from critical segments using SPAN ports or network taps. This approach does not interfere with normal operations and allows the organization to establish a baseline of expected network behavior. Over time, these baseline patterns make it easier to identify unusual device communications, unexpected engineering workstation connections, or unauthorized commands targeting IACS systems such as the PLCs, DCS, SCADA, and so on.

With the monitoring landscape established, it is important to understand how these alerts, whether real-time or asynchronous, translate into incident severity and operational impact. This brings us to the role of classification in an IACS environment.

Types of threat intelligence and monitoring systems

Monitoring in IACS environments generally falls into two categories: real-time monitoring and asynchronous alerts. Each serves a different purpose and complements the other, especially in facilities where visibility can be limited and processes cannot be interrupted casually.

Real-time monitoring

Real-time monitoring involves sensors, analytics platforms, and security tools that observe live traffic and system behavior within the OT network. These tools provide immediate visibility into abnormal activity and help responders detect issues as they unfold. In OT environments, real-time monitoring is typically implemented through passive sensors deployed at strategic network segments, often within the level 2 or level 3 zones of the Purdue model.

Common real-time monitoring tools include the following:

- **Intrusion detection systems (IDSs)** – Identify suspicious activities, but do not block traffic
- **Intrusion prevention systems (IPSs)** – Detect and actively block malicious traffic
- **Network traffic analyzers** – Monitor packet flows to identify unusual behavior
- **SIEM systems** – Correlate security alerts from multiple sources
- **Asset behavior analytics platforms** – Use machine learning to detect deviations from normal operational patterns

In IACS/OT, implementing these tools requires careful planning. Many vendors support only specific protocols; some legacy controllers do not generate standard logs, and production environments cannot tolerate unexpected latency or scanning. Engineering and operations teams must work together to place sensors where visibility is maximized without affecting process stability. For example, a passive IACS/OT sensor can be connected to a switch SPAN port to capture mirrored traffic, ensuring that no packets are interrupted or delayed.

Asynchronous and other alerts

Asynchronous alerts are generated at scheduled intervals rather than continuously. These alerts rely on periodic scans, manual observations, log reviews, and correlation tools that operate at slower intervals. Although not real-time, asynchronous alerts play a major role in IACS environments where many systems lack continuous telemetry.

In IACS/OT, asynchronous alerts are extremely valuable because they capture subtle changes that may not trigger immediate alarms. For example, a slow drift in historian trends, an operator's observation of unusual pump cycling, or a weekly file integrity report can reveal issues that real-time tools may miss. These alerts also supplement visibility when legacy systems do not support continuous monitoring.

Some of the commonly used asynchronous alerts/activities include the following:

- **Operator calls to on-call support** – Field operators report suspicious behavior or unexpected system responses.
- **Periodic security assessments** – Routine evaluations of system security, including access control reviews and vulnerability scans.
- **Emergency response periodic drills** – Simulated cyber incident response exercises to test preparedness and response effectiveness.
- **Periodic file integrity check** – Routine verification of log file integrity to detect tampering, missing entries, or unauthorized modifications.
- **Delayed log analysis** – Scheduled analysis of security logs to identify patterns, anomalies, or suspicious activities that may not be immediately visible in real-time monitoring. This can be automated or on demand.

Figure 7.2 illustrates a communication flowchart demonstrating how an asynchronous alert is processed during an incident.

Figure 7.2 – Asynchronous alert communication flow for OT incidents

For example, *Figure 7.2* shows how an asynchronous alert moves through the facility's communication pathway. Imagine a scenario where an operator notices that a conveyor motor starts and stops more frequently than usual. The operator reports this observation to the support team responsible for OT systems. If the issue is not related to OT, it is reassigned accordingly. If it is OT-related, a dedicated OT incident response team is activated. This team then notifies the site's emergency operations center so that the incident is tracked and managed while maintaining operational awareness.

This approach highlights the importance of structured communication, especially when alerts originate from human observation. Training the support team to ask precise diagnostic questions and ensuring that operators follow the correct reporting channels helps streamline incident detection and response. Even without real-time telemetry, such alerts can provide early warning of cyber activity, equipment malfunction, or process anomalies.

These alerts serve as early signals that something is unfolding, but they must be interpreted in the right context. This is where incident classification becomes essential. *Chapter 6* introduced the types of incidents and the fundamentals of incident classification, which help determine the level of urgency, the potential operational impact, and the appropriate escalation path.

Before we move into planning and response activities, it is helpful to revisit incident classification from an industrial perspective. *Chapter 6* introduced the FEMA incident types, cybersecurity **severity** (**SEV**) levels, and MITRE ATT&CK behaviors commonly associated with intrusions. Now, we will focus on how they apply specifically to IACS environments, where a small process deviation can carry significant operational or safety implications.

In an industrial setting, classification is influenced by three core factors: the difficulty of the incident, the severity of the threat, and its potential impact on the physical process. MITRE ATT&CK helps map observed activity to known adversary tactics, while the FEMA ICS incident types provide the operational structure that industrial facilities already use for escalating incidents and organizing resources. SEV ratings help determine urgency, while the ICS incident types help determine the scale of coordination and resource allocation required. When used together, these approaches create a common language for describing the incident and making timely escalation decisions.

For a combined view of how these frameworks align, including OT-specific examples, see *Table 7.1*. This unified table maps FEMA ICS incident types to SEV ratings and MITRE ATT&CK categories, providing a practical classification model for cyber-physical incidents.

FEMA ICS incident complexity	**Description (incident type)**	**Example**	**SEV level**	**Response action**
Type 5 (least complex)	Minor events, easily managed within a single team	Failed login attempts, routine phishing emails, isolated malware detections	SEV4 (informational)	Logged, no immediate action required
Type 4	Localized incidents with minor operational impact	Unauthorized USB device detected, brute-force login attempts, malware on non-critical systems	SEV3 (low priority)	Monitor, investigate, and document
Type 3	Moderate incidents requiring coordinated response	Successful phishing attack on an OT operator, lateral movement detected, minor DDoS attack	SEV2 (medium priority)	Assign to SOC/OT analysts, escalate if needed
Type 2	Major incidents with potential widespread impact	Ransomware in the OT network, control system compromise, persistent adversary activity	SEV1 (high priority)	Immediate containment, executive notification, crisis team activation

Type 1 (most complex)	Catastrophic incidents requiring a full emergency response	Nation-state attack, cyber-physical sabotage, coordinated attack on multiple CI sectors	SEV0 (critical)	National-level response, full crisis management, government agency involvement

Table 7.1 – Unified incident classification table (MITRE + FEMA ICS + SEV)

By incorporating MITRE ATT&CK examples, the integrated table connects technical threat behaviors with practical response actions, creating a structured way to interpret incidents in an industrial environment. It also establishes a clearer escalation path so that incidents are addressed efficiently and in proportion to their severity. This combined view gives ICS operators, security teams, and emergency response personnel a common understanding of what is unfolding, which supports a more coordinated and timely response to cybersecurity threats. With classification clarified, the next section focuses on planning and IACS-specific response considerations that support safe, structured, and coordinated recovery.

IACS-specific incident response planning

Incident response for IACS environments cannot rely on a generic IT-centric approach. Industrial systems behave differently, react differently to disruptions, and carry a much higher potential for cascading operational and safety consequences. The unique and complex nature of IACS environments, therefore, requires a multi-layered, highly specialized IRP that accounts for engineering constraints, process safety requirements, and the behavior of industrial automation systems.

For example, isolating a compromised workstation in a corporate IT network is a routine action. In contrast, isolating an engineering workstation in a chemical plant or manufacturing facility without understanding its role may interrupt the control loop that maintains temperature, pressure, or sequencing operations. A seemingly simple containment action could trigger a process upset, activate a safety instrumented function, or bring production to an abrupt halt.

In this section, we will explore how to build an IACS-specific **incident response plan (IRP)** using a structured planning approach:

- Defining the goals of the IRP
- Establishing the scope of systems and processes it covers
- Identifying key personnel who form the **incident response team (IRT)**

Throughout this discussion, we assume that the organization has already completed an asset identification and classification exercise covering OT networks, field devices, industrial controllers, and supporting systems.

Although the focus here is on the OT response, the facility's overarching IRP, which was introduced earlier in the book, remains the parent framework. The OT-specific plan integrates into that structure alongside IT, fire safety, physical security, emergency operations, and business continuity. The objective is not to create a separate OT IRP, but to ensure OT response activities align with the organization's established command and safety protocols.

Defining the goals of the IACS IRP

A meaningful starting point is defining the objective and scope of the OT IRP. At its core, the IRP aims to ensure that the organization can detect, respond to, contain, and recover from incidents that affect industrial control systems. This requires balancing cybersecurity objectives with operational continuity, process safety, regulatory expectations, and potential health, safety, and environmental consequences that may emerge during a disruption.

The goals of an OT IRP typically include the following:

- Maintaining safe and stable operation of industrial processes
- Preventing or minimizing production downtime
- Protecting human life, equipment, and the environment
- Preserving the integrity, reliability, and availability of IACS assets
- Ensuring consistent communication and decision-making during incidents
- Supporting regulatory and compliance obligations
- Enabling structured recovery within defined operational thresholds

These goals become the foundation upon which detection, containment, and recovery procedures are built.

Establishing the scope of the IRP

The scope defines what the IRP covers. In an industrial facility, this includes the following:

- OT networks, field instrumentation, PLCs, DCS systems, and historians
- Engineering workstations and HMI systems
- SISs
- On-premises and remote maintenance interfaces

- Interfaces between IT and OT networks
- Vendors, contractors, integrators, and remote support channels
- Upstream and downstream operational dependencies

The scope should clearly identify the following:

- Systems that require the highest protection
- Systems where downtime creates safety implications
- Systems that support life, environment, or critical production functions
- Interconnected assets where a cyber compromise can cause cascading failure

This scoped inventory allows the team to assign appropriate response tiers, communication paths, failover strategies, and recovery expectations.

Identifying key personnel for the IRT

An OT incident response effort relies on individuals with operational, engineering, and cybersecurity expertise. The IRT should include the following:

- OT/ICS engineers
- Control system specialists (PLC/DCS engineers)
- IT/OT network administrators
- Cybersecurity analysts
- Process operators and supervisors
- Safety officers
- Emergency operations representatives
- Communications/management liaisons

Each team member must have clearly defined responsibilities. The IRP should also specify the following:

- Who has the authority to isolate systems
- Who is allowed to shut down or restart processes
- Who communicates with executives, regulators, or emergency services
- Who performs forensic data capture or vendor coordination

The goal of IRP is to support the requirements in a **Business Continuity Plan (BCP)**. To understand how continuity integrates into the IRP, consider a realistic example from an automobile manufacturing plant. Our example facility relies on synchronized robotic assembly lines, PLCs, and automation systems. *Figures 7.3* and *7.4* illustrate the event progression.

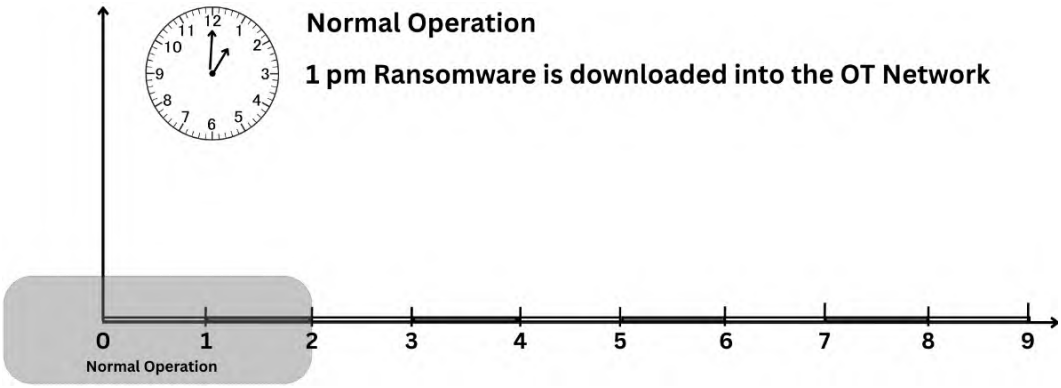


Figure 7.3 – The timeline shows normal operation before the cyber attack

At 1 p.m., ransomware is unknowingly downloaded into the OT network through some method, such as a compromised engineering workstation or a malicious file transfer. At this stage, the ransomware has not yet activated, and operations continue without visible disruption.

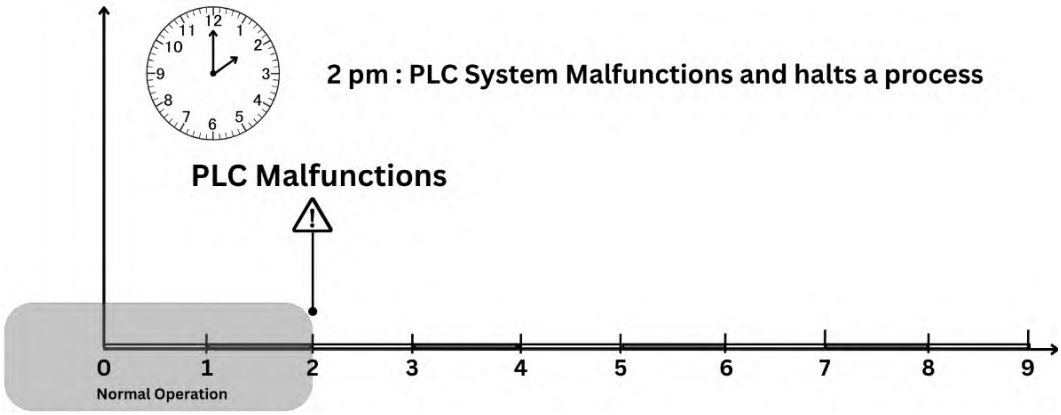


Figure 7.4 – Ransomware activates and brings down the operation

At 2 p.m., the ransomware activates through its programmed trigger and begins executing its payload, compromising the PLCs that control the robotic arms. As soon as the controllers are affected, the assembly line halts and production stops immediately.

The impact is not limited to downtime. The event may cause the following:

- Mechanical misalignment
- Safety system activations
- Loss of in-process batches
- Environmental venting or waste generation
- Extended supply chain delays

Through its business impact analysis, the organization has defined the continuity metrics that guide recovery planning in industrial environments. These parameters determine how quickly critical systems must be restored, how much data loss is acceptable, and how long operations can remain offline before the consequences become severe. They are established in advance so that responders understand the operational boundaries and recovery expectations before any disruption occurs.

The key predetermined metrics include the following:

- **Recovery time objective (RTO)**: The maximum amount of time allowed to restore a system or function after a disruption. RTO defines how quickly the organization must return the affected system to an operational state to prevent unacceptable consequences.
- **Recovery point objective (RPO)**: The maximum acceptable amount of data loss expressed in time. RPO indicates how far back in time the organization must be able to recover data to maintain safe and reliable operation.
- **Work recovery time (WRT)**: The time required after technical restoration to bring the system back to full, steady-state operation. WRT accounts for calibration, verification, safety checks, and process stabilization that occur after recovery.
- **Maximum tolerable downtime (MTD)**: The longest allowable time that a system or process can remain offline before the disruption results in irreversible or severe operational, financial, safety, or environmental consequences.

The following key metrics are defined in the OT-specific section of the IRP for the process:

- **RTO: 3 hours** – At 1 p.m., the ransomware is downloaded (1-hour mark), and malicious code enters the OT network, but the PLCs continue operating. At this point, nothing in the continuity metrics is triggered.

  At 2 p.m., the PLC malfunctions (2-hour mark), and the ransomware activates and causes the PLC to stop functioning. This moment becomes the RPO reference, because data and system state prior to 2 p.m. is considered recoverable.

  RPO = 2 p.m.

Between 2 p.m. to 5 p.m., the system is restored (RTO period); however, the PLCs remain offline, and the system is fully restored at 5 p.m., which reaches the end of the defined *RTO = 3 hours* (from 2 p.m. to 5 p.m.).

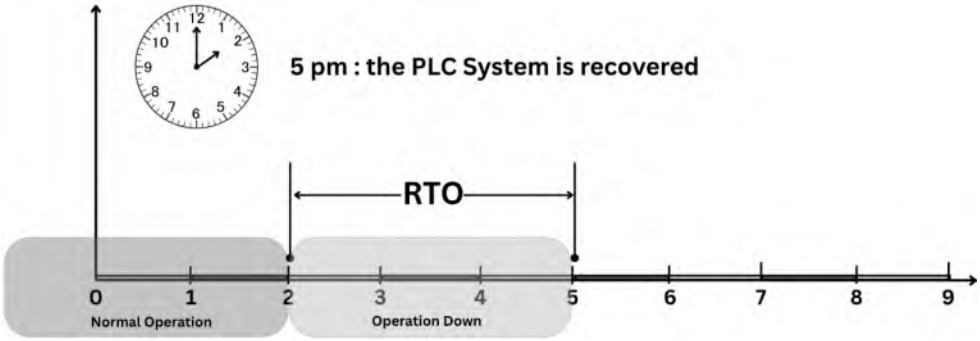


Figure 7.5 – Visualization of RTO and systems recovered but PLCs are still offline

- **WRT: 45 minutes** – Between 5 p.m. and 5:45 p.m. is considered the WRT, which is when the PLC is technically restored. Technicians require an additional 45 minutes to recalibrate equipment, validate operation, and return the line to a steady state. This period represents *WRT = 45 minutes*.

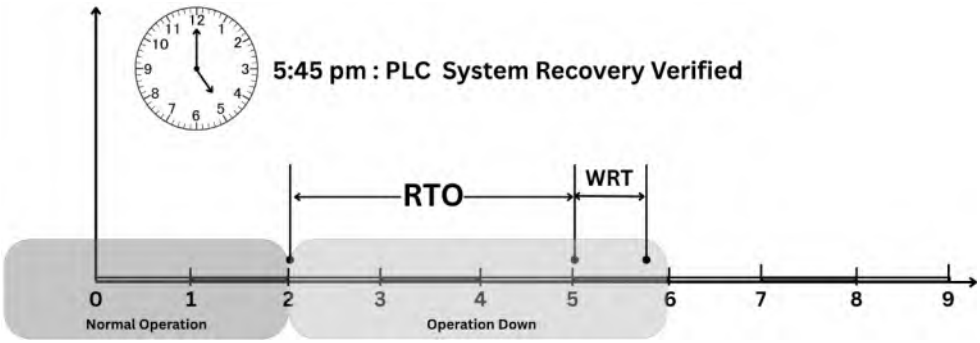


Figure 7.6 – Visualization of WRT shows additional work required to bring the operations online

- **MTD: 4 hours** – Now, we can calculate the MTD. The figures show the MTD window extending from the moment of failure at 2 p.m. to the absolute latest acceptable recovery point just before 6 p.m. In this case, this represents the MTD of four hours.

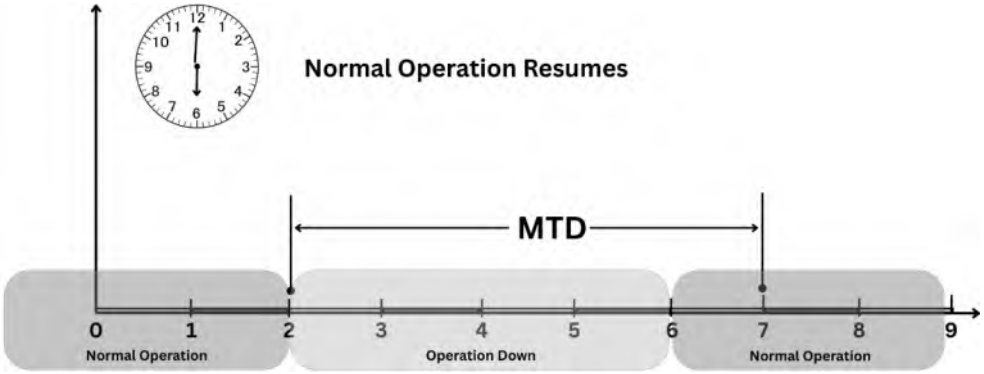


Figure 7.7 – MTD envelope for manufacturing line

Figure 7.8 illustrates a timeline of recovery for a PLC failure, showing the relationship between RTO, RPO, WRT, and MTD in an operational continuity strategy.

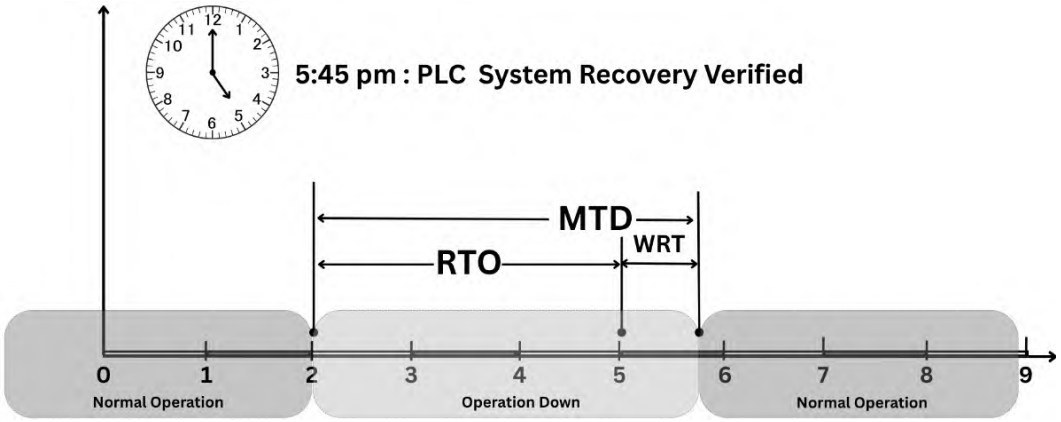


Figure 7.8 – Visualization of MTD, normal operation restored

MTD is the longest period of time a critical system or process can remain unavailable before the consequences become unacceptable for the organization. These consequences may include production loss, safety risks, regulatory violations, financial impact, or operational instability. MTD establishes the absolute upper limit for recovery efforts. If recovery exceeds the MTD threshold, the disruption begins to create irreversible or severe outcomes for the facility.

By defining these metrics, organizations can develop effective IRPs to minimize downtime and ensure seamless recovery from disruptions.

Now that we have outlined how recovery timelines and tolerances guide the response effort, it is equally important to examine how organizations uncover the root cause of an incident. This requires a disciplined approach to cyber forensics, tailored to the realities of industrial systems where uptime, safety, and process stability remain paramount.

Forensic data collection and incident documentation

Cyber forensics, or digital forensics, is the disciplined practice of collecting, analyzing, and preserving digital evidence to understand what occurred during a cyber incident. The objective is to identify the cause of the disruption, assess its impact, determine how the attacker gained access, and preserve evidence in a manner that is legally defensible if needed.

In traditional IT environments, forensic investigations often emphasize data confidentiality and focus heavily on retrieving logs, recovering deleted files, and analyzing memory. Industrial environments, however, require a different mindset. In OT and IACS settings, system availability, operational reliability, and safety take priority over deep forensic examination. When a critical workstation or controller goes offline, the first question is not "How do we extract evidence?" but "How do we safely restore the process?".

This distinction drives many of the forensic challenges in OT environments. To appreciate why OT investigations are so different, it is useful to look at the specific limitations that make forensic work uniquely difficult in industrial settings:

- **Limited or no logging**: Many PLCs, RTUs, HMIs, and standalone industrial devices do not generate robust logs. Some log only faults, not security events.
- **Aging hardware and legacy systems**: Older systems may not support modern forensic tools, and power-cycling a device to capture evidence may itself introduce operational risk.
- **Strict uptime requirements**: Taking a controller offline to image a disk or extract memory could jeopardize the physical process.
- **Safety and process impact**: If a system controls pressure, temperature, or sequencing, "pulling the plug" to conduct a forensic acquisition may trigger a trip, shutdown, or safety event.
- **Network segmentation**: OT networks are often isolated or have very limited visibility, which restricts the ability to capture real-time packet data.
- **Operational culture**: In many facilities, the priority is getting the equipment running again. Wiping and reloading a workstation, rebuilding a PLC image, or replacing a drive is often faster and safer than preserving a forensic copy.

As a result, responders must balance the need for meaningful forensic evidence with the operational realities of keeping an industrial process stable.

In industrial environments, these simple actions carry far more weight than they do in IT. Resetting generally means clearing software states or restarting a service on a device. Rebooting restarts the entire operating system. Power cycling removes electrical power completely and brings the device back online from a cold start.

While these seem routine, each action can interrupt process control, disrupt communications, and trigger unplanned failovers. Controllers, PLCs, and RTUs often run continuous processes that depend on stable scan cycles and uninterrupted field I/O. When a controller reboots or loses power, it may reload its program, re-establish all I/O connections, and renegotiate network sessions. If a new configuration or firmware has recently been downloaded, the controller may apply those changes only after a reboot, which can alter logic execution, timing, or fail-safe states.

This is why OT teams must evaluate process impact, interlocks, upstream and downstream equipment, and shift availability before performing any of these actions, no matter how routine they seem.

Why OT forensics is often incomplete

In many cases, only partial forensics are possible, and the team must collect whatever information can be captured safely without interrupting operations. In OT environments, the pressure to maintain system availability often outweighs the desire for a complete forensic investigation because downtime is costly, disruptive, and, in some cases, unsafe.

For example, if an engineering workstation shows signs of compromise during a production run, taking it offline to perform a full disk image may not be feasible. Instead, responders may gather screenshots, export available logs, and preserve the current PLC project files while keeping the workstation running long enough for operations to maintain control.

Alternatively, if the organization has implemented IACS monitoring using third-party network analysis tools that are OT-focused monitoring platforms, responders can rely on packet captures, baseline deviations, and historical communication records gathered by these sensors. These platforms often retain valuable forensic artifacts that would otherwise be lost when field devices are power-cycled, reformatted, or reset. While this approach still may not provide a complete forensic picture, it enables responders to piece together the sequence of events without compromising process stability.

This operational urgency often extends to HMIs, historians, and other critical interfaces, which may be rebuilt on the spot simply to restore visibility and control for operators. The faster these systems are brought back online, the more evidence is inevitably lost. This creates a natural tension between forensic thoroughness and operational reality. In CI, the priority is restoring safe and stable operation, which means forensic completeness is rarely achievable and often must take a secondary role.

Types of forensic methods used in IACS environments

Because traditional digital forensics cannot always be applied in industrial settings, OT investigations rely on multiple complementary methods. Each approach contributes a different piece of the picture, allowing responders to reconstruct what happened while still protecting process stability.

Network forensics

Network forensics focuses on capturing and analyzing traffic within the OT network to identify unusual communications, unauthorized connections, or suspicious lateral movement. In industrial environments, passive collection is preferred to avoid interfering with live control traffic.

For example, a passive OT sensor may reveal that a previously unknown workstation has begun sending write commands to multiple PLCs, or that a controller is communicating with an IP address outside the expected network range. These insights often provide the first indication that an attacker has moved into the control system.

Endpoint forensics

Endpoint forensics uses logs, alerts, and security agent data from engineering workstations, HMIs, historian servers, and other OT endpoints. These systems often hold critical clues because they sit at the interface between human operators and industrial controllers.

For example, an engineering workstation may show evidence of unauthorized project file uploads, or an HMI may generate repeated authentication failures that point to credential abuse. Reviewing these artifacts helps determine whether unauthorized changes were made to the process.

Log file forensics

Log file forensics involves reviewing event logs from servers, applications, firewalls, switches, historian databases, and syslog servers. In OT networks, logging capabilities vary widely, and logs may be incomplete or inconsistent, which makes correlation harder but not impossible.

For example, firewall logs may show blocked attempts to reach a PLC, while historian logs show unexpected parameter adjustments at the same time. Even if individual logs are sparse, correlating them can reveal the timeline of an intrusion.

Filesystem or disk forensics

Disk forensics includes acquiring storage media, recovering deleted files, analyzing PLC project folders, inspecting metadata, and identifying hidden or manipulated configurations. In OT environments, this method is more challenging because shutting down or removing drives may disrupt operations.

For instance, a compromised HMI might contain remnants of a malicious script in its temporary files, or an engineering workstation may hold older versions of PLC logic that indicate when changes were made. These artifacts can be invaluable but must be gathered without interrupting critical processes.

Controller or firmware forensics

Controller-level forensics focuses on extracting PLC logic, firmware, configuration files, or memory snapshots and comparing them to known-good baselines. This method is unique to OT environments and is rarely used in traditional IT investigations.

For example, downloading logic from a PLC may reveal new rungs (lines of code) added by an attacker to bypass safety limits, or firmware comparison may show that a controller was downgraded to a vulnerable version. These findings often confirm whether the attacker directly manipulated the physical process.

These forensic methods must be chosen carefully because every action carries operational risk. The goal is to gather as much insight as possible without interrupting process stability. In some cases, this may mean using only network and log forensics during the incident and saving deeper disk or controller-level forensics for a planned outage.

Another important aspect to cover is the process of restoring affected systems and returning the facility to a safe and stable operating state. This brings us to incident remediation and system recovery in IACS environments.

Incident remediation and system recovery in IACS

In IACS environments, recovery activities must consider operational dependencies, engineering constraints, and the physical effects of taking devices offline. A strong recovery process begins long before an incident occurs. It relies on clear identification of critical assets, an understanding of their role in the

process, and detailed knowledge base documents that outline how each system is recovered. These preparations allow responders to act with confidence when production or safety conditions are at risk.

During an incident, recovery often becomes a collaborative effort between internal OT, engineering, and operations teams and external vendors. For example, if an electrical utility experiences corrupted RTUs across several substations, internal teams stabilize operations by isolating affected segments and maintaining manual oversight. The OEM's substation specialist then works side by side with engineering teams to reload firmware, restore configurations, and validate control and telemetry behavior before returning each station to normal operation. This approach ensures that recovery is performed safely and correctly, while reducing the risk of further disruption.

Support contracts with OEMs and integrators play an essential role in this process. Many industrial devices and control applications require vendor-specific tools, firmware, or expert validation that internal teams cannot perform alone. Active support agreements give organizations direct access to specialized engineers, authoritative configuration files, and priority response channels during incidents, thereby improving recovery outcomes. Further, support contracts also help ensure that post-incident validation is completed properly. Vendors can confirm that restored logic, settings, and communication mappings match the intended design, reducing the risk of misconfiguration. Their involvement strengthens documentation, compliance alignment, and lessons learned, all of which support long-term resilience.

Together, these elements form a complete picture of incident remediation in IACS environments. Recovery is not only a technical exercise but a coordinated operational effort that depends on preparation, clear documentation, and strong collaboration between internal teams and external partners.

Exercise 1: Build your own OT-specific IRP

Objective: To help learners apply the concepts from this chapter by drafting the foundational structure of an OT-focused IRP tailored to their own facility or a fictional IACS environment

Scenario: Your organization operates a small industrial facility with the following components:

- PLC-based control loops
- A historian server
- Engineering workstations
- Remote vendor access through a jump host
- OT monitoring through a network sensor

Leadership has asked you to create the first draft of an OT IRP that can be integrated into the overall facility IRP.

Instructions: Using the knowledge from this chapter, complete the following sections:

- Define the goal of the OT IRP
- Write one paragraph describing what the OT IRP is meant to achieve
- Include operational continuity, safety, regulatory expectations, and integration with the corporate IRP
- Establish the scope
- Identify which systems, processes, PLCs, networks, and operational functions the OT IRP covers
- List at least the following:
    - OT network zones
    - Critical controllers
    - Engineering assets
    - Data sources (historian, sensors, and logs)
- Identify key personnel
- Build a simplified OT IRT
- Assign roles such as the following:
    - OT incident lead
    - Engineering lead
    - Operations lead
    - IT security liaison
    - Vendor support contact
    - EHS representative
- Define predetermined recovery thresholds
- Choose realistic values for the following:
    - RPO
    - RTO
    - WRT
    - MTD

- Explain why you selected these values
- Create a one-page OT IRP summary (combine the preceding items into a one-page summary that could be inserted into a real IRP)

Deliverable: A one-page OT IRP outline (goal, scope, team, and thresholds)

Exercise 2: Identify alerts and escalation paths in an OT environment

Objective: To help learners distinguish between real-time OT alerts and asynchronous alerts, and determine how each should be escalated

Scenario: Review the following alerts that occurred during a 6-hour shift. Your job is to classify each alert as real-time or asynchronous, and determine the correct escalation path:

- The OT network sensor detects a PLC receiving unexpected write commands from an engineering workstation
- The operator calls the on-call OT technician after noticing a pump cycling irregularly
- Daily security tool output shows expired local admin credentials on an HMI
- SIEM correlation rule triggers for abnormal SMB traffic inside the OT zone
- Weekly file-integrity scan reports the modification of a historian configuration file
- Vendor VPN attempts a connection outside scheduled support hours
- Shift supervisor reports slow HMI response and delayed trend updates

Instructions:

- For each alert, classify the alert type into the following:
    - Real-time monitoring alert
    - Asynchronous alert
- Explain the reasoning: why does it fall into this category?
- Identify the first responding role (choose from the list):
    - Operator
    - On-call OT support
    - Cybersecurity analyst
    - Vendor coordinator
    - EOC (if severe)

- Assign an escalation path
- Identify whether the alert stays local (OT team), routes to IT security, requires engineering involvement, or triggers an operational response

Deliverable: A completed table with classification, reasoning, responder, and escalation path for each alert

Exercise 3: OT forensics decision-making under operational pressure

Objective: To practice making forensic decisions in an OT environment where evidence collection must be balanced with operational continuity, safety, and vendor requirements

Scenario: A manufacturing facility experiences unusual behavior on an engineering workstation responsible for PLC programming. Production is still running. You are called to investigate, and the following evidence sources are available:

- Memory dump of the workstation (requires shutting it down for 3 minutes)
- Network captures from an OT sensor
- PLC logic backups (from last week)
- Local Windows event logs (accessible while running)
- Firewall logs from the OT DMZ
- Vendor technician available in 2 hours
- Option to reimage the workstation immediately to restore stability

Instructions:

- Answer the following decision-making questions:
    - What evidence can be collected without affecting operations?
    - Identify the sources that can be accessed live
    - What evidence is too risky to collect now?
    - Identify which actions could disrupt the process
    - What is your recommended immediate action?
- In this situation, what would you do (choose one)?
    - Preserve the workstation and collect a full forensic image
    - Collect partial forensic artifacts and keep the system running

    - Reimage the workstation immediately
    - Other (please state) _____

- **Reflection exercise**: Now that you have chosen an outcome, which forensic methods apply? Select methods such as the following:

    - Network forensics
    - Endpoint forensics
    - Log forensics
    - Controller/firmware forensics

- How would you document the chain of custody in this scenario? (List the minimum information you would record)
- What evidence will be permanently lost if immediate remediation is required? (This reinforces the trade-offs OT teams make)

Deliverable: A short decision memo (five or six sentences) summarizing your forensic approach and your justification for balancing evidence collection with operational stability

Summary

This chapter demonstrated why incident response inside IACS must be approached very differently from traditional IT environments. IACS assets interact directly with physical processes, so every action taken by responders has the potential to influence safety, production stability, environmental controls, and regulatory obligations. We explored the unique operational limitations that shape detection, access, decision-making, and containment in OT networks, such as limited visibility, vendor dependencies, restricted remote access, and the need to stabilize the physical process before initiating cybersecurity actions. Together, these factors create a response environment where operational continuity and safety form the foundation for all subsequent decisions.

We then examined how threat intelligence and monitoring enhance early detection and help translate network behavior into actionable indicators. Building on this visibility, the chapter outlined a structured method to develop an IACS-specific IRP by defining its goals, establishing scope, identifying key personnel, and integrating continuity thresholds such as RPO, RTO, WRT, and MTD. A real-world ransomware scenario highlighted how recovery expectations shape response timelines and how OT teams rely on predefined boundaries to make time-sensitive decisions.

Finally, the chapter discussed forensic data collection in an OT context and why traditional IT forensics often cannot be applied. To address the realities, the chapter outlined practical forensic methods suited for OT environments, including network forensics, endpoint artifacts, log correlations, disk analysis when feasible, and controller or firmware-level examination.

With these foundational practices in place, the next chapter introduces the major incident management standards and frameworks that support CI operations. *Chapter 8* provides a structured overview of FEMA ICS, NIST guidance, ISA GCA's ICS4ICS, and related frameworks that form the backbone of coordinated industrial incident management.

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

8

Introduction to Incident Management Standards and Frameworks for Critical Infrastructure

The incident management field has witnessed a significant evolution in recent years, with numerous standards and frameworks being developed. These frameworks, initially established within the public sector, have also increasingly found application in the private sector. This chapter delves into some of the most commonly referenced and utilized frameworks that form the backbone of effective incident response.

Early incident management frameworks were born out of the necessity for coordinated responses to large-scale emergencies within the public sector. For instance, the United States' fire departments developed the **Incident Command System (ICS)** to serve as a tool for fostering collaboration between various agencies during emergencies.

However, the value of these frameworks soon became apparent across industries. Organizations in the private sector, recognizing the benefits of standardized procedures and clear communication, began adopting and adapting these public sector frameworks.

Today, a multitude of incident management frameworks are tailored to specific industries and operational needs. This chapter aims to provide an overview of the various existing frameworks, offering a broad understanding of their scope and application.

This chapter will cover the following topics:

- Incident management frameworks
- Importance of choosing a framework

Incident management frameworks

An incident management framework should provide a structured and standardized approach to handling incidents. This ensures consistency within an organization through clearly defined roles, processes, and documentation. It should be scalable to handle incidents of different sizes and complexity, while also being flexible enough to customize according to specific needs and industry requirements. Thorough documentation is crucial, providing detailed guidelines and standardized record-keeping to support effective response and comprehensive post-incident analysis. This combination of structure, scalability, flexibility, and robust documentation allows organizations to efficiently manage incidents and adapt as needed. These principles are exemplified in several widely used frameworks within the CI space. Let us take a look at some of the widely adopted frameworks in our industry today.

Incident Command System

As discussed in *Chapter 6*, the ICS—developed by FEMA—provides a standardized, scalable framework for emergency response. Its strength lies in establishing a clear chain of command, standardized terminology, and defined roles that enable multiple agencies to coordinate effectively, regardless of incident size or complexity.

At its core, the ICS emphasizes the following:

- **Unified command**: Ensuring cross-agency collaboration under a single coordinated structure
- **Standardized terminology**: Reducing confusion during high-stress events
- **Scalability and flexibility**: Expanding or contracting the organizational structure based on incident demands
- **Incident action plans (IAPs)**: Guiding response efforts with clear objectives and resource allocation

Figure 8.1 shows the standard ICS organizational framework, illustrating the core command and support functions that enable effective coordination and decision-making during an incident.

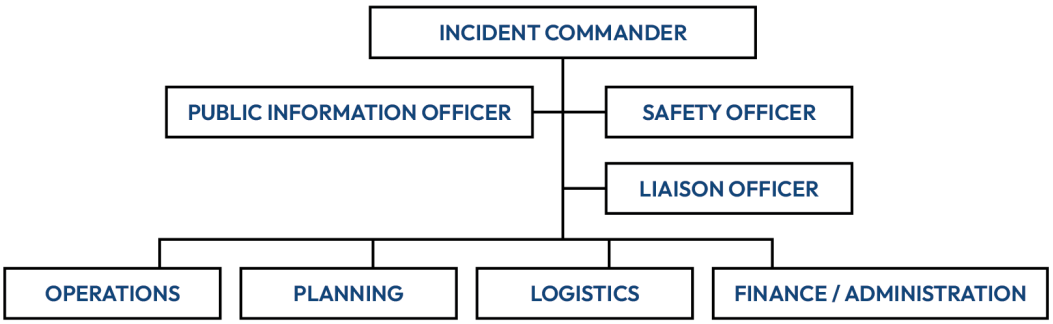


Figure 8.1 – FEMA's ICS framework

At the top, the incident commander oversees the overall response, supported by key officers responsible for public information, safety, and liaison functions. Beneath them, the operations, planning, logistics, and finance/administration sections manage tactical execution, resource tracking, logistical support, and financial accountability. This structure ensures clear lines of authority, effective communication, and efficient resource management across all phases of incident response and recovery.

CI operators in chemical manufacturing, oil and gas, and utilities, along with public safety and emergency response agencies, depend on the ICS as a proven framework for managing complex incidents. Whether responding to physical emergencies, cyber events, or large-scale disruptions, ICS brings structure, shared situational awareness, and coordinated decision-making across technical and operational teams. Whether dealing with natural disasters, industrial accidents, cybersecurity incidents, or large-scale events, the ICS ensures a structured response, clear communication, and effective resource management.

However, the ICS may not always be necessary or practical in small-scale, routine operations, particularly when the incident's complexity does not require a structured command system. In cases such as minor workplace issues, day-to-day administrative tasks, or situations with limited personnel and resources, a formal ICS structure might be excessive. Similarly, in highly specialized or technical fields where incident management demands niche expertise and rapid decision-making by small, experienced teams, the rigidity of the ICS could hinder a faster and more effective response.

This underscores the importance of considering other frameworks or more specialized ones. Different incidents and industries have unique needs that may not be fully addressed by the ICS.

NIST CSF

Frameworks such as the **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)** or **IT Infrastructure Library (ITIL)** provide tailored approaches focusing on specific areas such as cybersecurity or IT service management, offering precise guidance and best practices that align with particular operational contexts while complementing the broader ICS structure when necessary. We will cover some of the key requirements in the following sections for choosing the right framework.

The NIST CSF has evolved significantly since its initial release in 2014 (Version 1.0), with Version 1.1 following in 2018 and the new CSF 2.0 published in 2024. Designed to be flexible and sector-agnostic, the CSF provides organizations with a practical roadmap for managing cybersecurity risks in a structured, outcome-oriented, and scalable manner.

At its core are six key functions—Govern, Identify, Protect, Detect, Respond, and Recover—which together form the foundation of an organization's cybersecurity program, as shown in *Figure 8.2*.

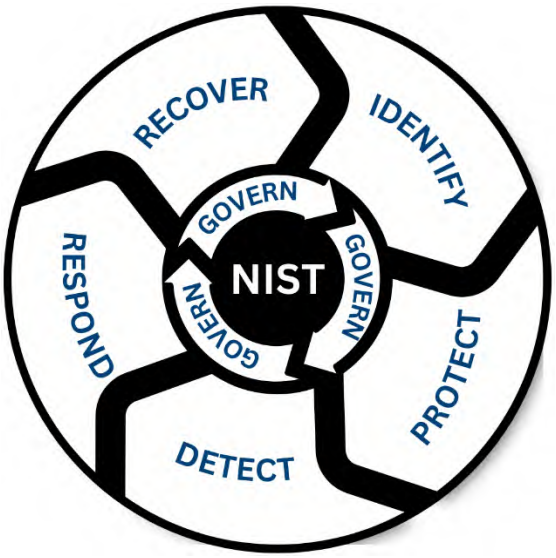


Figure 8.2 – NIST CSF 2.0

Each function plays a distinct yet interconnected role:

- **Govern**: Establishes and communicates the organization's cybersecurity risk management strategy, expectations, and policies. It ensures alignment between cybersecurity priorities and business objectives, reinforcing governance as a continuous process rather than a static policy.

- **Identify**: Develops an understanding of systems, assets, data, and capabilities to manage cybersecurity risks effectively
- **Protect**: Implements safeguards to secure CI services and maintain operational resilience
- **Detect**: Focuses on timely identification of cybersecurity events through monitoring, analysis, and anomaly detection
- **Respond**: Defines actions to contain and mitigate the impact of incidents while maintaining communication and coordination across teams
- **Recover**: Guides the restoration of services and improvement of security measures to strengthen resilience after an incident

In CSF 2.0, organizations are encouraged to develop **profiles**, which define their current and target cybersecurity posture. These profiles help chart a tailored improvement roadmap, allowing organizations to prioritize actions based on mission objectives, regulatory requirements, and available resources.

The framework remains non-prescriptive and adaptable, suitable for large enterprises, small businesses, government agencies, and CI sectors alike. By embedding incident response and recovery considerations across all functions, CSF 2.0 ensures that organizations are both prepared for cyber events and committed to continual improvement.

NIST CSF 2.0 reinforces several guiding principles, such as the following:

- **Outcome-focused**: Encourages defining measurable outcomes for cybersecurity and incident management
- **Risk-based prioritization**: Promotes identifying, analyzing, and prioritizing risks to guide strategic decisions
- **Flexibility and customization**: Allows adaptation across industries and organizational sizes
- **Continuous improvement**: Supports iterative enhancement based on lessons learned and evolving threats
- **Cost-effectiveness**: Emphasizes balancing investment with risk tolerance and business needs

To learn more about the NIST CSF, you can go to `https://www.nist.gov/cyberframework`.

NIST CSF and incident response considerations

The NIST CSF remains one of the most widely adopted tools for managing cybersecurity risk across sectors such as energy, healthcare, financial services, and manufacturing. In April 2025, NIST finalized its updated incident response guidance (SP 800-61r3), aligning it more closely with CSF 2.0 functions. This provides organizations with a structured yet flexible lifecycle for managing incidents, from preparation through recovery and continuous improvement.

At a high level, the framework emphasizes the following when it comes to incident response:

- **Preparation**: Governance, planning, training, and protection activities that establish readiness
- **Detection and analysis**: Identifying and validating potential incidents
- **Response and containment**: Coordinating actions to limit damage and maintain control
- **Recovery**: Restoring systems, services, and business operations
- **Lessons learned and improvement**: Feeding insights back into governance, planning, and protection to strengthen resilience

Figure 8.3 illustrates this life cycle, showing how incident response is tightly integrated with broader CSF functions.

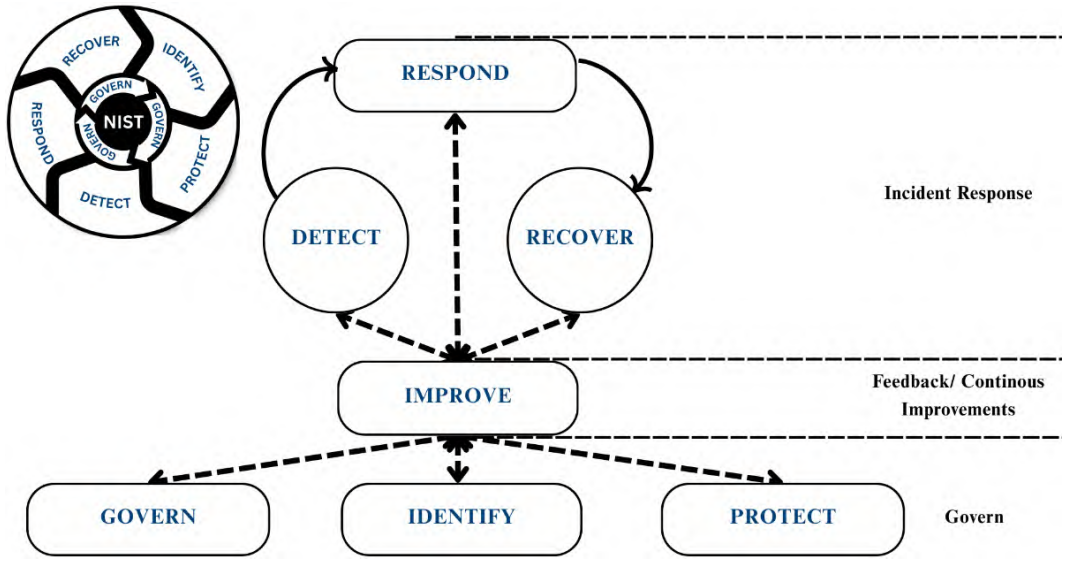


Figure 8.3 – incident response life cycle model inside the NIST CSF 2.0 functions

Unlike earlier drafts, the finalized version underscores continuous improvement as a central theme, reinforcing the idea that incident response is not a one-time cycle but an ongoing practice that strengthens organizational security posture.

Together, the CSF 2.0 and IRF (SP 800-61r3) form a comprehensive ecosystem for cybersecurity risk management and incident response preparedness. The CSF ensures that incident response is built into governance and strategic planning, while the IRF ensures that when an incident occurs, it is handled efficiently, systematically, and in alignment with organizational goals (`https://csrc.nist.gov/pubs/sp/800/61/r3/final`).

IT Infrastructure Library

Primarily used in IT service management, ITIL outlines best practices for incident management within the IT realm, including problem identification, resolution, and prevention. *Figure 8.4* presents a widely recognized depiction of the ITIL framework, illustrating its core components: service operation, service design, and service transition.

Figure 8.4 – ITIL service framework

These three phases represent critical stages in IT service management: service operation focuses on the day-to-day management of IT services, service design addresses the planning and structuring of services to meet business needs, and service transition oversees the deployment of new or changed services.

Some of the key principles of this framework are as follows:

- **Service-oriented approach**: It focuses on minimizing disruption to IT services and ensuring their availability to users
- **Incident logging and categorization**: It establishes procedures for logging and classifying incidents based on severity and impact

- **Problem management**: It goes beyond incident resolution by identifying and addressing the root causes of incidents to prevent future occurrences
- **Continuous improvement**: It promotes an ongoing cycle of improvement for IT service management processes, including incident management
- **Defined roles and responsibilities**: It clearly outlines roles and responsibilities for personnel involved in incident management within the IT service desk

To learn more about the ITIL framework, you can go to `https://wiki.en.it-processmaps.com/index.php/Main_Page`.

ITIL is extensively used in large- and medium-sized organizations across various sectors, including finance, healthcare, telecommunications, and government, where managing IT services efficiently and ensuring service continuity are critical. It is particularly beneficial in environments with complex IT infrastructures and where service reliability and user satisfaction are paramount. For example, major banks and healthcare networks often adopt ITIL to standardize their incident and change management processes, ensuring minimal downtime for online transactions or patient record systems. Similarly, telecommunication providers use ITIL frameworks to maintain service availability, coordinate large-scale infrastructure changes, and enhance customer experience across their networks.

ITIL may *not* be as relevant in organizations with minimal IT infrastructure or those that do not heavily rely on IT services. For example, small manufacturing plants or local businesses that operate primarily with manual processes may find limited value in implementing ITIL. Similarly, non-technical service organizations, such as small consulting firms or retail outlets, may not require the full scope of ITIL practices. Additionally, small businesses with straightforward IT needs might find ITIL's processes too elaborate or resource-intensive. ITIL is also less applicable in highly specialized fields outside of IT service management, such as industrial control systems or cybersecurity, where frameworks such as NIST CSF or ICS are more appropriate for addressing specific risks and requirements.

SANS Institute IRF

This framework, developed by the **SysAdmin, Audit, Network, and Security (SANS)** Institute, is a popular choice for organizations of all sizes. It emphasizes a structured approach to incident response, focusing on preparation, identification, containment, eradication, recovery, and lessons learned. The SANS framework provides a strong foundation for handling security incidents and complements technical expertise with best practices for communication, documentation, and team management. *Figure 8.5* presents the SANS **Incident Response Framework (IRF)**, which outlines six key steps that guide organizations through the phases of incident response.

Figure 8.5 – SAN'S IRF

These steps include preparation, identification, containment, eradication, recovery, and lessons learned, providing a structured approach for managing cybersecurity incidents, ensuring a methodical response from initial detection through recovery and post-incident analysis.

The key principles are discussed in detail here:

- **Preparation**: It emphasizes the importance of proactive measures, such as establishing an incident response team, defining roles and responsibilities, and conducting regular training exercises
- **Identification**: It focuses on effectively detecting and identifying security incidents through various methods, such as log monitoring and user reports
- **Containment**: It provides guidance on isolating the incident to prevent further damage and minimize its scope
- **Eradication**: It offers best practices for eliminating the root cause of the security incident to prevent future attacks
- **Recovery and Lessons Learned**: It guides organizations in restoring affected systems and conducting a post-incident review to identify areas for improvement

The framework emphasizes a structured approach to incident response, focusing on the key principles in *Figure 8.5*.

To learn more about the SANS IRF, you can go to `https://www.sans.org/white-papers/33901/`.

The SANS IRF is widely adopted across sectors such as finance, healthcare, technology, and higher education, where rapid detection, containment, and recovery from cyber incidents are critical to maintaining trust and continuity. However, SANS IRF may be less applicable in environments with limited digital exposure or simpler IT operations, such as small service-oriented firms or commu-

nity organizations that rely on basic networks and cloud tools. In specialized domains like IACS or OT, where incidents often intersect with physical processes and safety systems, frameworks such as NIST CSF, ISA/IEC 62443, or ICS-specific incident management models are typically a better fit due to their focus on operational continuity and system resilience.

ICS4ICS

The **Incident Command System for Industrial Control Systems (ICS4ICS)** framework, developed by the **International Society of Automation's Global Cybersecurity Alliance (ISAGCA)**, is designed specifically to handle cybersecurity incidents affecting IACS. It builds on the established ICS principles while integrating best practices for **operational technology (OT)** security and incident response. ICS4ICS fosters collaboration between IT and OT teams during cyberattacks, enabling a unified and efficient response. *Figure 8.6* illustrates this framework, highlighting the integration of incident command, ICS security, and IT security to address the unique security challenges of industrial environments, ensuring a coordinated and comprehensive incident management approach.

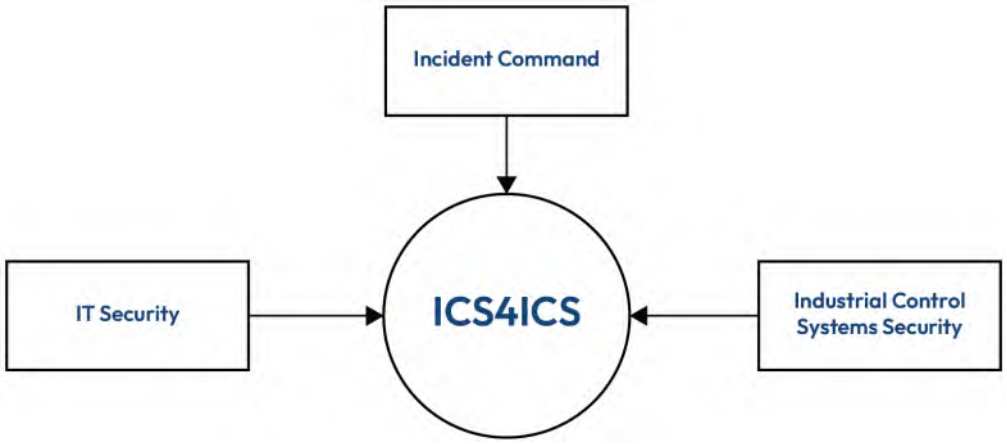


Figure 8.6 – ISAGCA's ICS4ICS framework

ICS4ICS specifically addresses cybersecurity incidents impacting ICS with the following core principles:

- **Leverages ICS structure**: It builds upon the existing ICS framework, utilizing its established command structure and standardized terminology for effective communication during an ICS4ICS response
- **OT security integration**: It integrates best practices for OT security into the incident response process, considering unique risks and vulnerabilities associated with industrial control systems

- **Public-private collaboration**: It acknowledges the importance of collaboration between public and private sector entities when responding to cyberattacks on CI
- **Phased approach**: It defines a phased approach to incident response, potentially including activities such as threat identification, impact assessment, system restoration, and post-incident review
- **Focus on business continuity**: It emphasizes the importance of minimizing disruption to critical industrial processes and ensuring business continuity during a cyberattack

To learn more about the ICS4ICS framework, you can go to `https://www.ics4ics.org/`.

ICS4ICS is predominantly used in sectors with significant industrial control systems, such as chemical manufacturing, oil and gas, and utilities. It is particularly valuable for organizations that need to address cybersecurity incidents while maintaining the continuity of critical industrial operations and ensuring effective coordination between different sectors.

ICS4ICS may be less applicable in organizations without industrial control systems or those where OT security is not a primary concern. Additionally, in environments where cybersecurity incidents do not impact industrial processes directly, such as general IT service management or small-scale IT operations, other frameworks such as NIST CSF or ITIL might be more suitable. In highly specialized, non-ICS domains, ICS4ICS might not address the unique challenges or regulatory requirements of those fields.

MITRE ATT&CK

As organizations mature in their understanding of cyber threats, it has become essential to have a common language that describes how attackers operate. The MITRE ATT&CK Framework fills this gap by offering a structured and globally recognized knowledge base of adversary tactics, techniques, and procedures. Unlike frameworks that focus on response governance, ATT&CK views incidents from the attacker's perspective and maps intrusions step by step across well-defined stages.

ATT&CK organizes adversary behavior into tactic categories such as **initial access**, **lateral movement**, **privilege escalation**, and **impact**. Each tactic contains techniques commonly used during real intrusions. For example, a ransomware event in a manufacturing plant may begin with a phishing email, followed by lateral movement using valid credentials, and finally, disruption of engineering workstations. Mapping these steps to ATT&CK helps responders understand the sequence of events, identify detection gaps, and anticipate what the attacker may attempt next.

This framework extends beyond traditional IT networks. The *ATT&CK for ICS* knowledge base focuses on OT and includes techniques that target PLC logic, safety functions, and industrial network components. This helps OT defenders visualize how sophisticated cyberattacks can affect control systems, physical processes, and operator actions. Many organizations combine ATT&CK with frameworks such as ICS4ICS to strengthen both situational awareness and response coordination.

Recent updates in ATT&CK v18, as shown in *Figure 8.7*, introduced expanded industrial asset objects, improved terminology alignment across sectors, and clearer distinctions between platforms and assets.

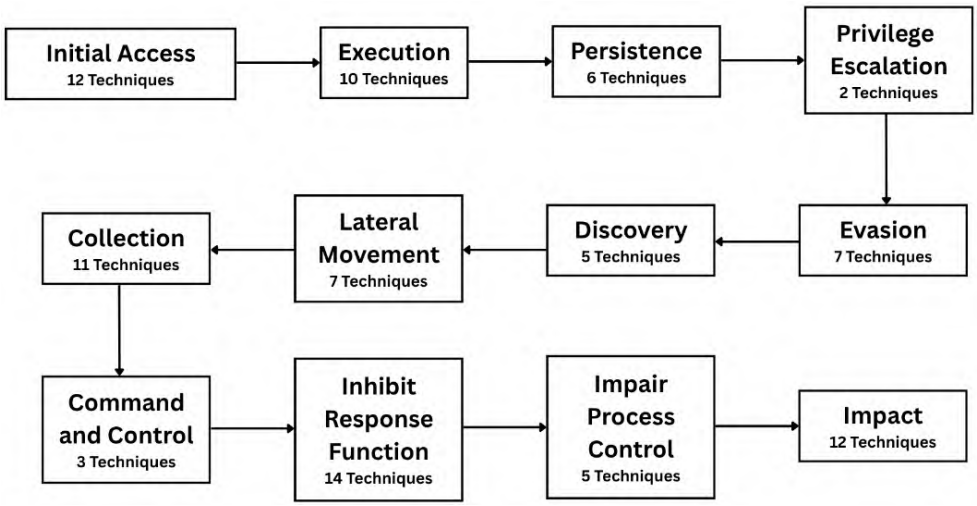


Figure 8.7 – Twelve IACS tactics and the corresponding number of techniques associated with each one

New device types, such as DCS controllers, industrial firewalls, and switches, now map directly to techniques that may affect them. The release also introduced a more structured detection model through detection strategies and analytics, giving defenders practical guidance on how to identify attacker behaviors. ATT&CK v18 further broadened coverage for enterprise, mobile, cloud, and containerized environments, reflecting the modern attack surface and supporting more comprehensive threat analysis

Future versions will continue refining technique organization, expanding IACS coverage, improving detection guidance, and evaluating how adversaries use emerging technologies such as AI. These ongoing enhancements, combined with community-driven governance, ensure that ATT&CK remains a practical and current resource for defenders across both IT and OT environments.

To learn more about the MITRE ATT&CK Framework, you can go to `https://attack.mitre.org`

Other frameworks

NIST **Special Publication (SP)** 800 61 remains one of the most widely used guides for building an effective incident response program. The latest revision, SP 800 61 Revision 3, updates the guidance significantly and aligns incident response with the NIST CSF 2.0. This version reinforces the idea that incident response is an enterprise responsibility that connects governance, risk management, communication, legal considerations, and operational recovery. It introduces clearer mappings between incident response activities and CSF 2.0 functions, provides updated expectations for coordination across technical and nontechnical stakeholders, and places greater emphasis on continuous improvement. The revision also modernises guidance to reflect today's hybrid environments, including cloud services, outsourced operations, and cyber-physical systems. These updates make SP 800 61 Revision 3 a valuable reference for organisations seeking a structured and scalable approach that connects technical response with business, safety, and regulatory requirements. For more information, you can visit `https://csrc.nist.gov/pubs/sp/800/61/r3/final`.

It is also worth mentioning the **Agile Incident Response for Industrial Control Systems (AIR4ICS)** because it represents one of the earliest attempts to capture the unique challenges of managing incidents in industrial control system environments. Developed through academic and industry collaboration, AIR4ICS applies Agile principles to ICS incident response, encouraging short iterative work cycles, rapid reassessment of conditions, and continuous collaboration between OT, IT, engineering, and security teams. The framework is notable for focusing on flexibility, process continuity, and real-time decision-making, which makes it especially useful in environments where physical processes cannot be interrupted and threats evolve quickly. For more information, you can visit `https://qmro.qmul.ac.uk/xmlui/handle/123456789/93044`.

Before concluding this chapter, it is important to step back and consider why choosing an appropriate incident management framework is so critical. Each framework we examined, from ICS and ICS4ICS to NIST CSF, SP 800 61, MITRE ATT&CK, ITIL, the SANS model, and emerging approaches such as AIR4ICS, offers a different perspective on how incidents unfold and how organizations should prepare, coordinate, and respond. Understanding these differences helps ensure that the framework you select aligns with your operational environment, regulatory responsibilities, and the specific challenges you face in both IT and OT systems.

Importance of choosing a framework

The choice of an incident management framework is not merely a procedural decision; it is a strategic choice that profoundly influences an organization's response capabilities, safety protocols, and overall resilience in the face of incidents. A framework well-aligned with the organization's

requirements, resources, and business needs ensures that response efforts are effective and sustainable in the long term. Here are the key factors that underline the importance of choosing the proper framework:

- **Performance and scalability**: A well-suited incident management framework is designed to optimize performance across various scales of operations. Organizations vary in size, complexity, and the nature of their operations, and the framework must be capable of scaling accordingly.

  Let's consider an example. A large energy company managing power grids across multiple states adopted the NIST CSF. This choice enabled them to scale their incident response from localized outages to large-scale disruptions caused by cyberattacks. The framework's modular approach allowed them to deploy targeted responses quickly, preventing minor incidents from escalating into widespread failures.

- **Flexibility, adaptability, and customization**: Organizations operate in diverse environments with unique challenges, making flexibility a crucial aspect of a practical incident management framework. A framework that allows for Customization can be adapted to the organization's specific needs, addressing unique risks and operational dynamics.

  For instance, let's say that an oil and gas company adopted the SANS Institute IRF, customizing it to address its specific operational risks, such as cyber threats targeting its industrial control systems. By tailoring the framework to its unique environment, the company ensured that its response protocols were well-suited to the critical nature of its operations, particularly in protecting against potential disruptions in the supply chain.

- **Community support and documentation**: The robustness of an incident management framework is often bolstered by the availability of community support and comprehensive documentation.

  Let's take an example. A mid-sized manufacturing company adopted the ICS4ICS framework, which benefits from an active global community and comprehensive documentation tailored to industrial control systems. This choice gave the company valuable peer support and practical implementation guides specific to their industry. The community-driven updates ensured they were always up-to-date with the latest security practices and emerging threats, allowing them to efficiently adapt the framework to their unique operational needs.

- **Safety and security considerations**: At its core, an incident management framework must prioritize safety and security. This includes the safety of personnel and the protection of critical infrastructure, data, and operations.

  Let's consider an example. A chemical processing plant adopted the ICS framework to enhance its response to safety incidents and cyber threats. The framework's emphasis on clear roles and responsibilities and its focus on maintaining safety during incident response allowed the company to effectively manage potential hazards while ensuring the protection of critical systems and processes.

- **Cost and resource availability**: Any organization must consider the cost of implementing and maintaining an incident management framework. This includes assessing in-house resources, the availability of mutual aid organizations, and geographical considerations.

  For example, an oil refinery in a remote area chose the ICS4ICS framework, considering its location's geographic challenges. The framework's focus on structured communication and coordination proved invaluable when external assistance was limited, and mutual aid organizations were far from the site. This allowed the refinery to effectively manage incidents using primarily in-house resources while maintaining a connection with external partners when possible.

- **Regulations and compliance requirements**: Regulatory compliance is a significant driver in selecting an incident management framework, especially in highly regulated industries such as chemical, oil and gas, and manufacturing.

  Let's consider an example. A manufacturing company operating in a highly regulated environment selected the NIST CSF to ensure compliance with industry regulations. By adopting this framework, the company ensured that all incident management activities were fully aligned with regulatory standards, reducing the risk of penalties and enhancing its ability to pass audits while maintaining a solid security posture.

When dealing with a highly specialized organization, selecting the right framework involves starting with a solid foundation and tailoring it to specific needs. ICS frameworks, like the beams and foundation of a house, provide essential structure and guidance for incident management. However, the way in which you decide to develop your incident response strategy—much like adding windows and doors to a house—is up to you. A good course of action could be to begin with a robust framework such as ICS4ICS for industrial control systems or NIST CSF for broader cybersecurity guidance, and then customize it based on your organization's unique requirements, risk profile, and operational environment. By integrating specialized practices and adapting the

framework to fit your specific context, you can ensure that your incident management approach is both comprehensive and effective, aligning with the unique challenges and demands of your specialized field.

Exercise: Choosing the right incident management framework for your organization

Objective: To help you evaluate multiple incident management frameworks and determine which one best fits your organization's needs, environment, and resources

Instructions:

- Read through the framework descriptions covered in this chapter (ICS, NIST CSF, NIST IRF, ITIL, SANS IRF, and ICS4ICS).
- Identify your organization's operational context and risk profile (see the following notes), such as manufacturing, utilities, healthcare, public services, and so on.
- Use the following worksheet to compare at least two frameworks based on factors such as scalability, relevance, cost, and regulatory fit.
- Conclude which framework or combination of frameworks is most suitable for your organization and why.

Category	**Framework 1**	**Framework 2**
Framework name		
Industry fit (is it suitable for your type of operations?)		
Scalability (can it adapt to both small and large incidents?)		
Flexibility (can it be customized for your organization's needs?)		
Community and support (is there documentation or a user community?)		
Regulatory alignment (does it meet your compliance needs?)		
Ease of implementation (how hard is it to adopt?)		
Resource requirements (does it need specialized training or large teams?)		
Safety and continuity focus (does it integrate safety and resilience?)		

Best suited for (e.g., OT operations, IT service management, or mixed environments)		
Notes or observations		
Final choice and reason		

Consider an example. You have a special sandwich that represents your asset, stored in a locked kitchen cabinet. The lock has a weakness, which is your vulnerability, and there is a sandwich thief who may try to steal it, which represents the threat. However, the kitchen is inside a building with round-the-clock security cameras. This means the likelihood of theft is low, but the impact of losing the sandwich might still be moderate because it has value to you.

By combining these two elements, likelihood and impact, on a grid, you can quickly visualize the level of risk. A situation with low likelihood and low impact might be acceptable, while one with high likelihood and high impact demands immediate attention.

Likelihood	**Impact**	**Risk level**
Unlikely and low	Low	Acceptable
Likely and moderate	Medium	Needs monitoring
High and significant	High	Requires mitigation
Very high and severe	Critical	Immediate action required

In cybersecurity and industrial operations, the same principle applies. A ransomware attack on a control network could have both a high likelihood and a severe impact, placing it in the red zone. A brief network delay on a non-critical system might have a low impact and a low likelihood, which would make it acceptable.

Example solution

Organization: City Water Utility

Operational context: Operates 3 water treatment plants and remote pumping stations serving 400,000 residents. Relies heavily on industrial control systems and remote monitoring.

Key stakeholders: State environmental agency, local government, and public customers.

Risk profile: High dependence on OT systems, increasing ransomware attempts, and strict public health regulations.

Conclusion: The utility company should prioritize frameworks that balance operational continuity and cyber resilience, such as ICS4ICS for structured incident response and NIST CSF for cybersecurity governance.

Category	**Framework 1: ICS4ICS**	**Framework 2: NIST CSF**
Framework name	ICS for Industrial Control Systems (ICS4ICS)	NIST Cybersecurity Framework (CSF) 2.0
Industry fit	Designed for industrial control and operational technology environments	Sector-agnostic, applicable to IT and OT systems
Scalability	Can be scaled from small plant incidents to multi-site coordination	Scales well from small organizations to national-level programs
Flexibility	Highly adaptable to industrial operations and OT incident response	Very flexible through customizable profiles and functions
Community and support	Backed by ISA's Global Cybersecurity Alliance, an active community, and case studies	Supported globally by NIST and industry groups; extensive guidance available
Regulatory alignment	Aligns well with **Maritime Transport Security Act (MTSA)** and chemical safety regulations	Meets federal and international cybersecurity requirements
Ease of implementation	Moderate; requires training in ICS command principles	High; easy to start with a baseline assessment
Resource requirements	Needs trained facilitators and cross-team coordination	Can be implemented with existing staff and external guidance
Safety and continuity focus	Strong focus on process safety, OT asset continuity, and coordination	Focus on cybersecurity resilience and business continuity
Best suited for	Chemical, manufacturing, energy, and utilities	Broad enterprises with IT and OT systems
Notes or observations	Ideal for organizations with physical processes and cross-sector dependencies	Excellent for defining cybersecurity strategy and maturity roadmap
Final choice and reason	**ICS4ICS**, supported by **NIST CSF**: ICS4ICS provides the operational structure, while CSF strengthens cybersecurity posture	

Summary

This chapter provided a broad view of the major incident management frameworks, including ICS, NIST CSF, NIST SP 800 61, MITRE ATT&CK, ITIL, the SANS model, ICS4ICS, and AIR4ICS, used across CI and enterprise environments. We explored how these frameworks create structure, clarity, and consistency during disruptive events by defining roles, processes, and documentation that support effective decision-making. Together, they show how incident management has evolved to address modern threats that span technical systems, physical processes, and complex organizational structures.

Selecting the right framework requires understanding how each model aligns with the realities of your organization. Performance, flexibility, community support, safety considerations, resource needs, regulatory expectations, and the nature of your operational environment all play an important role. A well-matched framework strengthens response capabilities, supports cross-functional coordination, and promotes long-term resilience. ICS continues to stand out as a foundational model for industries with complex operations, while frameworks such as NIST CSF and SP 800 61 provide strong cybersecurity governance and structured incident handling. MITRE ATT&CK enhances situational awareness by mapping adversary behaviors, and ICS4ICS and AIR4ICS extend these ideas into industrial control environments where process continuity and safety are essential.

Chapter 9 moves from theory into practice and focuses on training and exercises. Understanding a framework is important, but the real confidence and competence come from applying it through hands-on scenarios. By participating in drills and simulations, you will learn how teams communicate, coordinate, and make decisions under pressure. These exercises will help you develop the practical skills needed to respond effectively and build a stronger, more resilient incident management capability within your organization.

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

Part 4

Pillar 4 – Training, Exercises, and Continuous Improvement

Pillar 4 ensures that incident management capabilities are sustained, tested, and improved over time. Training and exercises transform plans and frameworks into practiced skills that function under real-world conditions.

This pillar focuses on designing, conducting, and evaluating exercises tailored for industrial environments, as well as scaling exercises from single facilities to multi-site organizations. It reinforces the idea that effective incident management is not a one-time effort, but a continuous process.

This part of the book includes the following chapters:

- *Chapter 9, Incident Command System Training and Exercises*
- *Chapter 10, Running an ICS Exercise*
- *Chapter 11, Optimizing Single-Site Exercises with Multi-Site Considerations*
- *Chapter 12, ICS Resources*

9

Incident Command System Training and Exercises

In this chapter, we will discuss different methods for using the **Incident Command System** (**ICS**) within an organization to train and practice managing cyber-related incidents in the context of CI. This includes handling cyber-induced incidents, dealing with security incidents, and working with the **Emergency Operations Center** (**EOC**), **Emergency Response Teams**, **Crisis Management Teams**, and the **Facility Security Officer**. We will also discuss ways to engage and collaborate with industrial control system personnel, crisis management teams, other relevant entities, and liaisons within the organization. The final pillar of incident management for CI, as shown in *Figure 9.1*, focuses on the hands-on **Training and Execution** (**T&E**) of ICS processes, actively supporting the development of robust incident response skills.

Figure 9.1 – Training and Execution as the fourth pillar of incident management for CI

This chapter offers a comprehensive overview of key training methods tailored to incidents involving **Industrial Automation Control Systems (IACS)**, including **Tabletop Exercises (TTXs)**, **drills**, **Functional Exercises (FEs)**, and **Full-Scale Exercises (FSEs)**. Each exercise method is explored for its unique strengths and limitations, allowing organizations to understand how each contributes to overall preparedness.

This chapter covers the following topics:

- Introduction to training and exercises
- Principles of effective incident management training for CI/OT environments
- Tailoring training and exercises
- Benefits and outcomes of effective training and exercises

Introduction to training and exercises

Effective training and exercises are fundamental in preparing personnel to respond to incidents involving CI. The unique blend of **operational technology (OT)** and **information technology (IT)** in ICS environments demands a structured approach to training. This section emphasizes the importance of a well-rounded training and exercise program in maintaining the integrity, availability, and security of ICS environments.

Note

To maximize effectiveness, organizations are encouraged to tailor their training and exercises to meet their specific needs, considering factors such as incident command size, complexity, risk level, budget, and available resources. By making informed decisions on exercise design, organizations can significantly strengthen their readiness to respond effectively to ICS incidents.

Providing training to employees involved in the day-to-day operations of CI organizations is crucial for ensuring swift and effective response during an incident. Trained employees possess a deep understanding of the operational environment and are well-equipped to identify anomalies, assess potential impacts, and take necessary actions to mitigate risks.

In CI sectors such as energy, water, and transportation, incidents, whether caused by cyberattacks, equipment failures, or natural disasters, can have severe consequences, potentially leading to widespread service disruptions, safety hazards, and economic loss. By equipping employees with the knowledge and skills to manage incidents, organizations can strengthen their overall resilience and ensure the continuity of operations.

Incident management training also enables employees to collaborate with specialized response teams, ensuring effective communication of critical information and efficient coordination of response efforts.

Additionally, understanding the importance of training is crucial. When humans face new or unfamiliar situations, they often freeze, either paralyzed by surprise, confusion, or panic and an inability to react—a reaction commonly referred to as being like a deer in the headlights.

Figure 9.2 – A deer frozen on a roadway, exemplifying the "deer in the headlights" effect

Similarly, during incidents in CI, untrained employees may become immobilized by the unexpected, highlighting the necessity for comprehensive incident management training. Training employees in incident management within CI organizations requires a multifaceted approach to ensure a comprehensive understanding of incident response. One essential method is experiential learning, or **learning by doing**, a concept historically known as **praxis** by the ancient Greeks. This approach is gaining renewed significance in CI and incident management as it enhances understanding by applying theoretical knowledge to real-world scenarios. Experiential learning fosters new ways of thinking and acting, which is crucial in CI environments where rapid and effective response is essential. Further, by integrating experiential learning with other training methods, organizations can significantly improve their personnel's ability to manage and mitigate incidents effectively.

We have established the importance of training for effective incident response; the types of training and exercises an organization chooses will depend on factors such as size, available budget, compliance requirements, and maturity level. Let's dive deeper into this in the next section.

Principles of effective incident management training for CI/OT environments

Effective training in industrial cybersecurity is not about checking boxes or completing annual compliance tasks. It is about preparing people to respond together when things go wrong. In CI and OT environments, incident management training serves as both a learning and a validation process. It helps teams understand what to do, how to collaborate under pressure, and how to apply both technical and procedural skills when it matters most.

In the next few sections, we will explore the principles behind designing and sustaining an effective training and exercise program. While attending external courses and industry workshops has value, true readiness comes from building and practicing within *your own environment*. Every facility, network, and team operates differently, and no generic course can fully replicate those conditions. Customizing training ensures that scenarios reflect your assets, dependencies, and operational risks. It also allows teams to grow together, learn from internal challenges, and mature their response capabilities over time. Developing a strong in-house training and exercise program transforms learning from an occasional event into an ongoing culture of preparedness. The following are some factors that make up an effective training program:

- **Clear purpose and contextual relevance**: Every training session should have a clear purpose that connects directly to the organization's operational and regulatory context. Whether it supports MTSA, NERC CIP, or TSA security requirements, or simply strengthens team readiness, participants must understand why the training matters. When people see how exercises relate to their real-world responsibilities, they engage more deeply and retain lessons that carry into daily operations.
- **Hands-on participation and scenario-based learning**: In an OT environment, learning by doing is essential. Simulations, TTXs, and role-based decision-making drills transform theory into muscle memory. These sessions allow participants to practice coordination, test procedures, and build confidence. It is not about achieving perfection but about learning to act decisively when systems fail or alarms sound.

- **Reinforcement through real-life case studies**: Training becomes powerful when it reflects reality. Reviewing actual incidents from manufacturing, energy, or transportation systems helps participants understand what worked, what failed, and how similar situations could occur in their own facilities. Real examples encourage meaningful discussions and deeper understanding.
- **Repetition of critical protocols**: Repetition builds discipline and consistency. Revisiting core processes such as escalation paths, communication flow, isolation strategies, and coordination with IT or emergency response helps participants internalize these actions. Each exercise should reinforce these fundamentals and gradually increase in complexity as team capability and maturity grow.
- **Testing and response drills**: A good training program evolves over time. It begins with discussion-based tabletop exercises, advances to functional drills that test coordination and timing, and eventually leads to FSEs that simulate real-life operational stress. Each stage enhances realism and pressure, helping the organization grow in maturity and confidence.
- **Active monitoring, mentorship, and collaboration**: Exercises are not just evaluations; they are opportunities for mentorship and growth. Facilitators, observers, and leaders play a vital role in guiding participants, identifying gaps, and encouraging open discussion. A *safe-to-fail* learning environment allows people to make mistakes and learn from them. Most importantly, training creates a shared platform for collaboration between IT, OT, and emergency response teams, helping bridge the gaps that often exist across departments.
- **Recognition and role validation**: Training should conclude with recognition and reflection. Acknowledging strong performance and highlighting effective teamwork reinforces accountability and motivation. Assigning defined roles such as Incident Commander, Communications Liaison, or Technical Specialist after the training helps validate what was learned and emphasizes the value of each function in an integrated response.

Developing a strong incident management capability requires consistent and structured practice. In CI and OT environments, training must move beyond theory and focus on real decision-making under pressure. Each step should strengthen coordination, communication, and overall readiness. Let us take a look at how the different types of training contribute to building maturity and confidence over time.

Classroom-based training/online or e-learning modules

This approach combines formal instruction, including lectures, presentations, and discussions, to provide foundational knowledge of incident management concepts, frameworks, and procedures with self-paced courses that allow employees to learn at their convenience. Courses often incorporate interactive elements such as quizzes and simulations, making them effective for introducing theoretical aspects and organizational protocols and ensuring consistent training standards across large organizations.

To achieve this, an organization can implement a structured training program that combines two methods. Formal instruction should be conducted periodically, such as quarterly or biannually, to cover essential concepts and updates. Self-paced courses can be offered continuously, allowing employees to access training as needed and fit it into their schedules. Hands-on testing is also crucial for reinforcing theoretical knowledge and ensuring that employees can apply what they've learned in real-world scenarios. Practical exercises build muscle memory and confidence, which are essential for effective incident response. Therefore, organizations should incorporate regular hands-on training sessions, such as simulations and drills, into their overall training strategy.

Organizations can obtain these types of training from specialized training providers, professional organizations, or consultants. ICS and OT Security consultants can offer tailored training solutions and hands-on workshops to address specific needs and scenarios within the organization. By leveraging these resources, organizations can develop a robust training program that enhances readiness and response capabilities.

Exercises

Exercises play a crucial role in preparing for and responding to incidents by providing practical simulations. They replicate different aspects of incident response, helping teams build confidence, test procedures, and improve coordination before facing a real incident.

Not all exercises are the same; each is tailored to serve a specific purpose. Organizations typically start with **TTXs**, where teams walk through scenarios in a low-pressure setting. Next are **Incident Response Drills** (**IRDs**), which focus on specific actions under pressure and without advance notice. From there, teams can advance to **FEs**, where larger portions of the response plan are carried out in real time. At the highest level are **FSEs**, which simulate real-world conditions with multiple teams and resources working together.

As shown in *Figure 9.3*, this progression allows organizations to start simple, refine their response strategies, and gradually move toward comprehensive, high-stakes simulations that validate the entire plan end to end.

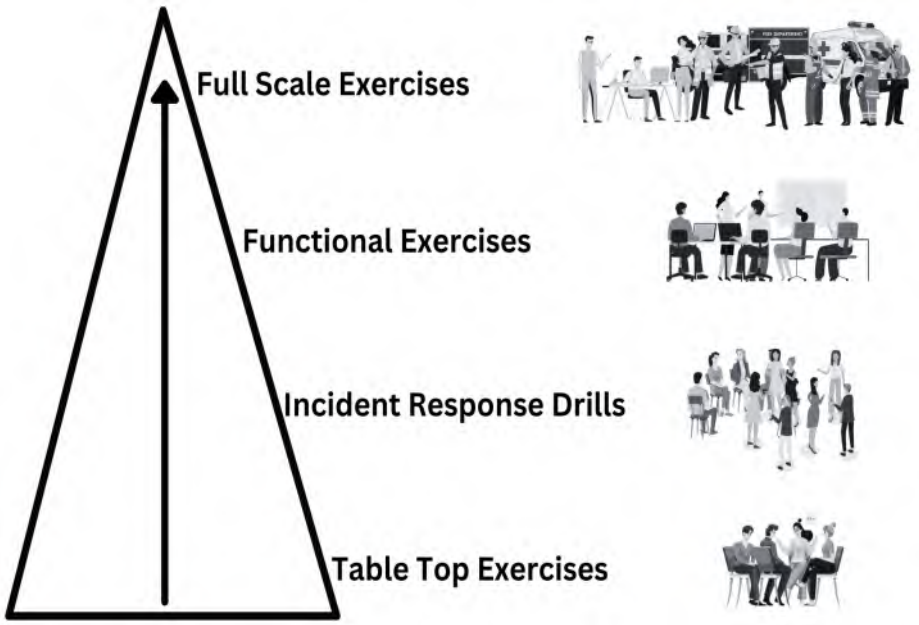


Figure 9.3 – Multiple types of exercises in ICS

Tabletop Exercises (TTXs)

TTXs are discussion-based sessions designed to walk team members through the response to a simulated incident in a low-stress environment. TTXs don't involve physical activity or the deployment of resources. Instead, participants gather around a table, either physically or virtually, to discuss the actions they would take in response to a hypothetical scenario. These exercises allow team members to explore their roles, engage in problem-solving, and enhance their understanding of the incident response plan.

Imagine a group of key personnel from an industrial facility, including automation engineers, IT security staff, and emergency responders, gathered around a conference table. A facilitator presents them with a scenario in which a cyberattack targets the facility's control systems, resulting in abnormal readings in critical equipment. The facilitator then leads the team through a series of questions: *How can they detect the attack?*; *Who leads the response?*; *What information is communicated to the wider organization?* As they discuss their actions, the team uncovers potential gaps in their procedures, such as unclear lines of communication or missing steps in the escalation process.

For instance, consider an auto manufacturing plant conducting a TTX focused on a simulated ransomware attack that locks operators out of critical control systems. During the exercise, team members may realize that while the IT team has protocols for network isolation, the OT team lacks a clear process for maintaining safe operations during a cybersecurity incident. This insight prompts them to revise their incident response plan, ensuring that both IT and OT teams are better prepared to coordinate in the event of a real attack.

Through these exercises, participants not only refine their response strategies but also develop the communication skills and confidence needed to effectively handle actual incidents.

Incident Response Drills (IRDs)

IRDs, often called **fire drills**, are structured activities that simulate specific aspects of an incident response, such as evacuation procedures or the deployment of emergency equipment. Unlike tabletop exercises, drills are conducted without warning to create a sense of urgency and realism. These drills allow employees to practice and refine their responses to particular scenarios, ensuring that each step is understood and executed efficiently under pressure.

An example could be an industrial facility where a simulated chemical leak is used to test evacuation procedures. The alarm is triggered without prior notice, and employees must immediately follow their emergency protocols. Operators quickly shut down critical processes, staff members don protective gear, and others move to designated assembly points. Emergency response teams deploy containment equipment and coordinate their efforts to manage the situation. Observers monitor the drill, noting any delays or confusion, such as unclear evacuation routes, which leads to further training and improvements.

IRDs can also be initiated as part of a cyberattack scenario. For instance, consider an automotive manufacturing plant where a simulated cyberattack triggers a series of emergency protocols. As the simulated attack unfolds, employees must execute incident response plans, such as isolating affected systems, communicating with IT and OT teams, and implementing recovery procedures. During the drill, any weaknesses in the response plan, such as slow decision-making or unclear communication channels, are identified and addressed.

By conducting these drills, employees gain practical experience in managing emergencies, building the confidence and skills needed to respond effectively in real-life situations, whether the incident is physical or cyber-related. These drills also provide valuable learning opportunities, keeping employees engaged and motivated to improve their response capabilities.

While drills test specific actions under pressure, functional exercises expand the scope by having teams carry out larger portions of the incident response plan in real time, connecting processes and coordination across functions.

Functional Exercises (FEs)

FEs go beyond discussion and bring in hands-on response activities, but still within a controlled scope. Unlike tabletop exercises, where the focus is on talking through scenarios, FEs require teams to actively carry out parts of the incident response plan in real time. They are designed to test specific functions, processes, or coordination points without the full complexity of a live simulation.

For example, a manufacturing facility may run an FE to practice isolating an infected OT network segment after a simulated ransomware attack. The IT and OT teams would execute their technical steps, system isolation, communication protocols, and initial recovery while observers evaluate timing, decision-making, and adherence to procedures. FEs are especially useful for validating escalation paths, testing technical capabilities, and giving staff the opportunity to practice their roles under some pressure but without the scale or resource demands of an FSE. They act as the bridge between low-stakes tabletop discussions and high-stakes full-scale simulations.

Once teams are confident in functional exercises, the next step is a full-scale exercise where the entire response plan is tested under realistic, high-pressure conditions that closely resemble an actual incident

Full-Scale Exercises (FSEs)

FSEs are the closest you can get to a real incident without the actual crisis. They bring together multiple teams, systems, and resources in real time, simulating every stage of an incident, from detection to recovery. The goal is to stress-test the entire response plan under conditions that mirror the complexity and pressure of an actual event.

For example, an automotive plant running an FSE could combine a ransomware attack with a fire on the assembly line. While IT teams work to contain the cyber threat and restore systems, emergency responders must evacuate personnel and manage the fire. This type of exercise exposes how well communication flows, whether resources are allocated effectively, and how smoothly IT, OT, and safety teams integrate their actions.

FSEs provide the highest level of realism and reveal how well teams perform under real pressure. They expose strengths, uncover gaps, and validate how effectively an organization can manage a complex incident from start to finish. For those already experienced with tabletop and functional exercises, full-scale exercises are the next step toward true operational maturity.

Not every organization needs the same level of intensity or scale. The real value lies in tailoring training and exercises to match the organization's size, risk profile, and operational environment. In the next section, we will look at how to design and adapt training programs that fit your specific needs and maturity level.

Tailoring training and exercises

Training and exercises work best when they are tailored to the realities of the relevant CI sector. The risks in chemical manufacturing, power generation, or transportation are not identical; some face OT-focused cyberattacks, others supply chain vulnerabilities, and others environmental hazards. Customization ensures that the scenarios used in exercises match the actual challenges organizations are likely to face, whether that's a cyberattack on control systems, a physical security breach, or a hazardous material release.

For example, a chemical plant might run an exercise around a cyberattack that disables safety systems, simulating how teams would prevent a toxic release. A smaller water utility, on the other hand, might focus on a simpler but just as disruptive scenario, such as a ransomware attack that locks operators out of remote pumps. Both cases show the importance of designing exercises that are relevant and actionable for the specific environment.

Tailoring also applies to roles. OT personnel need focused training on securing and responding to incidents that affect industrial control systems, while managers may need more emphasis on business continuity, safety compliance, and communication with regulators or external partners. This role-specific approach ensures everyone knows where they fit, from spotting the first signs of a problem to restoring operations.

Finally, as threats evolve, so should training. New cyber-physical risks, supply chain pressures, and attack techniques are constantly emerging. By keeping exercises current and role-specific, organizations build teams that are adaptable, confident, and capable of protecting critical operations even under changing conditions.

Choosing the right training and exercise methods

Selecting the right mix of training and exercises is not about using every format at once. It is about building capability in a deliberate and realistic way. Organizations should start simple and progress toward more complex scenarios as their maturity, resources, and risk profile evolve.

In the early stages, TTXs help teams practice decision-making and communication in a controlled setting. As the program develops, short and focused drills can be scheduled throughout the year to test specific actions such as isolating a compromised workstation, switching to backup control, or verifying escalation procedures. FEs usually occur once or twice a year, connecting multiple teams to simulate an active incident in real time. FSEs, because of the intense planning, coordination, and cost involved, may take place once every two years and serve as the ultimate validation of the organization's readiness.

To illustrate, consider two facilities that began developing their programs at the same time. The first started with a few tabletop sessions that reflected its actual operations. Over time, it added targeted drills each quarter and a single FE at the end of the year. When a real cyber event occurred, the team responded calmly and effectively, following procedures that had been repeatedly practiced before.

The second facility tried to jump directly into a large-scale exercise without establishing a foundation of smaller sessions, thus skipping practicing habits and understanding. Teams were unclear about their roles, communication broke down, and key steps were missed. The exercise revealed that without consistent and progressive training, even the most elaborate scenarios fall apart.

The lesson is that *progression should match readiness and resources*. Some organizations may focus more on TTXs and drills, while others can move quickly into functional or full-scale scenarios. What matters is choosing the methods that best fit the environment, risks, and operational complexity. Role-based training remains vital throughout, ensuring that every participant understands their part and can act with confidence when a real incident occurs.

In short, a strong program evolves over time. Multiple small drills keep skills sharp, annual exercises test coordination, and periodic full-scale events prove the organization's ability to manage real crises. Together, they create a culture of preparedness and continuous improvement across the entire operation.

Tip

As you plan your own program, consider the following questions: What scenarios could cause the greatest disruption? How quickly should your teams detect, contain, and recover? Which roles need the most practice? And most importantly, how will you use each exercise to refine your response plan?

The following are some of the practical points to keep in mind when designing and scheduling exercises. These suggestions can help you balance ambition with realism and ensure that every session adds measurable value to your organization's readiness.

- Plan an annual cycle with a mix of small drills, one or two tabletop discussions, and at least one FE.
- Reserve FSEs for major milestones, significant system changes, or after-action validation of large initiatives
- Document every session and review outcomes to track maturity growth over time
- Rotate facilitators and participants to develop depth across teams and prevent dependency on a single expert
- Include external stakeholders such as vendors, contractors, or emergency responders whenever possible to strengthen coordination beyond your own walls
- Keep scenarios fresh by rotating focus areas such as network compromise, safety system disruption, or vendor access misuse

Exercise 1: A thought experiment – running a drill and a functional exercise for a water utility

Step 1: Conduct a drill (targeted, short, action-focused)

Objective: Describe the single action or response you want to test.

Example: Test whether operators and IT/OT teams can quickly recognize and respond to a ransomware lockout on remote pumps.

Scenario context: Provide a short summary of the simulated situation, including what systems or processes are affected.

Example: A ransomware attack locks operators out of remote pumps at a water utility, disrupting control and threatening service delivery, public health, and regulatory compliance. Operators must coordinate with IT and OT teams to restore control.

Instructions:

- Identify one key process or skill to test
- Decide whether the drill will be announced or unannounced
- Determine how the scenario will be triggered (simulated alert, pop-up message, system notification, etc.)

- Assign observers or facilitators to record timing and decisions
- Plan a short debrief immediately afterward to capture lessons learned

Exercise 2: Conduct a functional exercise (broader, coordinated, real-time)

Objective: Define what coordination or multi-team process you are validating

Example: Validate coordination between operations, IT/OT security, management, and external partners during a ransomware incident

Scenario context: Describe how the scenario expands on the earlier drill.

Example: Building on the earlier ransomware scenario, the attack spreads across multiple remote sites, disrupting pump controls and limiting system visibility. Operations, IT, OT, and management must coordinate to contain the threat and maintain service continuity.

Instructions:

- Use outcomes from the drill to shape this larger exercise
- Activate multiple response teams in real time
- Introduce timed injects to simulate evolving conditions
- Engage leadership in decision-making and external communication
- End with a "hot wash" discussion to gather lessons learned

Please see the following for an example and some tips on how you can run these two exercises.

Example: Water utility ransomware

Scenario context: A mid-sized water utility detects a ransomware attack that locks operators out of remote pump controls. The simulated incident affects multiple stations responsible for water distribution. Operators cannot adjust flow remotely and must coordinate with IT/OT security teams to isolate infected systems and maintain service manually. The event threatens service continuity, regulatory reporting deadlines, and public confidence.

Exercise 3: Drill example

Objective: Test the operator's ability to identify a ransomware lockout and escalate the issue correctly.

Execution: A facilitator displays a simulated ransomware screen on the operator's workstation without prior notice. Operators follow existing playbooks by alerting supervisors, isolating the workstation, and contacting IT/OT support. Observers record actions and response times.

Evaluation:

- Did the operator recognize the incident quickly?
- Was escalation immediate and clear?
- Were backup systems or manual controls used correctly?
- What went well? What went wrong?

Duration: 25 minutes

Outcome: Identified unclear escalation channels between OT and IT and the need for clearer backup control instructions.

Exercise 4: Functional exercise example

Objective: Validate how operations, IT, OT, and leadership coordinate during a multi-site ransomware event.

Execution: Facilitators expand the scenario by simulating ransomware spreading to additional remote sites. Teams activate incident response procedures in real time, using actual communication channels. Injects include system alerts, missing configuration data, and media pressure for updates.

Evaluation:

Operational readiness

- Did operators immediately recognize the issue and take initial containment steps?
- Were manual control procedures or local overrides activated correctly?
- Was there any delay in isolating affected systems or switching to backups?
- Did the team have access to the correct documentation or playbooks during the response?

Coordination and communication

- How quickly were IT, OT, and operations teams able to connect and share situational awareness?
- Were communication channels (radio, phone, messaging, or incident management systems) effective under stress?
- Did each team understand who was leading the response at each stage?

- Were updates provided to leadership at appropriate intervals?
- Was there a single, clear communication line to external stakeholders or regulators?

Leadership and decision-making

- How well did leadership balance operational priorities with public and regulatory obligations?
- Were decisions about vendor access, media engagement, and notifications made using defined criteria or ad hoc judgment?
- Did leadership have enough technical insight to make informed choices, or did they rely solely on team inputs?

Technical containment and recovery

- Were infected systems correctly isolated without disrupting unaffected assets?
- Was forensic data collected for analysis, or was the focus solely on recovery?
- Did backups restore successfully, and were they validated before being placed online?
- Were lessons from the initial drill applied effectively to this broader scenario?

Resource and capability gaps

- Were any critical roles unfilled or unclear during the exercise?
- Did staff have the necessary access rights, credentials, and tools to perform their tasks?
- Were external partners or vendors contacted promptly and appropriately?

After-action reflection

- What parts of the response plan worked as intended?
- What specific steps caused confusion or delay?
- What new procedures or training topics emerged from this exercise?
- How can the organization better integrate OT operations, IT security, and emergency management in future exercises?

Duration: 3 hours

Outcome: Teams validated their communication flow, identified resource constraints, and recommended cross-training between operations and IT for better coordination.

Summary

Effective training and exercises are the backbone of a resilient incident response program. They do more than test procedures; they uncover weaknesses, build confidence, and foster a culture of continuous learning. For CI, the benefits include faster, more efficient responses, stronger coordination across teams, clearer role execution, compliance alignment, and a cycle of continuous improvement.

This chapter outlined the progression of exercises from **Tabletop Exercises (TTXs)** that build understanding, to **Incident Response Drills (IRDs)** that test specific actions, to **Functional Exercises (FEs)** and **Full-Scale Exercises (FSEs)** that validate full response plans under realistic conditions. Choosing the right mix, tailored to organizational maturity and sector risks, ensures training remains practical and impactful.

In *Chapter 10*, we will prepare and run our first incident management exercise, building on FEMA's Incident Command System and adapting it to the unique challenges of industrial control systems, and creating tailored exercises that drive real preparedness.

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

10

Running an ICS Exercise

Industrial Automation and Control Systems (IACS) environments present unique challenges when managing cybersecurity incidents and planning preparedness exercises. The **Incident Command System (ICS)** framework, developed by FEMA, provides a strong foundation for coordinating response and recovery. However, its direct application to IACS and **Operational Technology (OT)** settings often requires thoughtful adaptation.

In this chapter, we explore how organizations can leverage the core principles of the ICS while integrating specialized frameworks such as the SANS incident response methodology and other sector-specific standards to build a resilient and coordinated response posture. Additionally, we will look at how to build a structured exercise program that strengthens these capabilities through systematic planning, execution, and continuous improvement.

This chapter also includes a case study showing how ICS principles were applied during an exercise, highlighting the benefits and challenges of adapting standardized command structures to real-world industrial environments.

By the end, you will understand how to apply these frameworks effectively and tailor them to your organization's size, culture, and operational needs for a practical and scalable incident management approach.

The following main topics are covered:

- Building a continuous improvement program
- Program management and governance
- Exercise planning and design

- Scenario planning
- Execution and facilitation of an exercise
- Improvement and integration
- Case study: Running an IACS/ ICS exercise

Building a continuous improvement program

Many organizations today face increased regulatory pressure and rising expectations for internal compliance. Yet preparedness exercises themselves are not a new concept. Industrial and critical infrastructure facilities have been conducting safety and emergency drills for decades, often in coordination with local agencies, mutual aid groups, or third-party responders.

The purpose has always been consistent: to test readiness and improve response capability. During these exercises, teams ask practical questions such as the following:

- How effectively do we communicate during an incident, and where do gaps exist?
- Where are our critical resources and spare parts stored?
- Who are the key contacts for different scenarios, especially after hours or on weekends?
- How do we coordinate across departments and facilities?
- Which communication channels or radio systems are most reliable?

While tabletop exercises often provide valuable insights into communication flow and planning gaps, they remain discussion based. When the objective shifts from reviewing procedures to validating actual systems, configurations, or workflows, a more immersive approach becomes necessary. Complex scenarios such as testing a network segmentation policy, validating control system failover, or simulating a ransomware attack on operational networks require a functional exercise environment that mirrors real conditions.

For example, during a cyberattack simulation, the incident management team might not only discuss containment procedures but also execute a script to reconfigure VLANs or firewall rules within a controlled IACS test environment. This hands-on validation assesses whether the response plan functions as intended under operational stress, revealing hidden dependencies, timing issues, and human factors that tabletop discussions alone may overlook.

As organizations mature in their incident management and IACS security programs, their approach to exercises evolves as well. What begins as isolated drills can transform into structured programs that are repeatable and measurable programs focused on continuous improvement and organizational resilience.

Whether you are developing a new exercise program or refining an existing one, the foundational elements are similar. *Figure 10.1* illustrates the key components that make up an effective ICS exercise program.

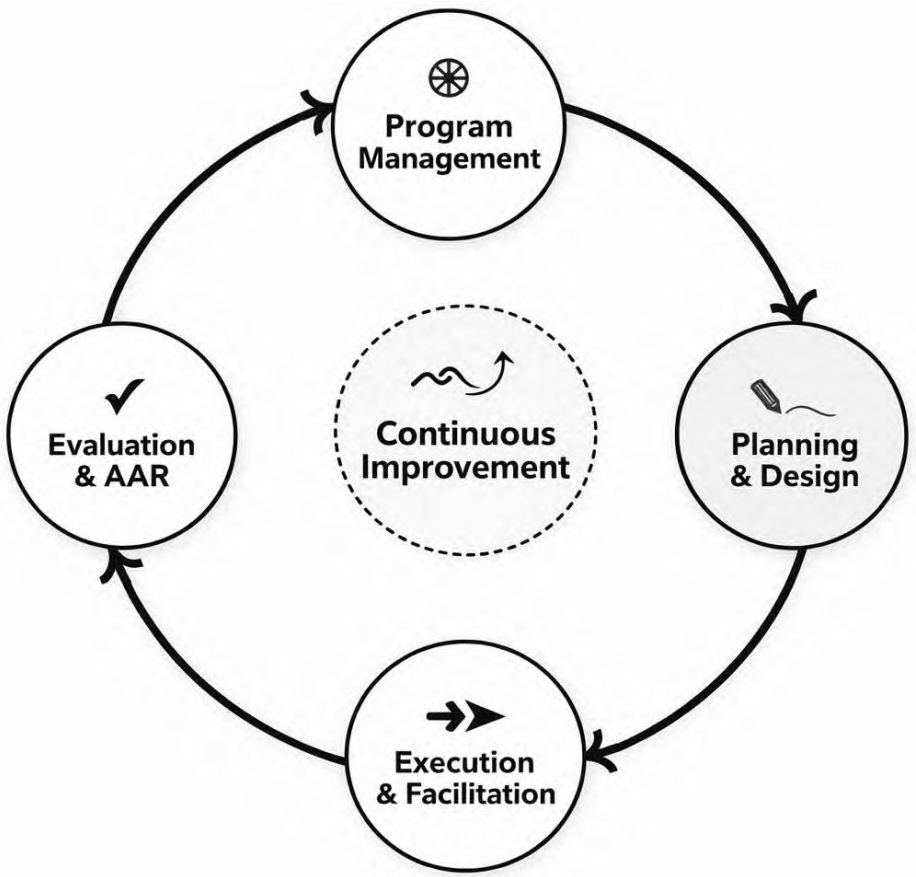


Figure 10.1: ICS exercise program cycle

At its center is continuous improvement supported by program management, planning, execution, evaluation, and integration. These components can be expanded as follows:

- **Program management and governance**: Establish ownership, leadership support, and oversight to ensure accountability, documentation, and continuous improvement
- **Exercise planning and design:** Define objectives, create realistic scenarios, and choose the right exercise type
- **Execution and facilitation:** Conduct the exercise using timelines, injects, and standard ICS documentation

- **Evaluation and After-Action Review:** Capture lessons learned and document strengths and gaps
- **Improvement and integration:** Apply findings to improve plans, procedures, and future exercises

Now that we've introduced the essential components that form an ICS exercise program, it's time to look more closely at how each one works in practice. Each element plays a specific role in shaping an organization's overall readiness. We'll begin with program management and governance, which serves as the foundation that supports every other phase of the exercise lifecycle.

Program management and governance

Strong program management forms the foundation of a lasting exercise strategy. It ensures exercises are planned, repeatable, and aligned with the organization's risk profile and operational priorities.

Every facility is different in culture, size, and maturity. The key is to build a program that fits the environment, practical enough to sustain yet structured enough to demonstrate measurable progress.

Leadership commitment and ownership

In most industries, every new project begins with management approval. The same applies here. An exercise program succeeds only when leadership visibly supports it. Their involvement provides direction, resources, and legitimacy.

Position the program as a strategic enabler rather than a compliance activity. Executives respond better when they see how exercises reduce operational risk, improve recovery time, and meet regulatory expectations. Connecting the program to familiar outcomes such as safety, reliability, and compliance helps sustain engagement.

For example, a one-hour network isolation drill each quarter can reduce mean time to recovery by 30 percent. Similarly, a joint IACS and IT tabletop exercise supports ISO 27001 and ISA/IEC 62443 compliance goals.

Leaders should also be encouraged to participate directly by opening or closing an exercise or attending the debrief. Their presence reinforces organizational commitment and shows that preparedness is a shared responsibility.

Formalize that commitment by assigning a program sponsor who approves the annual exercise calendar, allocates resources, and reviews outcomes during safety or EHS meetings.

While the financial investment required to conduct exercises is often minimal, the true cost lies in the time commitment and consistency of participation. To demonstrate value and sustain organizational support, exercise programs should define and track clear performance measures. These measures may include indicators such as incident detection time, escalation speed, and the effectiveness of cross-functional coordination.

For example, an organization may track average incident response time across successive exercises and compare results over time. In one such program, this approach showed a reduction in response time from approximately 40 minutes to 22 minutes, alongside a 60-percent decrease in audit findings related to coordination gaps. Using objective metrics in this way helps translate exercise participation into demonstrable operational improvement.

Program structure and documentation

Establishing a sustainable exercise program requires clear ownership and structure. Organizations should designate a program coordinator or exercise manager with a working understanding of both IACS and IT operations. In many environments, this responsibility can be embedded within an existing function, such as the Safety or Physical Security team, particularly where those groups already manage drills, audits, or regulatory exercises. Regardless of where the role resides, the coordinator serves as the connective link across departments, aligning technical teams, operations, and leadership.

This role is responsible for managing exercise logistics, scheduling, documentation, and follow-up. Developing an internal charter that defines the scope, frequency, and objectives of the exercise program helps formalize expectations and maintain consistency over time. For each exercise, organizations should retain detailed records, including agendas, injects, participant sign-ins, after-action reports, and improvement logs. These artifacts not only support compliance and audit needs but also provide critical reference points for future planning and maturity tracking.

Most importantly, exercises should be treated as a continuous learning cycle rather than isolated events. Each iteration should follow a deliberate progression of planning, execution, evaluation, and improvement. Lessons learned must be systematically fed back into incident response plans, procedures, and training materials so that every exercise incrementally strengthens the organization's resilience and readiness.

To keep the program sustainable, maintain an exercise register, a centralized log or SharePoint list that tracks all exercises, their objectives, dates, key findings, and corrective action status. This simple yet powerful tool provides visibility into organizational progress and helps ensure accountability for follow-up actions.

With governance established, the next step is to design exercises that are purposeful, realistic, and aligned with organizational priorities.

Exercise planning and design

The planning and design phase transforms intent into a structured, goal-oriented exercise. This phase defines what will be tested, why it matters, and how success will be measured.

Some of the key activities of exercise planning and design include the following:

- Defining clear objectives
- Determining the exercise type
- Regulatory considerations
- Developing a repeatable process
- Annual planning and scheduling
- Scenario planning

These are discussed in detail next.

Defining clear objectives

Exercise objectives should be specific and measurable. Whether testing escalation protocols, communication flow, or technical response actions, objectives must be clearly articulated and aligned with organizational priorities.

The **SMART** framework, which stands for **Specific, Measurable, Achievable, Relevant, and Time-bound**, provides a practical method for defining effective objectives. Applying this approach ensures exercises produce actionable outcomes rather than vague observations.

The SMART goal-setting method was first introduced by George T. Doran in 1981 in *There's a S.M.A.R.T. Way to Write Management's Goals and Objectives*, published in *Management Review*. It remains one of the most effective frameworks for creating clear, measurable, and actionable objectives in organizational planning and exercises.

The SMART framework provides a structured approach for defining effective exercise objectives. Each objective should be Specific, clearly outlining what needs to be achieved and by whom; Measurable, with defined criteria to assess progress or success; Achievable, ensuring it is realistic within available resources and constraints; Relevant, aligning with the organization's priorities and overall mission; and Time-bound, setting a clear deadline or timeframe for completion. Applying the SMART approach ensures that exercise goals are focused, actionable, and capable of producing measurable outcomes that drive continuous improvement in incident preparedness and response.

Determine the exercise type

Select the right format based on maturity and available resources. Options include the following:

- **Tabletop Exercise (TTX)**: Discussion-based, ideal for evaluating plans and communication.
- **Functional Exercise (FE)**: Hands-on, simulates real operations using systems and data.
- **Full-Scale Exercise (FSE)**: Involves physical deployment of personnel and resources.
- **Incident Response Drill (IRD)**: Short, focused drills to validate specific response actions or technical controls. (See *Chapter 9* for a detailed discussion of IRDs.)

The choice of exercise type depends largely on the organization's maturity level and previous experience conducting exercises. As discussed in *Chapter 9*, organizations that are new to structured incident management programs should begin with TTXs, which focus on discussion-based scenarios and decision-making in a low-risk environment. As the organization matures, it can progress to FEs, which test systems, roles, and coordination in real time, and eventually to FSEs, which simulate realistic conditions across multiple departments and agencies. This phased approach allows teams to build confidence, validate procedures, and strengthen cross-functional coordination before engaging in more complex, resource-intensive exercises.

Regulatory considerations

Exercise planning must account for applicable regulations. For example, U.S. Coast Guard regulations mandate periodic security and cybersecurity drills and exercises for regulated facilities

(https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-105/subpart-B/section-105.220). Incorporating regulatory requirements into the exercise calendar ensures compliance while reinforcing preparedness goals.

Under United States Coast Guard regulation 33 CFR § 101.635, for MTSA-regulated facilities, owners/operators must conduct at least two cybersecurity drills each calendar year and at least one cybersecurity exercise per year (with no more than 18 months between): https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F/section-101.635

Including regulations in your planning ensures your exercise calendar meets external obligations while aligning with internal preparedness goals.

Develop a repeatable process

Exercises should follow a consistent process to avoid becoming one-off events. Planning, standardization, and feedback integration are essential for building a program that matures over time.

For example, an organization may establish a standard exercise lifecycle in which each exercise defines objectives, uses a common scenario and inject format, captures actions through standardized documentation, and tracks corrective actions in a centralized improvement log. Using the same structure across exercises allows progress to be measured, results to be compared, and response capabilities to improve over time.

In smaller organizations, the process may be simpler. A single coordinator may lead quarterly tabletop exercises using a consistent agenda, a short scenario outline, and a basic after-action worksheet. Each session can focus on one or two decision points, such as escalation or vendor notification, with notes captured and reviewed at the conclusion of the exercise. Repeating this lightweight approach builds familiarity and helps identify recurring gaps without significant overhead.

Once a repeatable process is in place, it can be applied across an annual cycle. Annual planning and scheduling help sequence exercises, manage complexity, and ensure lessons learned from one exercise inform the next.

Annual planning and scheduling

Building an annual exercise calendar is essential for creating a structured, repeatable program. This calendar should outline the types of exercises, their objectives, and the resources required. Start with TTXs in the early stages to build familiarity and confidence, then gradually incorporate FEs and, eventually, FSEs as the program matures.

The following shows an example annual schedule:

- Q1: TTX focused on communication and escalation workflows
- Q3: Functional exercise validating network segmentation procedures
- Year-End: Multi-team full-scale exercise simulating a ransomware event

Planning can be annual, semi-annual, or quarterly, depending on organizational needs, regulatory requirements, and available resources. Whether you manage your schedule using Microsoft Outlook, a shared Teams or Google Calendar, or a simple spreadsheet, the key is to ensure that all stakeholders are informed and aligned well in advance.

Table 10.1 provides a structured view of an annual exercise schedule, ensuring planning is consistent and transparent.

Quarter	**Exercise Type**	**Objective**	**Key Participants**	**Resources Needed**
Q1 (Jan – Mar)	Tabletop Exercise (TTX)	Test communication and escalation workflows.	IACS team, IT, operations leads, site managers.	Meeting room, scenario slides, facilitator, notetaker.
Q2 (Apr – Jun)	Tabletop Exercise (TTX) (Optional for smaller orgs)	Validate incident response playbooks for detection and analysis.	Cybersecurity, compliance, external consultants (if needed).	Updated IRPs, templates, lessons learned from Q1.
Q3 (Jul – Sep)	Functional Exercise (FE)	Validate network segmentation and response procedures in a live environment.	IACS engineers, network admins, security analysts.	Test lab environment, scripts, monitoring tools, checklist.
Q4 (Oct – Dec)	Full-Scale Exercise (FSE)	Simulate multi-site ransomware attack; test multi-team coordination.	Executive leadership, IACS/IT teams, comms, vendors, regulators.	War room setup, simulation tools, external observers.

Table 10.1: Sample annual exercise calendar

By mapping exercises by quarter, type, objective, participants, and required resources, organizations can better coordinate across teams, allocate resources efficiently, and track progress toward a mature and repeatable exercise program. It also helps stakeholders visualize the balance between tabletop, functional, and full-scale exercises throughout the year.

Scenario development is where planning becomes practical, allowing teams to test communication, coordination, and technical response in a realistic but controlled setting. Regardless of the exercise type, this step is critical and stands on its own because it defines how participants will experience and engage with the event. In the next section, we explore how to design scenarios that are both realistic and relevant to your organization's environment.

Participation drives success. Confirm the availability of everyone involved, from technical responders to leadership, to ensure the exercise provides meaningful, actionable insights. Without full participation, the effectiveness of the exercise is significantly reduced.

Scenario planning

Scenario planning defines how participants experience the exercise. Effective scenarios are realistic, relevant, and designed to test decision-making, communication, and coordination.

Scenario development typically begins with pre-planning meetings involving representatives from operations, IACS, IT, safety, and communications. These discussions help identify risks, align learning objectives, and ensure scenarios reflect real-world conditions.

Building a scenario involves defining the core event, identifying impacts, establishing a timeline, creating injects, defining expected actions, and preparing supporting materials. This structured approach ensures scenarios remain focused while providing enough complexity to challenge participants.

Customize scenarios to reflect your organization's environment, processes, and technology stack. Generic scripts rarely engage participants or test real operational conditions.

In the next section, we will look at how to build a scenario step by step, using examples that illustrate how a simple concept can evolve into a structured, realistic, and effective exercise.

Building the scenario

Once the scenario planning team has agreed on the focus and learning objectives, the next step is to build the scenario itself. This is where ideas are turned into a structured storyline that guides the flow of the exercise. A strong scenario should be realistic, encourage critical decision-making, and test communication and coordination under pressure.

Figure 10.2 illustrates the six-step process used to develop effective scenarios.

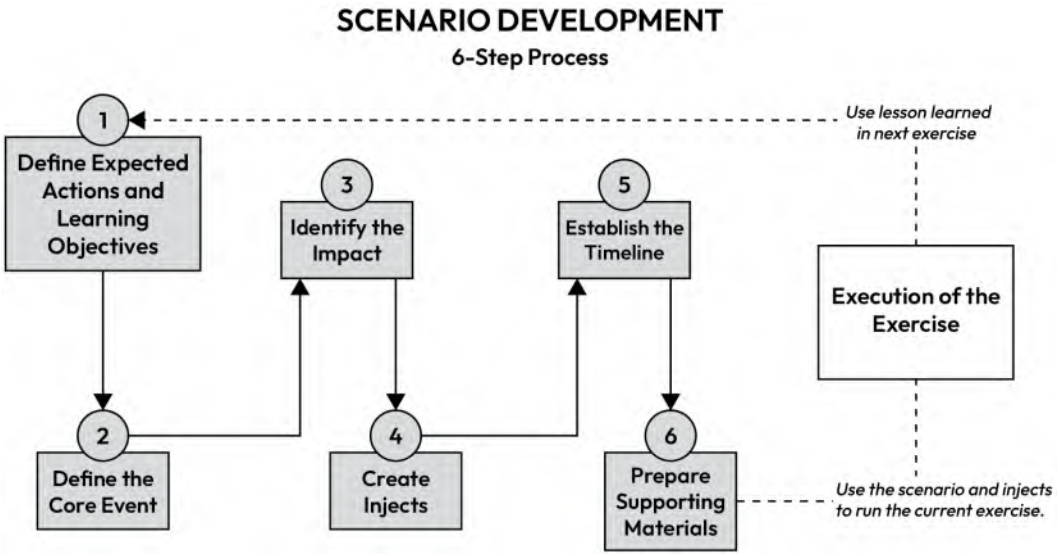


Figure 10.2: The cyclic scenario development process

This process focuses on identifying key drivers and uncertainties, building realistic situations around them, analyzing potential outcomes, and developing strategies for response. Scenario planning is a continuous process that should be revisited and refined as new lessons are learned and operational conditions evolve.

The following section explains each of the six steps in detail, outlining how they connect to one another and how each contributes to creating a realistic and effective exercise scenario.

Step 1: Define the core event

Start with a simple but critical question: What event are we trying to simulate? This could be a cyber incident, an equipment failure, a power disruption, or a combined scenario that links multiple risks together. The event should align with your organization's key vulnerabilities or operational priorities.

During this step, it helps to ask guiding questions such as: What systems are critical to operations? Which failures would have the highest impact? Who would need to respond first? These questions help narrow the focus to scenarios that will produce meaningful insights rather than theoretical discussions.

Example: A **programmable logic controller (PLC)** begins to behave erratically after a firmware update, causing unexpected valve movements in a mixing process and raising safety alarms.

Step 2: Identify the impact

Once the core event is defined, identify how it affects your organization's operations, safety, communications, and overall business continuity. Impacts can vary widely — from localized system disruptions to cascading failures that affect entire production lines, logistics, or even downstream customers.

Consider the broader implications as well. For example, if the organization is part of a larger supply chain, an outage could delay shipments or trigger penalties under contract agreements. In regulated industries, such as energy or water, the impact could extend to environmental or public safety consequences, as defined by your **Top Site Issues (TSIs)** or similar critical designations.

Continuing with the previous example, the PLC malfunction disrupts production for two hours, triggers safety alarms, and delays a scheduled shipment to a key automotive client. This scenario tests how teams prioritize containment while balancing production, quality, and contractual obligations.

Step 3: Establish the timeline

A clear timeline keeps the exercise structured and manageable. Define when key events, updates, or injects will occur during the session. The timeline doesn't have to reflect real-world durations exactly. In most cases, time is intentionally compressed – what would take 30 minutes in reality might be represented as two minutes in the exercise. This helps maintain momentum and keeps participants focused on decision-making rather than waiting for simulated responses.

Time compression also trains teams to think faster and adapt under pressure, which is especially useful in ICS and IACS environments where every minute counts.

Here's an example timeline:

- 09:00 – Event begins; alarms received in the control room
- 09:10 – Operators attempt a restart; system fails to respond
- 09:20 – IACS security investigates firmware integrity
- 09:35 – Communication sent to IT and management for escalation

Step 4: Create injects

Injects are short prompts or updates introduced during the exercise to simulate real-world developments. Each inject should serve a purpose and should be used to test communication flow, validate escalation, or challenge a specific process.

However, don't overthink injects. They can be as simple or complex as needed. Even seemingly irrelevant injects, such as a side issue or an unrelated email from another department, can be valuable. They test how well participants manage distractions and prioritize critical actions. Learning how to address or ignore nonessential issues during a response is an important part of realistic training.

Here are some example injects:

- The control system vendor reports a corrupted firmware file
- The production supervisor requests an immediate update for senior management
- IT security detects abnormal traffic on the engineering workstation subnet

By crafting injects that reflect plausible issues in your operational context and combining them with unexpected distractions, you bring realism to the exercise and create stronger learning moments.

For additional injects and guidance on designing your own scenario injects for exercises, visit `https://durgeshkalya.com/icsbookresources/injects.html`.

Step 5: Define expected actions and learning objectives

For every inject, define what the expected action should be and what learning objective it supports. This helps facilitators measure performance and guide the **After-Action Review**. Expected actions are based on documented procedures, but learning objectives go deeper; they show what the exercise is really testing, whether it's decision-making, communication flow, or technical containment.

Here are some examples:

- **Inject**: Control room alarms persist despite containment efforts
- **Expected action**: IACS security isolates the affected subnet and provides an update to leadership within 10 minutes
- **Learning objective**: Evaluate containment efficiency, communication speed, and leadership awareness

Step 6: Prepare supporting materials

Supporting materials bring the scenario to life. Prepare situation summaries, network diagrams, sample alerts, or ICS forms to keep participants engaged. Depending on the setup, these materials can be printed handouts, slides, or digital files shared through platforms such as SharePoint or Teams.

Here are some example materials:

- ICS-201 (Incident Briefing Form) and ICS-214 (Activity Log) forms
- Simplified process or network diagrams
- Sample alert messages or email templates
- Incident log or activity tracker

Collect supporting materials such as visuals, system logs, ICS forms, and communication templates to make the exercise more realistic and engaging. A well-prepared set of materials helps participants visualize the problem, communicate clearly, and make better decisions during the simulation.

Customize your scenarios to reflect your organization's environment, processes, and technology stack. Generic scripts often fail to engage participants or test real-world conditions effectively.

Once the scenario is developed, it is time to bring it to life in an exercise. This is where all the planning and preparation come together, transforming the narrative and injects into an interactive learning experience.

The execution phase, discussed next, allows participants to apply their knowledge, test decision-making under pressure, and practice coordination in a safe but realistic environment.

Execution and facilitation of an exercise

Preparation, facilitation, and engagement all play a critical role in making the exercise realistic, organized, and valuable. Whether it is a tabletop or functional exercise, success depends on setting clear expectations, guiding participants through the scenario, maintaining flow, and capturing key observations for later analysis, which we will break down into four steps, namely the following:

- Preparation and setup
- Running the exercise
- Managing flow and engagement
- Observation and documentation

The next section, *Preparation and setup*, outlines how to ensure that all logistics, materials, and communication channels are ready so the exercise can start smoothly and stay focused on its objectives.

Preparation and setup

Before the exercise begins, ensure all logistics and technical arrangements are in place. Verify that meeting invites have been sent, communication channels are working, and participants have received pre-read materials such as the exercise overview, objectives, and ground rules. For hybrid exercises, test the virtual platform (such as Teams or Zoom) in advance to avoid delays.

Facilitators should prepare all injects, documents, and supporting visuals, such as slides, timelines, and forms (ICS-201, ICS-214, or situation reports). Having printed or digital copies of participant guides, checklists, and evaluation forms helps streamline the flow of the exercise.

Further, a short pre-briefing is recommended before the session begins. During this, the facilitator should remind participants that the goal is to learn and improve, not to evaluate or assign blame. Emphasize that the exercise is a safe space to identify challenges, test communication flow, and validate procedures.

Core teams in an ICS exercise

Running an effective ICS exercise requires more than a good scenario – it depends on having the right team structure. Exercises work best when participants understand their defined roles, responsibilities, and boundaries. The core teams concept provides this structure, aligning simulation roles with real-world operational functions.

Core teams ensure that every action, decision, and observation has intent. By clearly defining who simulates threats, who responds, who observes, and who facilitates, organizations can move beyond informal discussions into coordinated, outcome-driven exercises.

This approach mirrors real-world response operations by incorporating all key perspectives:

- **Red team**: Simulates adversaries or disruptive triggers
- **Blue team**: Responds to incidents, executing detection, containment, and recovery
- **White team**: Oversees exercise conduct, controls scenario flow, and evaluates performance
- **Green team**: Provides logistical or technical support to maintain exercise integrity
- **Gold team**: Represents leadership and decision-making authority

While color designations such as Red, Blue, and White are widely recognized, there is no universal standard for team colors beyond these. Some organizations also add a Purple team to bridge Red and Blue. The intent is to keep the exercise organized and roles easily recognizable, improving communication and coordination throughout the session.

Scaling the model

Not every organization begins with a full structure, and that's perfectly acceptable. Smaller facilities can start with just response and observation teams, adding others as capacity and maturity grow. The goal isn't to replicate military or cybersecurity competition formats but to scale proportionally to the organization's needs.

Running the exercise

The facilitator begins by introducing the scenario, explaining the background, and describing the initial event. Participants are encouraged to respond as they would during a real incident. As the exercise progresses, injects are introduced according to the planned timeline to simulate unfolding developments.

During a tabletop exercise, these injects usually prompt discussion around questions such as "What would you do next?" or "Who needs to be informed?" In a functional exercise, participants might actually execute response actions, such as isolating a network, drafting communication to leadership, or initiating containment protocols.

The facilitator's role is to guide the conversation, maintain pace, and ensure objectives are being met. Observers or note-takers document important actions, decision points, communication handoffs, and any confusion or delays that occur.

Throughout execution, it is useful to monitor and record the following:

- How quickly participants identify and respond to injects
- How communication flows between teams and leadership
- Whether established procedures are followed or adapted
- What points of friction or misunderstanding arise

These observations become valuable inputs for the after-action review.

Managing flow and engagement

Maintaining momentum is key to keeping participants engaged. If the exercise slows down, facilitators can introduce new injects or shift the scenario slightly to re-engage discussion. If a conversation drifts off-topic or becomes overly technical, redirect it to focus on decision-making and communication instead of troubleshooting.

Encourage all participants to contribute, especially those from different departments. Exercises are most effective when they foster collaboration and help people understand how their roles interact with others in real incidents. This cross-functional participation builds awareness and improves organizational coordination.

Observation and documentation

Designate an evaluator or scribe to document all key points during the exercise. Observations should capture what was done, how it was done, and what challenges were encountered. Use timestamps where possible to measure response times and communication flow.

At the end of the exercise, conduct a quick *hot wash*. This is an informal debrief where participants share initial impressions, identify what worked well, and highlight areas for improvement. The hot wash should be open, honest, and focused on learning.

After the exercise concludes, facilitators gather notes, logs, and participant feedback to prepare a formal **After-Action Report (AAR)**. This step consolidates all findings and translates observations into actionable improvements.

Use consistent file names and color-coded templates for forms (e.g., blue headers for Operations, green for Logistics). After the exercise, archive all materials – including notes, screenshots, and inject logs – into a shared drive or exercise register for documentation and continuous improvement tracking.

An exercise does not conclude when the final inject is delivered. The close-out phase is a critical extension of execution, ensuring that observations, participant feedback, and performance data are captured while context is still fresh. This is discussed next.

Exercise close-out and transition to improvement

The activities discussed in this section outline a practical approach to closing an exercise and preparing inputs for evaluation and improvement. Each step contributes to closing the feedback loop and embedding continuous learning across the organization:

1. **Conduct a hot wash**: Immediately following the exercise, hold a short, open discussion with participants to capture first impressions while the experience is still fresh. Encourage candid feedback about what went well, where challenges were encountered, and what improvements could be made. The purpose of the hot wash is to speed-collect immediate insights before formal analysis begins.

2. **Collect formal feedback**: Distribute feedback forms or online surveys to gather structured input from participants. Focus on categories such as scenario realism, communication flow, decision-making clarity, and coordination between OT, IT, and leadership teams. This helps capture diverse perspectives and ensures that quieter voices are also heard.
3. **Analyze metrics and performance data**: Review the metrics and KPIs collected during the exercise (e.g., response time, decision accuracy, plan adherence, communication flow). Compare these against established benchmarks to identify trends and areas needing attention. Quantitative data adds credibility to your analysis and helps guide improvement priorities.
4. **Compile the AAR**: The AAR should be written within a few days of the exercise and reviewed by leadership to ensure accuracy and alignment with organizational goals.
5. **Track and incorporate improvements**: Developing an improvement plan or corrective action tracker based on the AAR findings ensures that lessons learned translate into measurable organizational progress. Each identified issue or gap should have a designated owner, defined deadlines, and a clear follow-up process to verify completion. This structured approach turns post-exercise reflection into tangible improvement, embedding accountability and progress tracking into your incident management program.

While ownership and validation of corrective actions continue into the improvement and integration phase, identifying and assigning these actions begins during exercise close-out.

The next subsection focuses on the AAR process, explaining how to analyze exercise results, document lessons learned, and integrate them into your organization's incident response plan for continuous improvement.

Evaluation and after-action review

The evaluation phase transforms observations from the exercise into meaningful insights and improvements. This is where teams capture what worked, what didn't, and how the organization can strengthen its response posture.

The purpose of this phase is to evaluate performance objectively and ensure lessons learned are systematically applied to refine the **Incident Response Plan** (**IRP**), playbooks, and standard operating procedures. This review process turns an exercise from a single event into a continuous improvement tool.

At the heart of this phase is the **AAR**, a structured document that captures outcomes, findings, and corrective actions. Just as in a real incident, documenting results provides practical insight into how effectively the organization responds under simulated pressure.

A well-written AAR should include the following:

- Summary of the exercise objectives and scenario
- Timeline of key actions and decisions made
- Gaps identified in processes, communication, or tools
- Recommended improvements with responsible owners and completion timelines

Inputs from the exercise close-out, including hot-wash observations, participant feedback, and recorded metrics, form the foundation of the AAR. Further, structured participant feedback collected during exercise close-out is analyzed alongside observations and performance data to inform the AAR. Once feedback and observations are collected, compile them into the formal AAR document. This report should be reviewed and approved by management, then used to create an **Improvement Plan (IP)** or corrective action tracker. Each action item must be assigned an owner, given a due date, and tracked to completion.

Treat the AAR as a living document, one that evolves with each exercise. Use it to refine IRPs, update training materials, and guide future tabletop or functional exercises. By closing the feedback loop, organizations ensure that every lesson learned becomes a measurable step toward greater resilience.

Continuous improvement is not an optional phase, but it is the true indicator of program maturity. The key is not just identifying weaknesses but integrating them into actionable changes that enhance the IRP, playbooks, and **standard operating procedures (SOPs)**. Every corrective action should feed into updated documentation, new training modules, or process revisions. Leadership oversight is essential to ensure that recommendations are not only recorded but also implemented and validated in subsequent exercises.

Participant feedback forms

Gathering feedback from participants ensures that the exercise program evolves based on real user experience. Participant feedback highlights logistical challenges, identifies training needs, and measures the engagement level of teams during exercises. These insights help refine the design and delivery of future exercises.

The following are some sample questions for a feedback form:

- Was the exercise scenario realistic and relevant to your role?
- Did you feel engaged and included in the discussions?
- Were the objectives of the exercise clear and well communicated?

- Do you see a need for additional training or follow-up sessions?
- How would you rate the facilitation and flow of the exercise?
- What improvements would you suggest for future sessions?

Keep feedback forms brief and focused. Summarize key findings and share them with participants after the exercise. This demonstrates transparency and reinforces that their input is valued, fostering greater engagement in future activities.

Follow-up and validation

Where feasible, the same scenario or a slightly modified version should be replayed to test whether new measures or procedures effectively address previous gaps. This iterative approach builds confidence and helps institutionalize effective behaviors.

Schedule a follow-up tabletop or functional exercise within 60–90 days to validate that identified improvements have been implemented effectively. This helps close the feedback loop, reinforces accountability, and promotes a culture of continuous learning and preparedness across all levels of the organization.

Improvement and integration

Once metrics and lessons learned are captured, the next step is to translate them into actionable improvements. This phase ensures that every exercise, no matter how small, contributes to a stronger and more resilient incident management program.

Improvement begins with a structured review of AARs and feedback collected from participants. Each observation should lead to a specific corrective action that is assigned to a responsible owner with a clear target date for completion. These actions may involve updating procedures, refining communication protocols, adjusting escalation paths, or enhancing training for key roles.

Integration is where these improvements take root. Updated processes should be incorporated directly into operational documents such as the IRP, SOPs, and site emergency plans. For example, if an exercise reveals confusion over communication channels, the correction should be reflected in the IRP and validated during the next scheduled drill.

Over time, this creates a continuous improvement loop made of planning, exercising, evaluating, and improving. Further, to sustain momentum, organizations should regularly track the progress of corrective actions using metrics such as issue closure rate or plan revision frequency, which

we discuss further in the *Metrics and KPIs* section. While the cost of this phase is often minimal, it requires consistency, time, and commitment across departments so that lessons learned develop into measurable readiness.

Metrics and KPIs

Tracking metrics and **key performance indicators (KPIs)** is essential for measuring the success and effectiveness of your exercise program. These indicators provide objective, measurable insights into program performance, allowing teams to make data-driven decisions, track progress, and continuously improve both the exercise program and the overall incident management strategy.

Metrics are smaller, activity-level measurements, while KPIs focus on the critical drivers of success. Together, they create a framework for evaluating performance, optimizing response processes, and measuring maturity over time.

Table 10.2 shows some of the key metrics and KPIs that are commonly used in the industry.

Type	Name	What It Measures
KPI	Response Time	Measures how quickly an organization detects, analyzes, escalates, and begins containment actions during an incident or exercise.
KPI	Communication Flow	Evaluates the efficiency and accuracy of information sharing between teams, departments, and leadership.
KPI	Decision Accuracy	Assesses the quality of decisions made by comparing them to the organization's playbooks or incident response plans.
Metric	Plan Adherence	Tracks how closely the exercise followed documented procedures and playbooks.
Metric	Exercise Participation	Monitors attendance and the level of active engagement during the exercise.
KPI	Issue Resolution Rate	Measures the percentage of issues identified in the AAR that are resolved before the next exercise.

Table 10.2: Key metrics and KPIs for managing the exercise program

The metrics and KPIs are discussed in detail next.

Response time measures how quickly an organization detects, analyzes, escalates, and responds to an incident. A faster response minimizes the impact on operations, reduces downtime, and limits safety or financial risks.

For example, suppose an organization simulates an IACS network failure as part of an exercise. The network failure may be introduced at 09:00 hours, with a designated scribe capturing key event timestamps to measure response performance. In this scenario, the incident is first detected at 09:07 when an operator contacts the site IT support hotline to report communication errors displayed on an HMI screen. The issue is analyzed and scoped by 09:15, escalated to management by 09:18, and containment actions begin at 09:25, after the organization's security operations center confirms a potential impact on a monitored business system and coordinates containment steps with local IT staff. These precise time markers allow the team to evaluate communication flow by tracking how quickly and accurately information was shared, assess decision accuracy by comparing actions taken against predefined response playbooks, and measure plan adherence to determine how closely procedures were followed during the event. The response time components can be laid out as follows:

- Detection Time: 09:07 (RT1)
- Analysis Completed: 09:15 (RT2)
- Incident Escalated to Management: 09:18 (RT3)
- Containment Actions Began: 09:25 (RT4)

The response time calculation would look something like this:

Total Response Time=Time of Containment−Time of Detection

=RT4−RT1=09:25−09:07=18 minutes

Therefore, the total time from detection to the initiation of containment was 18 minutes. This demonstrates an efficient capability to move from awareness to action, a KPI for effective incident response.

Communication flow is a metric that evaluates how efficiently and accurately information is shared between teams, departments, and leadership during an incident or exercise. Effective communication is essential because it ensures that critical updates reach the right people at the right time, minimizing confusion and enabling coordinated, timely responses.

Let's consider an example in which an initial alert is sent to the ICS response team at 10:02. The IACS lead acknowledges the notification within two minutes, followed by a briefing to the IT security team to assess potential cyber impacts. Operations leadership is informed by 10:10 to ensure management awareness and coordinated response.

The communication timeline would look something like this:

- Initial alert sent to ICS response team (T1): 10:02
- IACS lead acknowledged notification (T2): 10:04
- IT security team briefed (T3): 10:06
- Operations leadership notified (T4): 10:10

The **Communication Delay (CD)** would be T4−T1=10:10−10:02=8 minutes

Therefore, the total communication delay was *8 minutes*.

If the organization's target KPI for communication is five minutes or less, this outcome indicates a need to improve notification protocols, escalation paths, or communication tools to ensure faster and more reliable information flow during incidents.

Decision accuracy measures the quality of decisions made during an exercise by comparing them to predefined playbooks or IRPs. This metric is critical because accurate, well-informed decisions aligned with established procedures help standardize responses, minimize errors, and improve recovery speed during real incidents.

Let's consider an example. During a simulated network isolation exercise, the response team was expected to execute *five* containment steps defined in the playbook. The team correctly completed *four* of the five steps but failed to activate a redundant network link, which was a required action to maintain operational continuity during isolation.

The decision accuracy calculation would look like this:

Decision Accuracy (%) = (Correct Decisions / Total Decisions) × 100

= (4 / 5) × 100 = 80%

A decision accuracy of *80 percent* indicates that while the overall response followed the playbook, at least one critical action was missed. This outcome highlights the need for targeted training, clearer procedural guidance, or improved role clarity to ensure all required decisions are executed correctly in future exercises or real incidents.

Plan adherence measures how closely an exercise follows the organization's documented procedures and playbooks. This metric is important because it reveals whether the established processes are practical, clear, and familiar to the team, or if additional training and updates to documentation are required.

Let's consider an example. During a functional exercise simulating a SCADA system disruption, the response plan defined *12 specific action steps* to guide containment and recovery. The *team executed 10 of those steps exactly* as documented, while *two steps were either delayed or not performed* during the exercise.

The plan adherence calculation would look like this:

Plan adherence (%) = (Steps followed/Total Steps) x 100

= 10/12 x 100 = 83.3%

A plan adherence rate of *83.3 percent* indicates that the team generally followed established procedures, but that certain steps may not be sufficiently clear, well-practiced, or feasible under real-world conditions. This insight can be used to refine documentation, adjust workflows, or focus future training on the steps most likely to be missed during an incident. **Exercise participation** tracks both attendance and the level of active engagement during an exercise. This metric is vital because high participation ensures that key personnel have the opportunity to practice their roles, validate response processes, and contribute to improving organizational readiness. For example, consider an exercise for which 15 participants were invited, with 13 attending the entire session and 2 joining late or missing important planning discussions. While attendance was strong overall, the late arrivals could signal the need for better scheduling coordination or clearer communication of expectations. Monitoring participation helps identify gaps in readiness and ensures that future exercises are conducted with full team engagement for maximum effectiveness.

Issue resolution rate, sometimes simply referred to as resolution rate, measures how effectively an organization addresses the issues and gaps identified during an exercise, particularly in the post-exercise improvement phase. This metric is important because it reflects the strength of the organization's feedback loop and its commitment to continuous improvement.

Let's consider an example. During a tabletop exercise, the AAR identified *10 specific issues* requiring corrective action. Before the next scheduled exercise, the organization successfully resolved *seven of those issues*, while *three remained open* and were carried forward for future follow-up.

The issue resolution rate calculation would look like this:

Resolution rate (%) = (Issues resolved/Total issues identified) x 100

= 7/10 x 100 = 70%

An issue resolution rate of *70 percent* indicates meaningful progress between exercises, while also highlighting the need to track and prioritize remaining gaps. Monitoring this metric over time helps organizations assess whether corrective actions are being completed consistently and whether the exercise program is driving sustained improvement rather than one-time findings.

Beyond core metrics such as response time, communication flow, decision accuracy, plan adherence, participation, and issue resolution rate, there are many other metrics and KPIs that organizations can track to gain deeper insights into their exercise performance and overall readiness. These are discussed next.

Additional metrics and KPIs

Beyond the core metrics previously listed, organizations can expand their program with more advanced indicators as maturity grows. These may include the following:

- **Downtime impact**: Evaluates operational and financial impact of simulated incidents
- **Training effectiveness**: Measures how well participants apply their roles and responsibilities
- **Resource utilization**: Tracks how efficiently resources and personnel were deployed
- **Mean Time to Recovery (MTTR)**: Calculates how long it takes to restore systems to normal operations
- **External coordination efficiency**: Evaluates collaboration with third-party vendors, regulators, or mutual aid partners

The key is to start with a few high-value metrics and expand gradually, tailoring measurements to the unique needs and complexity of the organization.

While metrics and KPIs are essential for evaluating exercise outcomes and program maturity, they are only effective when embedded within a well-structured exercise process. The following case study focuses on how an IACS-focused exercise was planned, executed, and facilitated in practice, illustrating the application of the concepts discussed throughout this chapter in a real operational setting.

Case study: running an IACS/ICS exercise

An automotive parts manufacturing company (about 100 employees and 30 on-site contractors) operated a mixed IT/OT production environment, producing critical rubber gasket components for automotive headlights. Uptime and operational safety were paramount, so the organization took a proactive approach to improve its incident response capabilities, not in reaction to any

specific incident, but to strengthen preparedness. At the time, their security maturity was still developing. For instance, physical security procedures were well established, but there was limited visibility into how IT systems supporting manufacturing were managed and how physical events could impact digital systems.

Early planning conversations revealed confusion over which systems fell under IACS/OT versus IT, who owned those systems, and how an issue in one area might affect the broader operation. These gaps highlighted the need for clearer boundaries and coordination between the plant's OT and IT security teams.

To address these challenges, the company leveraged the ICS framework as a foundation to build and mature its exercise program. The goals of these efforts were to validate the facility's IRP, strengthen cross-functional communication, and test decision-making under pressure. In short, the exercise initiative aimed to improve coordination between the IACS and IT security teams, identify procedural gaps, and generate actionable insights to guide further improvements.

Under executive sponsorship, they established a cross-functional planning team and decided to start small: the program began with a *four-hour TTX* as an introductory step and later evolved into a more comprehensive *FE lasting around six hours*. The details are outlined in the next subsections.

Exercise objectives

The initial tabletop drill helped surface baseline issues. For instance, it showed strong safety coordination but uncertainty in handoffs between IT and IACS teams and when to escalate issues. Lessons from that tabletop were used to refine the scenario and plans for the exercise.

During planning, the team decided on a **hybrid exercise format**. This meant the exercise would combine elements of a tabletop (discussion-based decision making) with some functional simulation (participants actually performing certain actions, such as filling out real forms or simulating device checks). The exercise duration was planned for approximately **6 hours.** In planning the full hybrid exercise, the organization defined several specific objectives aligned with ICS and best practices. The exercise was designed to do the following:

- **Test the readiness** of the ICS-focused incident response team in a realistic scenario
- **Evaluate and strengthen cross-functional communication** between IACS/OT, IT, and leadership teams during an incident
- **Practice structured incident management** using ICS principles – participants would perform roles such as Incident Commander and section chiefs, and follow the ICS *Planning P* process

- **Validate the team's ability to detect, escalate, and contain** a simulated cyber-physical incident affecting production
- **Identify lessons learned** and generate feedback to refine the IRP and related playbooks for continuous improvement

By setting these objectives, the organization ensured the exercise would be both practical and evaluative, training staff on ICS roles while also pinpointing improvements for their incident response process.

Exercise design and planning

The exercise was planned by a core group led jointly by the site's IT security lead and physical security supervisor, with active participation from operations and OT engineers and support from an executive sponsor. This group brought together stakeholders from across departments (IT, OT/IACS engineering, operations, safety, etc.) to shape a realistic scenario and ensure buy-in. All participants who would have an active role in the exercise were required to complete basic ICS-100 and ICS-200 training beforehand, so that everyone shared a common baseline understanding of ICS roles and terminology (many planners and responders had already attended ICS courses or were ICS-trained staff as per the planning roster). This preparation addressed known training gaps and helped the team speak the same language during the exercise.

Structured planning phases

The team followed a structured planning process with multiple phases to design the exercise. *Table 10.3* summarizes the planning and preparation phases, which were adapted from standard exercise best practices and tailored to the organization's needs:

Phase	Description	Meetings	Attendees	Outputs and Examples
Pre-Planning	Establishes the need for the exercise, identifies organizational goals, and brings together the core group that will shape the direction of the program. Focus is on understanding gaps, defining scope, and aligning expectations.	1–2 short meetings, 45–60 minutes	IACS Engineering Lead, IT Security Lead, Physical Security Supervisor, Operations Manager, Safety Representative, Exercise Coordinator	Initial gap analysis (security and process gaps identified), clarification of IACS versus IT system ownership, a draft exercise purpose, early scenario concept ideas, and agreement on who would participate in planning.

Planning and Design	Develops the detailed structure of the exercise, including scenarios, injects, objectives, role assignments, and required documentation. Ensures the exercise reflects real operational conditions.	3–5 detailed working sessions, each 60–90 minutes, plus optional follow-up calls or document reviews	Core Planning Group, Control System Engineers, Network Administrators, Incident Command ICS-trained staff, Vendor Support (optional), Legal or Compliance (optional)	Finalized scenario narrative (loosely based on the facility's actual control systems and network), a timeline of injects, defined ICS forms to use, communication pathways, room setup plans, pre-read materials, identified training needs, escalation paths, and a detailed exercise script.
Execution Prep	Completes logistical arrangements, distributes materials, verifies readiness of participants, and confirms support systems such as communication tools and documentation workflows.	1–2 coordination meetings, each 30–45 minutes, plus internal readiness checks	Exercise Coordinator, Section Chiefs (Planning, Operations, Logistics), IT and IACS Support Personnel, Facilities, HR or Communications (as needed)	Distributed the IRP and role-specific job aids to participants, prepared resource packets, confirmed the participant roster, set up remote access for the hybrid format, printed network diagrams, validated inject timing, and issued final briefing instructions. Also prepared standard ICS forms (e.g., ICS-201 Incident Briefing and resource request forms) to streamline documentation and coordination during the exercise.

Table 10.3: Summary of the planning phases for developing and executing the IACS exercise

Scenario and inject planning

The scenario and injects were carefully scripted to be **realistic** yet safe: they were loosely based on the facility's actual systems and operations, so that participants would recognize the context, but

structured to avoid any real disruption. For example, actual network diagrams of the plant were used as references, and the hypothetical threats targeted similar equipment to what the plant used.

Planners developed a core threat narrative in which an initial **OT disruption** would occur and then lead to a **cyber escalation** affecting IT systems. In practice, this meant the exercise scenario would start with a malfunction or anomaly on the industrial control network (e.g., PLCs or SCADA) and later reveal an evolving cyberattack (e.g., malware/ransomware on the IT network). Specific incident **injects** (discrete simulated events) were defined to drive this story forward. These injects, such as *detection of unusual network traffic*, *equipment failures*, or *threat alerts*, would be introduced by the facilitators at planned times during the exercise. The planning team decided that all injects would be simulated by the exercise facilitators or controllers (via printed messages, emails, phone calls, etc.), rather than actually interfering with any live systems.

In some cases, the scenario involved outside entities (for instance, an external vendor or law enforcement contact); those roles were referenced and simulated by staff acting as that third party, instead of involving real external personnel during the drill. This approach kept the exercise realistic while remaining controlled.

The planning phase also addressed **logistics and tools** to support the exercise. Because the exercise would include remote participants, the team set up a secure video conference line and tested it in advance. All relevant documents, such as the IRP, contact lists, ICS form templates, scenario inject sheets, and past AARs, were made available on a SharePoint portal accessible to all participants, as shown in *Figure 10.3*:

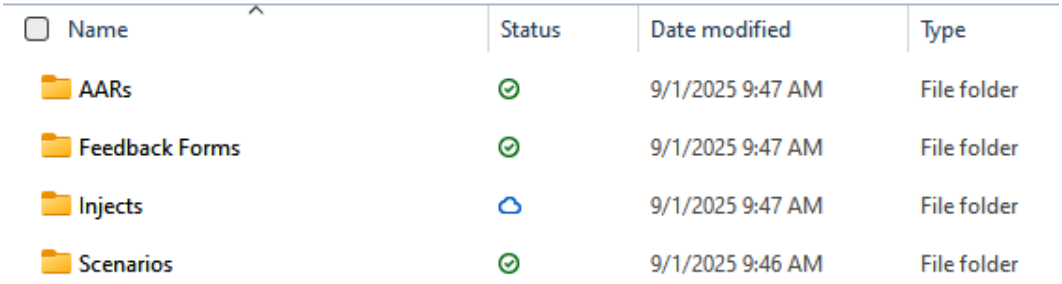


Figure 10.3: Microsoft SharePoint-like site for centralized storage and sharing of incident management resources

This centralized repository ensured that both in-person and remote team members could quickly retrieve information during the exercise, mirroring a best practice that would be valuable in real incident response as well (having a single source of truth for incident documentation).

Exercise execution

On the scheduled day, the exercise was delivered as a 6-hour hybrid incident simulation. It took place in the facility's main conference room with key staff gathered in person, while some participants (and observers from leadership) joined via a secure video conference link. A brief kickoff meeting started at *08:00* with management introductions and a review of ground rules. By *08:30*, the facilitators provided an initial situational briefing to all participants. In this briefing, the *scenario's opening conditions* were described: for example, the plant's control system network was experiencing abnormal communication between two PLCs shortly after a routine firmware update. This simulated an operational technology disruption that the team would need to investigate. Participants were expected to respond as if this were a real incident, following their IRP and the ICS structure.

Participants walked through simulated event triggers, assessed decision-making flow, tested communication between plant operations and management, and even practiced selected containment and recovery actions in a controlled environment. No actual equipment was taken offline, but the teams discussed and documented exactly what they would do if the scenario were real.

The hybrid format allowed for some functional elements. For instance, the team actually filled out incident management forms and made mock phone calls, which added realism beyond a pure tabletop discussion. To facilitate the flow of the scenario, the facilitators used a slide deck that outlined the exercise objectives, scenario background, and the timeline of events. *Figure 10.4* shows the presentation slides prepared to guide the exercise:

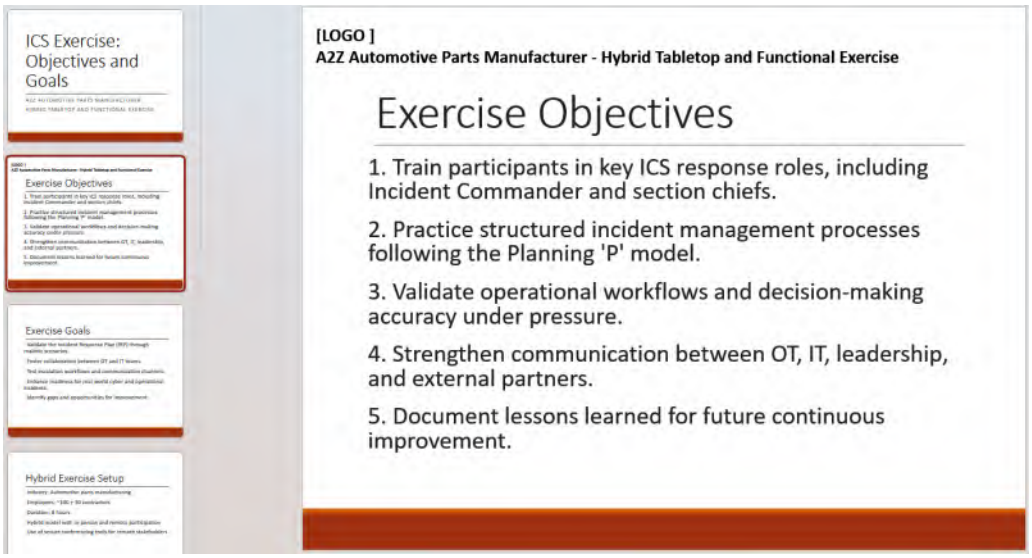


Figure 10.4: Presentation slides prepared to support the execution of the exercise

This slide deck had been shared with participants beforehand, allowing everyone to familiarize themselves with the exercise plan.

As the scenario unfolded, the facilitators introduced a series of injects (simulated incident developments) at planned intervals to escalate the situation from the initial OT anomaly to a broader cyber crisis.

Injects used

The major injects were as follows (see *Table 10.4* for a summary of events, actions, and gaps):

- **Initial trigger (08:30)**: The abnormal PLC communication issue mentioned earlier signaled a potential **OT systems malfunction**. The IACS engineers on the team responded by verifying the firmware integrity of the PLCs and then escalating the issue to the incident management team, treating it as a suspected incident. The Incident Commander position was assumed by a senior manager who began organizing the response. The team documented the situation on an initial ICS-201 Incident Briefing form (capturing what was known, initial resources, and immediate actions).
- **Inject 1 (10:15)**: After the team had addressed the first issue, a **network security alert** was injected. The plant's network monitoring tools (simulated by the facilitators) flagged anomalous traffic on the engineering workstation subnet. This represented a possible cyber intrusion. The IT security staff had to investigate and contain it. They identified the source of the abnormal traffic and initiated a containment by logically isolating that segment of the network, per the IRP. They communicated their findings and actions to the Incident Commander, ensuring the OT side was aware of the potential cyber threat.
- **Inject 2 (11:00)**: A critical vendor suddenly **could not authenticate** to the plant's production scheduling system. This meant the just-in-time delivery coordination might fail, adding operational pressure. The operations team had to quickly contact the vendor's support (simulated via a controller playing the vendor role) and work with IT to check if the access issue was due to the cyber incident. They also kept leadership informed about potential production impacts. This inject tested how the team handles coordination with external partners under duress.
- **Inject 3 (early afternoon)**: A **SCADA interface failure** was then simulated (time marked as "TBD" in the plan, meaning the facilitators introduced it at an opportune moment, around lunch). The interface that control room operators use to monitor a production line went blank, causing a temporary loss of visibility into that part of the process. The IACS engineers had to respond by reverting to manual monitoring on the plant floor and communicating status updates to the operations chief while they worked to diagnose and restore the SCADA HMI. This event tested the team's **operational resilience** and situational awareness – could they continue safe operations despite a blind spot?

- **Inject 4 (13:00)**: In the early afternoon, the scenario escalated to a worst-case cyber incident: a **ransomware alert** was triggered on a server that shared production data with enterprise systems. This was a pivotal moment of the exercise, representing a full-fledged cybersecurity attack overlapping with the OT disruption. The Incident Commander and IT security lead now had to work together to activate containment procedures (e.g., isolating the infected server, cutting off its network access) and initiate data protection measures. They discussed invoking backups and even contacting an external incident response vendor for support (as per the IR plan). All of these actions were simulated through discussion – for example, the team went through the motions of *pulling the plug* on the server and drafting an email to the incident response partner, without actually performing those external communications. This inject tested the **full IRP activation**, as the scenario now had both IT and OT crisis elements.
- **Inject 5 (15:00)**: As a final twist, corporate leadership (the executive team outside the plant) **requested a status update** to share with external stakeholders and possibly the media. This inject was delivered via a simulated phone call from a corporate communications official asking for an executive summary of the situation. It forced the team to consolidate what had happened into a clear report under time pressure. The Planning and Liaison sections collaborated to compile an **executive briefing** using the logs and notes taken throughout the exercise (for instance, they used the ICS-214 activity log and the latest ICS-201 form as references). This tested the team's documentation discipline and communication flow to leadership – could they accurately summarize the incident and response actions in a way that executives could understand?

Table 10.4 summarizes the key activities:

Stage / Time	Trigger or Inject	Expected Actions	Objective Tested	Gaps
08:30	IACS network showing abnormal communication between two PLCs after a firmware update.	IACS team validates firmware integrity, escalates to the incident management team, documents event using ICS 201. See *Figure 10.3* for a sample.	Incident identification, escalation, documentation accuracy.	Delay in escalation due to lack of secondary contacts when the primary IACS lead was unavailable. Need for role redundancy.

Inject 1: 10:15	Abnormal traffic detected on the engineering workstation subnet.	IT security validates source, initiates containment by isolating affected segment, communicates findings to the Incident Commander.	Coordination between IT and IACS, response time, communication flow.	Escalation path between IT and IACS teams was unclear. Initial communication routed through informal channels.
Inject 2: 11:00	Vendor unable to authenticate to the production scheduling system.	Operations contacts vendor support, coordinates with IT to validate access logs, and updates leadership on production impact.	Vendor coordination, decision accuracy, escalation protocol.	Delay in contacting vendor due to uncertainty on who had authority to engage external parties. External communication protocol to be clarified in IRP.
Inject 3: TBD	SCADA interface failure causes temporary loss of visibility on production line.	IACS engineers switch to manual monitoring, report status updates to operations, and assess restoration options.	Operational resilience, cross-team communication, situational awareness.	
Inject 4: TBD	Ransomware alert detected on the shared production server.	Incident Commander activates containment plan, initiates data recovery procedures, and requests support from external response vendor.	Containment procedures, IRP activation, external coordination.	

Inject 5: 15:00	Corporate leadership requests a status report for external communication.	Planning and liaison sections compile executive briefing using ICS 214 activity logs and ICS 201 summary.	Reporting accuracy, communication flow to leadership, documentation discipline.	Executive summary lacked visuals (network maps, event timeline). Recommendation: add visual summaries in future reports.
15:30	Hot wash and participant feedback session.	Teams review actions taken, identify strengths and gaps, and suggest corrective actions for next iteration.	Evaluation and continuous improvement.	Participants requested more frequent short-format drills to practice communication and escalation workflows.

Table 10.4: Summary of the planning phases for developing and executing the IACS exercise

Throughout the exercise, the participants used the ICS incident command structure to guide their actions. An incident command post was simulated in the conference room: the Incident Commander led regular briefings, and the Planning, Operations, and other section chiefs (played by various managers and engineers) practiced their role functions. For example, after the second major inject (ransomware), the Incident Commander convened a tactics meeting around 14:00 to discuss containment strategy and assign tasks, following the *Planning P* model. By 15:00, the team had even drafted an updated IAP for the next operational period, outlining how they would continue to respond if the incident were real. This IAP was not executed, since the exercise was ending, but creating it helped the team think through extended response steps.

Documentation and finalization

The players documented their actions and decisions using ICS forms and logs – treating the exercise like a true incident. For the initial briefing, the team filled out a pre-formatted ICS-201 Incident Briefing form with all known information (incident description, initial response objectives, resources assigned, etc.). As the exercise progressed, team members kept notes on ICS-214 Activity Log forms to record significant actions, communications, and decisions made. All of this was done to practice good incident documentation habits.

Figure 10.5 shows the example pages from the ICS-201 Incident Briefing form used during the exercise.

INCIDENT BRIEFING (ICS 201)

1. Incident Name:	**2. Incident Number:**	**3. Date/Time Initiated:**
OT Network Disruption and Ransomware Simulation Exercise	EX-2025-01	Date: April 10, 2025 Time: 08:00 hrs

4. Map/Sketch (include sketch, showing the total area of operations, the incident site/area, impacted and threatened areas, overflight results, trajectories, impacted shorelines, or other graphics depicting situational status and resource assignment):

The simulated event originated in the Mixing Unit control system, impacting PLC communication and the production scheduling system. Subsequent ransomware activity was detected on the shared production server and engineering workstation subnet. Plant areas affected included Mixing and Assembly zones, along with vendor communication systems through the ERP interface.

5. Situation Summary and Health and Safety Briefing (for briefings or transfer of command): Recognize potential incident Health and Safety Hazards and develop necessary measures (remove hazard, provide personal protective equipment, warn people of the hazard) to protect responders from those hazards.

At 08:00 hrs, participants were briefed on a simulated OT network anomaly following a firmware update on a PLC controlling the Mixing Unit. Abnormal communications were detected between PLCs and the HMI, leading to loss of visibility.

Health and safety emphasis: this is a discussion-based and partially functional simulation. No live systems were affected. All activities were to be conducted in a safe, controlled environment using isolated or simulated networks.

6. Prepared by: Name: Dough Kayla Position/Title: Exercise Facilitator Signature: _____

ICS 201, Page 1 Date/Time: 08:15 hrs

Figure 10.5(a): Page 1 of Incident Briefing form

INCIDENT BRIEFING (ICS 201)

1. Incident Name:	2. Incident Number:	3. Date/Time Initiated:
OT Network Disruption and Ransomware Simulation Exercise	EX-2025-01	Date: April 10, 2025 Time: 08:00 hrs

7. Current and Planned Objectives:

Validate the organization's Incident Response Plan (IRP) and escalation procedures.

Test communication and coordination between OT, IT, and Operations.

Evaluate documentation using ICS forms (201, 214).

Identify response gaps and training needs for follow-up actions.

8. Current and Planned Actions, Strategies, and Tactics:

Time:	Actions:
08:30	Initial scenario briefing and incident identification.
09:10	OT validates firmware integrity; IT begins monitoring network traffic.
10:15	Inject 1 – Abnormal subnet traffic prompts containment discussion.
11:00	Inject 2 – Vendor authentication failure; Operations and IT coordinate response.
13:00	Inject 3 – SCADA visibility loss; manual monitoring initiated.
14:00	Inject 4 – Ransomware detected on production server; containment plan activated.
15:00	ICS 214 logs reviewed; IAP and communication summary developed.
15:30	Hot wash conducted; lessons learned and corrective actions documented.

6. Prepared by: Name: Dough Kayla Position/Title: Planning Section Chief Signature: _____

ICS 201, Page 2 Date/Time: 8:15 hrs

Figure 10.5(b): Page 2 of Incident Briefing form

(a) Page 1 captures the situation overview, initial response actions, and resources on scene. *(b) Page 2* continues with summary information and immediate next steps. Using standardized ICS forms like this helped participants organize information and ensured a common format for reporting. In the exercise, participants completed these forms as if the incidents were real, which highlighted any areas where the IR plan's documentation process could be improved.

As mentioned earlier, **no real operational changes were made** during the exercise. All activities were either talk-through or simulated on paper. For example, when a network segment "needed" to be isolated due to malware, the IT lead announced the action and noted it in the documentation, but did not actually disconnect anything.

The **hybrid format** proved effective: in-person participants huddled around tables with network diagrams and ICS forms, while remote participants contributed via video chat, all following the scenario in real time. The slide deck guided the exercise timeline, and the SharePoint portal was actively used to reference documents (for instance, the remote Incident Commander pulled up the IRP PDF from SharePoint when deciding on notification steps). The facilitators paced the injects to keep everyone engaged and under a degree of pressure without overwhelming the team.

By 15:30, after the last inject (leadership briefing) was completed, the exercise portion ended. The Incident Commander declared the simulated incident *contained* for the purpose of the drill.

Findings and lessons learned

Immediately following the exercise, the facilitators led a **hot wash** debrief session with all participants. In this open forum, team members candidly discussed what went well, what issues they encountered, and how they felt about the response. The goal was to capture **lessons learned** while the experience was still fresh. The debrief was frank and constructive – participants were encouraged to provide honest feedback without fear of blame, focusing on improving the process.

Several key findings and gaps were identified during the exercise debrief:

- **Communication flow**: Information sharing between teams did improve compared to earlier drills, but **delays were noted in escalation**. In particular, when the operations/OT team needed to alert IT leadership about an issue on the plant floor, it did not happen as quickly or efficiently as desired. This indicated room to streamline how incidents in the industrial environment are reported up to IT and management.
- **Decision accuracy**: Overall, teams executed most of the required response steps correctly. However, they **missed a critical escalation step during the ransomware phase** of the scenario. Specifically, the team initially failed to notify one of the corporate stakeholders, as outlined in the IRP, when the ransomware infection was discovered. This pointed to a lapse in following the playbook under pressure and underscored the need for clearer triggers for escalation in the procedures.

- **Plan adherence**: The IRP provided a solid, high-level framework, and the team did refer to it for guidance. Nonetheless, the IRP **lacked certain detailed procedures**, most notably for coordinating with external vendors during an operational disruption. This gap became evident during the vendor access inject – participants were unsure who had the authority to call the vendor and what exactly to communicate. It highlighted that the IRP and playbooks needed expansion in the area of third-party communication protocols.
- **Participation**: There was **strong engagement from all departments** throughout the exercise. Every relevant function (operations, IT, OT, safety, etc.) was represented and actively contributed to the response. This was a positive sign. However, the exercise also revealed that some **junior IACS engineers would benefit from additional training** in incident management. These less experienced engineers were sometimes hesitant or unsure about their roles in the ICS structure. More coaching or drills for these individuals would increase their confidence in a real incident.
- **Issue resolution rate**: Approximately **70% of the action items identified in the previous tabletop exercise had been resolved** by the time of this functional exercise. This showed clear progress; for example, many procedural changes recommended after the tabletop had been implemented. However, it also means about 30% of prior issues were still outstanding, leaving room for further improvement. Some items take longer to fix (such as procuring new technology or fully training staff), but the goal is to continue driving this closure rate higher in future exercises.

Across these findings, the **most significant gap** observed was **a lack of clarity in escalation pathways and authorities**. Multiple injects exposed this issue: initial incident escalation from OT to IT was slower than expected, and later, there was confusion about who should contact the external vendor and when higher management should be notified. Essentially, the team realized that their IRP did not spell out escalation **triggers and responsibilities** in enough detail, which led to ad hoc decision-making during the exercise. This was a crucial insight, as timely escalation is vital in incident response. The participants agreed that clarifying **who contacts whom, under what conditions, and how quickly** must be a top priority in refining their plans.

On a positive note, the exercise underscored that using the ICS framework helped impose structure on a chaotic scenario; communication was generally systematic (despite some delays), and everyone practiced keeping logs and following a chain of command. Participants also noted that having the SharePoint repository and prepared documents was very helpful. In fact, one recommendation from the team was to use that SharePoint site for **real-world incident documentation** going forward, not just for exercises.

Additionally, participants requested **more frequent short-format drills** to reinforce what they learned. They felt that brief, focused exercises (even 1-hour discussion drills or *tabletop refreshers*) conducted quarterly could help maintain skills, especially around communication and escalation. This feedback reflected an understanding that one big exercise per year might not be enough, and that practicing specific elements (such as just the notification process) more often would improve performance.

All of these findings were captured by the exercise facilitators in an initial AAR.

Outcomes and continuous improvement

The outcome of the exercise was not just the lessons learned, but the actions the organization took afterward to improve its incident response readiness. Immediately after the hot wash, the planning team and Incident Commander worked to compile an **Executive Summary report** of the exercise for senior leadership. This report highlighted the key outcomes:

- It noted that cross-team coordination had measurably improved and that critical decisions (such as containment of the malware) were made more quickly than in past drills
- It explicitly pointed out the gaps in escalation and communication that were discovered, as well as some resource and training shortfalls

The following figure presents an excerpt from the report:

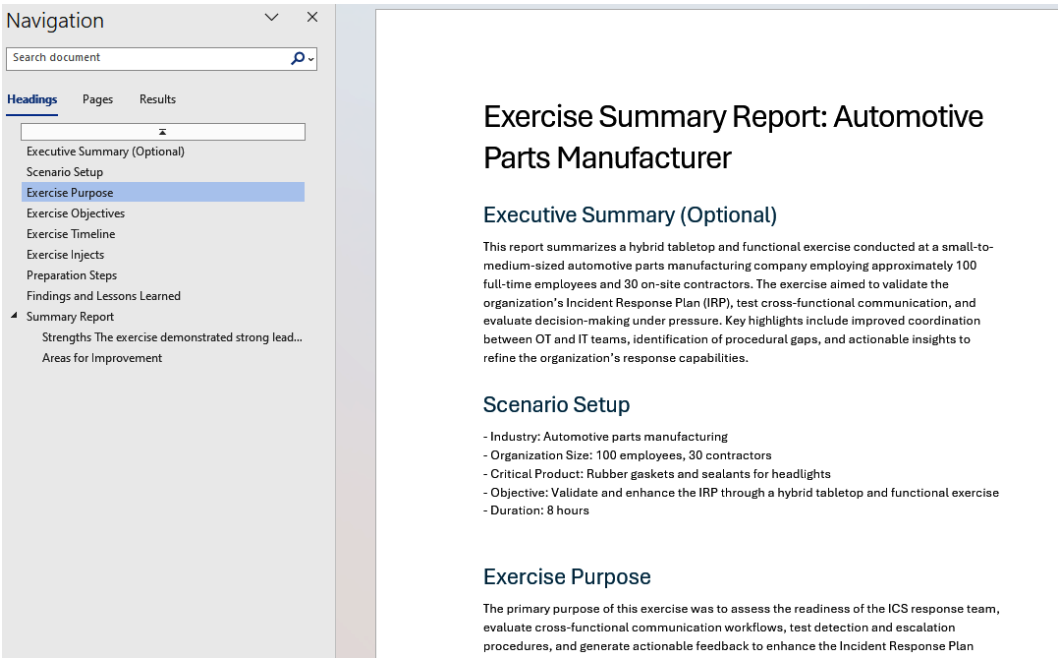


Figure 10.6: Executive report of the exercise

Sharing this report not only demonstrated transparency and accountability but also helped **secure continued executive support** for the incident response program. Leadership could see the return on investment from the exercise and the path forward.

With management backing, the organization moved quickly to update its IRP and procedures based on the exercise findings. All the specific gaps identified went into an **improvement tracker**. The following changes were made:

- Escalation paths were refined and clearly documented in the IRP – the revised plan now defines exactly who (by role) must be notified for different incident types and severity levels, and within what time frame.
- A decision matrix was added to the plan to help Incident Commanders determine when to involve certain external parties or higher management.
- Responsibilities for backup roles were clarified as well.
- During the exercise, when the primary OT lead was unavailable briefly, there was confusion; to fix that, the IRP now assigns designated alternates for each key role to ensure redundancy.
- The contact lists and resource inventories (e.g., vendor support contacts, government notifications, etc.) were also updated as some of that information was discovered to be outdated during the drill.
- These updates were all drafted within weeks of the exercise and approved by the relevant department heads. The changes were then incorporated into brief refresher trainings for the team, so that everyone was aware of the new and improved procedures.

Follow-up

Essentially, the organization treated this exercise as part of a **continuous improvement cycle** rather than a one-off event. It scheduled a follow-up exercise – a shorter *four-hour tabletop* – roughly two months later to validate the updates made to the IRP and ensure that the lessons learned truly led to better performance. In that follow-up tabletop, they revisited a similar scenario (with some twists) and observed whether the previous trouble spots (such as escalation) had improved. Indeed, during the follow-up drill, the escalation of an incident was carried out much more quickly and smoothly, indicating that the clarifications in the IRP were effective. This closed-loop testing ensured that improvements were not just documented on paper but actually put into practice and proven.

By maintaining this feedback loop of **plan -> exercise -> lessons -> improve -> re-test**, the company demonstrated a commitment to building a resilient, evolving incident response capability. What started as an isolated drill has now grown into a structured program with executive support.

Each exercise, no matter how small, feeds into the next, gradually elevating any organization's readiness.

The use of ICS provided a scalable framework, but the organization also smartly **adapted ICS to its reality,** focusing on communication and decision processes that fit its size and culture, and intentionally simplifying certain formalities (for example, conducting a tactics meeting in 15 minutes because that's what the schedule allowed, even though the ICS textbook might allocate more time). These purposeful deviations kept the exercise practical and sustainable, while still aligning with industry best practices.

In summary, this case study shows how a medium-sized manufacturing company proactively strengthened its incident response through a well-planned exercise. The hybrid tabletop/functional exercise tested the team's technical and organizational response to an OT and IT attack scenario. It revealed critical insights, particularly about communication and escalation, which were then used to drive tangible improvements. By iterating on the process – training, exercising, evaluating, and updating – the organization fostered a culture of continuous improvement in security preparedness. The next time a real incident occurs, it will be far more prepared: the teams have **practiced together**, the plans have been **refined**, and leadership is **engaged and supportive** of these efforts. This proactive approach moves the organization one step closer to true operational resilience, transforming lessons learned into lasting readiness.

Summary

This chapter explained how organizations can apply the **Incident Command System (ICS)** to improve preparedness and incident management in industrial and IACS environments. It emphasized moving beyond one-time drills toward structured exercise programs built on consistent planning, execution, and evaluation. You learned how to define objectives, design realistic scenarios, facilitate exercises, and capture lessons that drive continuous improvement.

The case study demonstrated these concepts in practice through a hybrid tabletop and functional exercise conducted in a manufacturing setting. It illustrated how ICS roles, standardized documentation, realistic injects, and after-action reviews can be used to strengthen communication, coordination, and decision-making. Together, these elements show how exercises can become practical learning tools rather than compliance-driven events.

Each exercise, regardless of size or scope, contributes to organizational resilience by building familiarity, confidence, and disciplined response behaviors across teams. Once an organization can consistently run effective exercises at a single site, it establishes the foundation needed to expand those capabilities more broadly.

The next chapter, *Chapter 11*, *Optimizing Exercises Across Single and Multiple Sites in Your Organization*, focuses on scaling these practices. It explores how to standardize exercise planning, coordinate participation across locations, manage resources, and maintain consistency while accommodating site-specific operational needs.

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

11

Optimizing Single-Site Exercises with Multi-Site Considerations

In this chapter, we explore advanced strategies for conducting incident management exercises within a single organization, whether it operates at a single site or across multiple locations. No two organizations are ever the same, even if they were built using the same blueprint; the focus is on tailoring exercises to be truly effective by customizing the goals, scope, and scenarios to reflect the organization's unique structure, risks, and operational realities. We'll also address the unique challenges of coordinating exercises across multiple sites, including how to maintain consistency, enable clear communication, and support scalable response capabilities.

While this chapter introduces both single-site and multi-site exercises, the emphasis is intentionally placed on mastering single-site execution first. A well-run single-site exercise becomes a building block for effective multi-site coordination. Throughout this chapter, each planning element is first explained in a single-site context and then extended to highlight the adjustments required when scaling across multiple facilities.

Single-organization exercise planning and execution

Within a single organization or site, the impact of an incident can be very severe. This could include operational downtime, realization of safety hazards, damage to the environment, and, in some cases, even reputational losses or the revocation of licenses to operate, which ultimately leads to significant business disruption. Having a strategy and a well-practiced response plan ensures that the organization can act swiftly, decisively, and in a coordinated manner whenever a disruption occurs.

In the previous chapter, we talked about running exercises ranging from tabletop to functional exercises, and the following benefits were identified:

- Identifying gaps in roles, communication, procedures, missing checklists, staffing issues, and inadequate resource planning
- Encouraging cross-functional collaboration by bringing together various groups and departments, especially OT, IT, facility security, and safety teams
- Supporting organizations in meeting regulatory expectations and strengthening overall incident response preparedness

In this section, we'll explore two hands-on strategies for running exercises. We will cover a single exercise first and then draw out the differences and adjustments needed to run the same exercise in a multisite environment.

Running an exercise in a single-site environment allows for a controlled and focused approach, which is ideal for organizations beginning their exercise program or looking to refine existing processes. Every aspect of planning, from scope to evaluation, is streamlined, as participants are physically co-located, communication channels are simpler, and decision-making is often more direct.

Figure 11.1 highlights the key strategy steps needed to plan a single-site exercise.

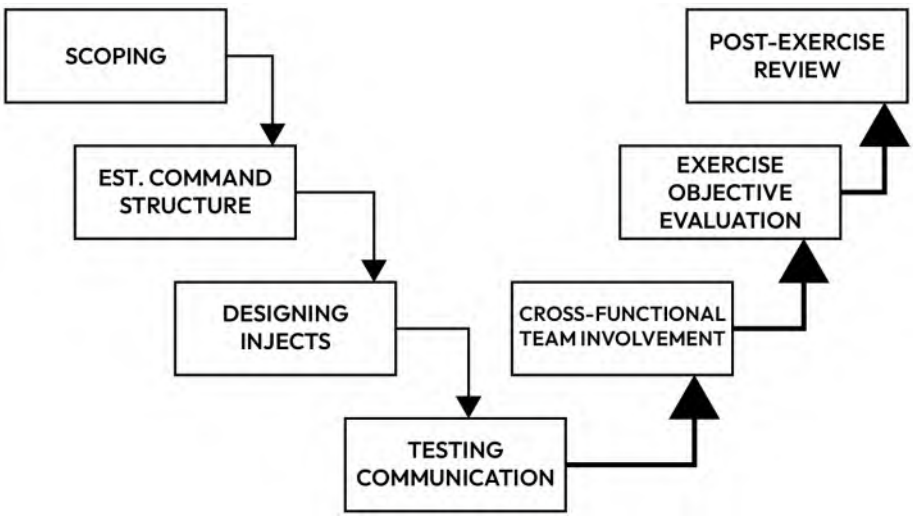


Figure 11.1 – Strategy Steps needed to plan an exercise for a single site

The idea here is simple: understand how to plan and run an exercise at one site first, because that becomes the foundation for scaling up to a multi-site exercise later. By now, you're probably familiar with the steps, but let's take a closer look next.

Scope

Think of an exercise as starting a new project; the principles are the same. The scope is critical because it drives everything else: who will participate, what resources will be needed or made available, the level of management interest and support you can expect, and ultimately, whether the exercise will meet its objectives.

The exercise scope defines the boundaries, objectives, and scale of the exercise – essentially, what will be tested and what won't. A well-defined scope ensures the exercise stays focused, manageable, and aligned with organizational priorities.

Think of this step as setting the blueprint for your exercise. In a chemical plant or oil and gas facility, the scope often has to balance operational realities (such as shift schedules, safety requirements, and process dependencies) with cybersecurity needs. Breaking the scope down into clear parameters makes planning and execution smoother:

- **Determine the "crown jewels"**: Identify the most critical systems and processes, both from a technology and business standpoint, that, if compromised, would have the most significant impact.

  Some examples include **Safety Instrumented Systems (SIS)**, batch control systems, or the **Distributed Control System (DCS)** managing high-pressure reactors. For environments such as in oil and gas, examples include pipeline SCADA systems, compressor station control, or custody transfer measurement systems, where downtime equals lost revenue and potential safety hazards. In a water utility, think of the control network managing pumping stations and chemical dosing systems. In a manufacturing plant, consider **programmable logic controllers (PLCs)** managing automated production lines or robotic systems. In an airport's baggage handling system, there are the centralized OT servers that keep belts and scanners running.

  When organizations operate across multiple sites, crown jewels are rarely isolated to a single facility. In many cases, the most critical assets are shared services that support multiple locations, such as centralized OT monitoring platforms, remote access infrastructure, identity and authentication services, patch management systems, and enterprise backup environments. An exercise that spans multiple sites should deliberately test how the loss or degradation of these shared assets affects operations across the organization. This often introduces the need for enterprise-level prioritization, where leadership must decide which sites receive limited technical support, recovery resources, or operational attention first. Incorporating these shared crown jewels into a multi-site exercise helps reveal hidden dependencies and exposes risks that may not be apparent when exercises are designed around a single facility.

- **Map the network path**: Trace the network connectivity to these critical assets to understand potential attack paths or points of failure – for example, mapping how a contractor VPN connects to a substation's SCADA systems in the energy sector or documenting the path between a corporate network and a process historian in a food processing plant, identifying weak points such as outdated firewalls or unsecured wireless links.
- **Align with threat intelligence**: Leverage current threat intelligence, internal assessments, and regulatory reports to guide your scenario design. For example, if a recent advisory highlights ransomware targeting OT systems, build a scenario where an attacker pivots from IT to OT systems during a shift change. For transportation hubs, you could simulate cyber-physical risks such as a compromise in signaling systems or automated gates based on industry threat reports or vendor advisories.
- **Test policies and procedures**: Use the exercise to validate your **incident response (IR)** processes and collaboration between teams.

  For example, in a pharmaceutical plant, test whether teams can safely isolate an infected workstation without impacting quality control systems. In a water utility, check if operators know the escalation path when telemetry data shows inconsistent readings during a suspected cyber event.

- **Focus on decision-making**: Tabletop exercises or functional exercises often aim to test decision-making and communication under pressure in a realistic, simulated environment – for example, a regional power grid operator deciding whether to disconnect a substation during a suspected malware event.
- **Define exercise type**: Choose the type of exercise that matches your goals. Tabletop exercises, which are discussion-based, are great for testing strategies, communication, and decision workflows, whereas functional or full-scale drills are hands-on and ideal for validating technical responses in real time with live systems or simulated environments. For example, a tabletop session could simulate phishing emails targeting engineering accounts, whereas a functional drill might involve activating backup control systems during a live test window.
- **Scenario realism**: One of the main scoping objectives should be to build scenarios that reflect your sector's real-world challenges and risks to make the exercise relatable and practical – for example, a ransomware event impacting historian data in a steel plant, a spoofed telemetry in a water distribution system leading to unsafe pressure conditions, network congestion through various attack methods such as DDoS, UDP floods, and so on in a smart port disrupting automated crane operations.

- **Duration of the exercise**: Match the time frame and scale of the exercise to the complexity and objectives of your scenario. A shorter, focused tabletop – often two to three hours – works well for localized incidents, such as a single facility responding to a ransomware event or a control system failure. On the other hand, complex scenarios, such as a coordinated cyberattack affecting multiple operational nodes across a regional energy grid or a series of disruptions in a transportation network, often require a multi-day functional exercise to allow for realistic planning, response, and recovery activities.

Expanding an exercise beyond a single facility adds additional complexity to the scope, requiring careful consideration of how sites interrelate. When an exercise spans multiple locations, scope definition must account for interdependencies between facilities and clearly articulate the level of coordination involved. For example, you should determine whether the scenario will test each site's response independently, escalate issues to a regional or corporate team, or both. It's also vital to distinguish between impacts contained to one site and those that have enterprise-wide consequences, such as the failure of shared authentication servers, centralized data historians, or other common services that multiple sites rely on. By broadening the scope in this way, you prevent a multi-site exercise from becoming unmanageable while still capturing realistic cascading risks across the organization.

Command structure

Command structure is the hierarchy and set of roles established to manage incident response during an exercise. A well-defined structure not only clarifies decision-making authority but also improves coordination and ensures the exercise mirrors real-world incident management frameworks.

In a single-site environment, the command structure often depends on the size of the operation and the resources available. For example, a large facility may have a dedicated **Emergency Response Team** (**ERT**), IACS specialists, OT network engineers, and even malware analysts on-site. These individuals are trained for their specific roles and can respond quickly during both real incidents and exercises.

However, not every site has the luxury of specialized personnel for every function. In smaller facilities, roles are often shared or combined. For example, an ICS engineer might also serve as the application specialist, or the IT lead might double as the OT liaison during an incident. Recognizing these overlaps during planning is critical, as it helps ensure that exercises remain realistic and reflect the actual capabilities of the site.

When gaps exist in expertise or staffing, organizations often rely on external support, such as vendor partners or **managed service providers (MSPs)**, to fill key roles. Any such reliance should be incorporated into the exercise design. Including these third-party partners in your command structure through mutual aid agreements, standing contracts, or even informal arrangements ensures that when a real incident occurs, communication and collaboration with external responders are already established.

Ultimately, an effective command structure is about realism and alignment. By planning with your actual organizational resources in mind, whether they are on-site personnel, shared roles, or vendor support, you create exercises that are not only practical but also valuable training opportunities for the teams that will be called upon during a real-world event.

Once exercises move beyond a single facility, command structures must scale accordingly.

When an exercise involves multiple sites, the incident command structure must adapt to include both local and central leadership roles. In a multi-site scenario, it is critical to delineate site-level command from enterprise-level coordination. Site **Incident Commanders (ICs)** should retain authority over local operational decisions, while a unified or corporate command oversees strategic priorities, resource allocation across sites, and external communications. The exercise plan should explicitly test escalation procedures – for instance, when and how a local incident is elevated to corporate attention – and clarify decision-making authority and handoffs between site leadership and headquarters. By design, the multi-site exercise should surface any ambiguity in command relationships, since unclear authority is a common failure point in real incidents that span several locations. Establishing these boundaries and escalation paths beforehand ensures that when multiple facilities are involved, everyone knows who is in charge of what, at both the site and enterprise levels.

Inject design

This is one of the most critical components of an exercise because injects are the planned events or pieces of information introduced during the exercise to simulate real-world triggers. Well-crafted injects drive realistic decision-making, push teams to think critically, and challenge them to act under pressure, just as they would during an actual incident.

Injects can range from simple notifications, such as an alert from a security system or a phone call reporting an anomaly, to complex, cascading events that escalate the scenario over time. For example, during a ransomware attack exercise, an initial inject might simulate the detection of malicious files on an engineering workstation. A follow-up inject could then introduce a failure of the DCS interface because the control server managing critical processes has been encrypted, forcing the team to make rapid, high-stakes decisions to prevent unsafe conditions.

For single-site exercises, injects are generally easier to manage because their impact is localized. However, they must remain highly relevant to the specific environment. The key is realism; injects should directly reflect the operations, technologies, and risks of your facility. For instance, in a water treatment plant, an inject might simulate a sudden loss of remote telemetry data, forcing operators to switch to manual mode to maintain water quality.

Similarly, in a manufacturing facility, an inject could be a PLC failure caused by a simulated malware infection, disrupting automated production. Or, in an energy substation, a scenario might introduce false readings on protective relays, testing the operators' ability to cross-verify data and prevent unnecessary shutdowns.

On the other hand, unrealistic injects, such as simulating an airline check-in system outage at a site that manages industrial chemicals, undermine the exercise's value. Your team should be able to relate to the injects, understand their operational significance, and respond in a way that mirrors what they would do in a real incident.

As exercises expand to include multiple facilities, inject design must also evolve. Designing injects for a multi-site exercise demands an extra level of coordination so that participants aren't overwhelmed, yet realistic escalation paths are tested. In scenarios that involve several facilities, injects must be carefully timed and synchronized across sites. One approach is to use **staggered injects**: one site experiences an issue first, then ripple effects occur at other locations, mimicking a spreading incident. Another approach is to introduce **simultaneous injects** at different sites, which emphasizes enterprise-level coordination and communication. In both cases, well-crafted multi-site injects should challenge more than just each site's technical response. They must also exercise information sharing, joint prioritization of issues, and decision-making across geographically dispersed teams.

By tailoring injects to your facility's realistic risk scenarios, you not only make the exercise more engaging but also ensure it generates actionable insights. Well-designed injects keep teams focused, build confidence, and provide a controlled environment to test both technical and procedural responses under pressure.

Testing communication

Reliable, familiar communication tools are critical because communication is the backbone of any effective response. Without clear, dependable communication, decision-making slows, confusion builds, and even minor incidents can escalate into major disruptions.

During an exercise, it's important to use the same tools you would rely on in a real incident, so participants gain experience with systems they already know. This might mean using your corporate email platform, secure messaging apps, two-way radios, or dedicated incident management tools. But realism also means anticipating failures and planning for them.

Imagine a scenario where your primary systems fail:

- **Network outage**: Email and internal chat platforms are down, leaving teams scrambling for alternatives
- **Phone failure**: During a hurricane or regional disaster, cell towers may be offline or overloaded
- **Software malfunction**: Your incident management dashboard freezes or becomes inaccessible just when you need it most

Such scenarios highlight the importance of redundancy and adaptability. Some organizations incorporate radios, satellite phones, or even paper-based processes as backup options. In a single-site but multi-building facility or campus, having runners hand-deliver critical information—a simple *mailroom run* approach—can maintain communication when technology is unavailable.

Your exercise should test these contingencies. For example, you might simulate a network outage and evaluate whether teams can switch smoothly to radios or backup phone lines. Test your contact lists and escalation trees to ensure they are current and accessible offline. The more realistic your approach, the better your teams will perform under actual pressure.

Communication challenges are amplified when an incident affects more than one site. In multi-site scenarios, factors such as different time zones, added organizational layers, and dependence on enterprise-wide communication systems can hinder the swift flow of information. It's important to verify that local incident updates reach senior leadership quickly and in a usable format, and conversely, that guidance from leadership is clearly relayed back to all affected sites. Backup communication methods also take on greater importance: if a primary channel (for example, the corporate chat or incident management platform) fails, that outage can disrupt coordination across every facility. A multi-site exercise should therefore test redundant communication paths and protocols to ensure each site can stay in sync even under communication strain. Finally, maintaining clear reporting structures and standardized status updates across the organization will help prevent confusion and information overload when multiple sites are issuing reports at once.

Cross-functional team involvement

Team involvement from every critical group – OT, IT, security, safety, operations, and leadership – is the backbone of a successful exercise. Including the right mix of people promotes cross-functional collaboration and prepares the organization for a truly coordinated response when a real incident occurs.

When planning an exercise, the first step is to identify key individuals from each group or department who are directly involved in day-to-day operations or who would play a role in responding to an incident. This ensures that the exercise reflects the real-world systems, processes, and decision-making paths in your environment.

Here are some examples:

- If there's a loss of connectivity in your OT environment, you need your OT network engineer in the room to validate troubleshooting steps and recovery plans
- If a power outage disrupts the control room, facilities or electrical engineers must be available to support safe restoration
- In a scenario where you need to procure emergency equipment, such as a dozen Chromebooks to establish an alternate communication setup, someone from procurement or finance must be present to approve the requisition and fast-track delivery
- During a malware infection, having both the OT security specialist and IT incident responder in the exercise ensures seamless coordination between operational recovery and forensic analysis

Pre-exercise training is also critical. The training doesn't have to be extensive, but it should introduce each group to the terminology, systems, and expectations of others. The EOC team should understand the basics of industrial control systems, how OT networks differ from IT, and what operational risks look like. Likewise, OT teams need to be familiar with the protocols, priorities, and communication style of the EOC and corporate leadership. Further, cross-training IT and OT staff builds trust and eliminates silos, making the exercise and the real-world response more effective.

In a multi-site exercise, you must involve not only the local responders at each site but also enterprise-level functions such as *corporate security*, *legal, communications*, *procurement*, and *executive leadership*. Many of these groups play only a minor role in a single-site drill, but they become pivotal when an incident affects several locations at once. The exercise should assess how well these diverse teams work together across organizational boundaries – for instance, how site

engineers interact with corporate crisis managers or how local safety officers coordinate with the central legal team. It is essential to confirm that roles and responsibilities remain clear as the incident expands beyond one site. By involving a full spectrum of stakeholders and testing their collaboration, a multi-site exercise ensures that the organization can mount a unified response when real crises span multiple facilities.

Exercise objective evaluation/assessment

To evaluate and improve incident management exercises, it's important to balance quantitative metrics with qualitative insights, creating a well-rounded view of your team's readiness. In *Chapter 7*, we already covered critical parameters such as **Recovery Point Objective (RPO)**, **Recovery Time Objective (RTO)**, **Work Recovery Time (WRT)**, and **Maximum Tolerable Downtime (MTD)**. In addition to these, the following performance measures can be applied during incident response planning and when running exercises to assess effectiveness:

- **Mean Time to Detect (MTTD)**: Measures how quickly your team identifies an incident, showing the strength of your monitoring systems
- **Mean Time to Resolve (MTTR)**: Tracks the speed and efficiency of restoring normal operations, reflecting how well your processes work under pressure
- **Mean Time to Contain (MTTC)**: Highlights the ability to stop the spread of an incident before it escalates
- **SLA compliance rate**: Shows how often incidents are resolved within agreed time frames, a clear indicator of reliability and discipline during response

To better visualize key performance parameters, the following figures illustrate two different scenarios. *Figure 11.2* represents an ideal situation where all key metrics – MTTD, MTTC, and MTTR – meet their target values:

Figure 11.2 – Optimal response timeline with MTTD, MTTC, and MTTR on target, showing full SLA compliance

Figure 11.3, in contrast, highlights a scenario where the target thresholds are not achieved.

Figure 11.3 – Delayed response with MTTD, MTTC, and MTTR overruns, highlighting SLA gaps

The visualization clearly shows where the response performance exceeded the set limits, impacting the overall SLA compliance.

Evaluating a multi-site exercise means comparing key metrics across sites to identify any disparities in capability or readiness. For example, you might look at whether the mean time to detect, contain, or resolve an incident differs from one facility to another. This would help you highlight inconsistent monitoring or response processes. Multi-site evaluation should also capture enterprise-level factors that wouldn't appear in a single-site review. These include measuring **decision latency at the corporate level** (how long it takes for critical decisions or approvals to flow through headquarters) and examining **resource allocation among the sites** during the exercise. By analyzing performance across multiple locations in this way, the organization can spot systemic weaknesses or coordination gaps that a single-site exercise might never reveal.

From a qualitative standpoint, **After-Action Reports (AARs)** deliver insights that raw metrics simply can't capture. They take a closer look at how people, processes, and communication actually performed during the exercise. Feedback can be gathered from participants through a simple sheet or questionnaire. When creating these feedback tools, key areas to focus on include the following:

- Did everyone know their responsibilities, or was there confusion that slowed decision-making?
- Were updates clear, timely, and routed through the right channels?
- How well did teams make critical decisions under pressure, and were they supported by accurate information?
- Did teams such as OT, IT, safety, and leadership collaborate effectively, or were silos still an obstacle?

Unlike quantitative data, qualitative methods can be challenging to track; however, they provide you with context-rich insights into behaviors, decisions, and communication dynamics that numbers alone can't explain. Qualitative analysis can also be applied during real incidents by capturing observations from incident responders, noting decision-making patterns, or documenting communication flows in real time. This information becomes invaluable during post-incident reviews, helping you identify strengths, gaps, and opportunities for improving processes and response strategies.

Table 11.1 summarizes the two methods, outlining their purpose and providing examples for each.

Category	**Parameter**	**Purpose**	**Example**
Quantitative	Mean Time to Detect (MTTD)	Measures detection speed for incidents.	SOC detection for OT malware within 15 minutes of alert
Quantitative	Mean Time to Resolve (MTTR)	Evaluates recovery efficiency.	OT system restored within 2 hours after a network intrusion
Quantitative	SLA Compliance Rate	Tracks adherence to agreed timelines.	95% of incident tickets closed within the 24-hour SLA
Qualitative	Clarity of Roles	Evaluates role awareness during an incident.	Team members correctly identify who handles containment, communication, and reporting during a ransomware simulation
Qualitative	Effectiveness of Communication	Reviews communication speed and accuracy.	Incident updates shared in real time via Google Meet and ICS dashboards without errors
Qualitative	Cross-Functional Coordination	Assesses collaboration between departments.	IT, OT, and Facilities teams jointly execute shutdown procedures smoothly during a simulated ICS failure

Table 11.1 – Mapping exercise evaluation metrics

In the next section, we'll shift our focus to **Post-Incident Reviews (PIRs)**, where these methods are applied to gain a clearer understanding of what worked well and where gaps may exist. By combining quantitative metrics with qualitative feedback, PIRs help create actionable insights to strengthen processes, improve communication, and enhance future incident response efforts.

Post-incident review

The **Post-Incident Review (PIR)**, often called a *hot wash*, is one of the most important steps in the exercise cycle. It's the point where the organization pauses to analyze what happened, what worked, what didn't, and what needs to change. This step typically leads to an AAR, turning raw observations into actionable improvements that build stronger preparedness for future incidents.

A PIR is usually conducted as a facilitated discussion immediately after the exercise while the events are still fresh in everyone's minds. It often involves all key participants, including active roles (such as responders and coordinators) and passive roles, such as observers, evaluators, or vendor partners, to ensure every perspective is captured.

During the exercise, a **scribe** or dedicated note-taker, sometimes multiple people, should carefully record all relevant communications, decisions, key actions, and notable events.

Capturing these details is critical for the following reasons:

- It provides a timeline of events for analysis
- It helps identify unanswered questions or assumptions that need to be resolved
- It documents successful responses that should be reinforced in future playbooks

The output of this review can take several forms, depending on the audience, purpose, and depth of analysis required. Common documentation methods include *presentations*, *summary briefs*, *dashboards*, *visual timelines*, and even *interactive reports*. However, the two most commonly used and widely recognized formats are as follows:

- **Executive summary report**: A concise, high-level overview highlighting key takeaways, successes, and areas for improvement. This format is tailored for senior leadership or executive teams who need clear insights without excessive technical detail.
- **AAR**: A comprehensive document that includes detailed timelines, performance metrics, identified gaps, lessons learned, and recommended corrective actions. This report often serves as part of the organization's continuous improvement process and acts as a benchmark reference for future exercises, audits, or incident responses.

Reviewing the PIR of a multi-site exercise requires a structured approach to distinguish local issues from organization-wide lessons. After a complex exercise spanning several facilities, some findings will point to improvements needed at a specific site, whereas others will demand changes at the enterprise level. It's important to separate these in the AAR.

For instance, one plant might need additional technician training, while the company as a whole might need a policy update or an architecture change (such as redesigning a network interconnection) to benefit all sites. You can consolidate lessons learned into categories to ensure that local corrective actions (handled by the site) are tracked alongside broader fixes (owned by corporate teams). The most effective multi-site post-exercise reviews result in a centralized improvement plan that covers the entire organization. This plan should clearly assign ownership for each recommended action, whether to a site manager, a regional coordinator, or a corporate executive, and set timelines for implementation. This way, even though the exercise took place across multiple locations, the follow-up is coordinated and consistent everywhere.

Exercise: Planning your first exercise

This exercise is designed to help you translate incident management theory into practical application. It intentionally blends a traditional safety event with a concurrent OT cybersecurity incident, reflecting the reality that industrial incidents rarely occur in isolation. The objective is not to achieve a perfect outcome, but to surface gaps, assumptions, and decision-making challenges across safety, operations, OT, and IT.

By completing this exercise, you should be able to do the following:

- Evaluate how safety-driven decisions impact OT and IT incident response activities
- Practice escalation and coordination between OT, IT, and plant leadership during a compound incident
- Assess preparedness for isolating OT network segments without disrupting life-safety functions
- Identify communication bottlenecks that emerge when multiple response teams operate simultaneously

This is a functional exercise. No physical actions are required. Participants should walk through decisions, communications, and escalations as if the incident were real.

Scenario overview

You are part of the incident response team at a mid-sized chemical manufacturing facility. During normal operations, a fire alarm is triggered in one process unit, requiring partial evacuation. Almost simultaneously, the control room reports abnormal behavior in the DCS.

The incident begins as a safety event, but quickly escalates into a combined safety and cybersecurity situation. Leadership must prioritize personnel safety while ensuring that the control systems remain stable and protected from further compromise.

Assumed environment

Consider the following details for the organization:

- The facility operates a segmented OT network with a dedicated control network, an OT DMZ, and limited connectivity to the corporate IT network
- The DCS supports both safety-critical and production-related functions
- The organization has an established but untested OT/IT incident escalation procedure
- External responders (fire department) are available and familiar with the site layout, but not the OT architecture

Roles for the exercise

Assign or assume the following roles. One person may play multiple roles if working through this individually.

- **Incident Commander**: Overall authority for incident decisions
- **Safety Officer**: Responsible for personnel safety and evacuation decisions
- **Control Room / Operations Lead**: Manages process stability and operator actions
- **OT Technical Lead**: Assesses control system integrity and network behavior
- **IT / Cybersecurity Lead**: Evaluates potential cyber threats and external indicators
- **Communications Lead**: Coordinates internal and external communications

Exercise injects

Work through the injects in sequence. After each inject, pause and answer the discussion questions before moving on.

Inject 1: Fire Alarm and Initial Evacuation: A fire alarm activates in Unit B. Smoke is reported near a **motor control center (MCC)**. Operators initiate evacuation procedures for the affected area. Here are the discussion points:

- Who assumes Incident Commander responsibilities at this stage?
- What systems must remain operational during evacuation?
- How is the control room informed, and what authority do they retain?

Inject 2: Abnormal OT Network Activity: While evacuation is underway, the OT engineer notices a sudden spike in network traffic on an OT switch connected to the DCS environment. Here are the discussion points:

- At what point does this become a cybersecurity incident?
- Who is notified first: IT, OT leadership, or plant management?
- What information is required before making any network isolation decisions?

Inject 3: Partial DCS Degradation: Several HMI screens freeze briefly. Operators report delayed feedback from field devices, but safety interlocks remain functional. Here are the discussion points:

- How do safety priorities influence cyber response actions?
- Is it acceptable to isolate parts of the OT network during evacuation?

Inject 4: Ransomware Indicator: IT reports that a known ransomware signature has been detected on a system in the OT DMZ. There is no confirmation yet that controllers are impacted. Here are the discussion points:

- How is this information communicated to the Incident Commander?
- Does the presence of external malware change the evacuation strategy?
- What is the threshold for engaging external cybersecurity support or law enforcement?

Communications exercise

Identify the following:

- Primary communication channels used during each phase of the incident
- Backup methods if primary channels fail
- How information is shared with external responders without overwhelming them with technical detail
- Document where delays, confusion, or conflicting messages occurred

Evaluation criteria

Use the following to self-assess or facilitate group discussion:

- Quantitative considerations
- Time to recognize cyber involvement

- Time to escalate from operations to executive awareness
- Qualitative considerations
- Clarity of decision authority
- Effectiveness of OT–IT collaboration
- Alignment between safety and cybersecurity priorities

Post-exercise reflection

Answer the following questions:

- What assumptions about safety versus cybersecurity were challenged?
- Where did existing procedures help, and where did they slow the response?
- Which roles experienced the most conflict or ambiguity?

Deliverables

Produce a short, written summary (1–2 pages) that includes the following:

- Key decisions made during the exercise
- Identified gaps in procedures, training, or tooling
- At least three corrective actions that can be implemented within 30–60 days

This deliverable should be suitable for sharing with plant leadership and used as input for future tabletop or live exercises.

What changes when this same incident happens across multiple sites? This is discussed next.

From single-site execution to multi-site reality

The exercise you just completed was intentionally designed as a single-site scenario. This mirrors how most organizations begin their exercise programs and, more importantly, how real incidents often start, localized, ambiguous, and constrained by on-site resources.

However, the same incident does not remain simple once it crosses site boundaries. Shared services, centralized decision-making, enterprise communication platforms, and competing operational priorities introduce an entirely new layer of complexity.

To guide this process, we'll be using the Exercise Planning Matrix, *Table 11.1*, which outlines the key differences in planning, command structure, communication tools, and evaluation methods for single-site versus multi-site scenarios.

Planning Aspect	**Single Site**	**Multiple Sites**
Exercise Scope	Localized to one facility or plant	Expands to interconnected facilities, shared services, and enterprise-wide operational impacts.
Command Structure	Internal ICS team or department-based ICS	Unified or corporate command coordinating multiple site-level Incident Commanders and priorities.
Inject Design	Specific to single-site risks and response timelines	Coordinated or staggered injects that test cross-site escalation, prioritization, and information flow
Communication Tools	Site-level radios, internal alerting systems, email	Enterprise-wide platforms (Teams, Zoom, Hybrid EOCs)
Team Involvement	Facility teams, local OT/IT support	Broader participation, including corporate security, legal, communications, executive leadership, and external partners.
Evaluation Method	Site-specific metrics, qualitative feedback	Comparative site performance metrics, cross-site feedback
Post-Exercise Review	Internal debrief with localized corrective actions	Joint after-action review, centralized improvement plan

Table 11.2 – Exercise planning matrix: single- versus multi-site coordination

This matrix provides a moment to step back from the single-site exercise and examine how the same incident would change once it extends beyond a single facility. While the core planning elements remain the same, their impact increases as the scope expands to include shared systems, enterprise dependencies, and competing priorities across locations. Command structures evolve from direct, site-level control to coordinated leadership; injects must account for timing and escalation across sites, and communication becomes as much an organizational challenge as a technical one. Evaluation and post-exercise review likewise shift from localized lessons learned to enterprise-wide insights that strengthen preparedness and coordination for future incidents.

Summary

In this chapter you examined how to build effective incident management exercises. We started by reviewing single-site considerations and used the same to expand to multi-site responses. Exercises need to reflect real operational risks, people, and systems, and the key elements that make them useful, such as scope, roles, injects, and communication should be clear and realistic. The chapter also highlighted how teams make decisions under pressure, where coordination breaks down, and how to turn those lessons into real improvements. Finally, we tied all concepts together with a practical exercise that combined a safety event with an OT cybersecurity incident, encouraging you to think through priorities, coordination, and escalation.

Chapter 12, ICS Resources, provides you practical tools and references to support real-world incident response and exercise planning.

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

12

ICS Resources

This is the final chapter, and it aims to provide you with practical resources that you can use to run your incident response efforts as well as to plan ICS exercises. In today's fast-moving technology landscape, threats to **IACS** and CI are becoming more complex and far more destructive.

As discussed in *Chapter 2*, the concept of a *license to operate* goes far beyond compliance or maintaining system uptime. In today's environment, a single cybersecurity event can halt production, endanger people, trigger environmental consequences, and severely damage reputation. Preparation is no longer optional; it is the starting point.

Strong incident management for IACS requires readiness on two fronts: ensuring operational continuity while safeguarding health, safety, and the environment.

To make this easier to understand and apply, the resources have been divided into two categories:

- **Internal resources** that translate strategy into daily action and give responders tools they can use under pressure
- **External resources** that provide regulatory guidance, proven frameworks, and industry-wide lessons

This chapter starts with the internal resources every organization should build and maintain, and then highlights the external sources available to support them. The following topics will be covered:

- Internal readiness tools
- Exercise inject libraries
- Federal and state ICS resources

- Industry standards and best practice groups
- Forms and job aids

Internal readiness tools

Most organizations today rely on a mix of traditional on-premises file servers, such as Microsoft Windows Server and Microsoft SharePoint, and cloud-based systems for file sharing and document management. Reliable access to these resources is critical, especially during response operations. For our discussion, this collection of tools will serve as the central repository, regardless of platform, vendor, or system type, where essential information can be found.

In this section, we will break these resources down into practical and tangible document types, because organizations must translate strategy into usable tools. Internal resources provide the structure needed to make responses repeatable, consistent, and adaptable under stress.

Internal resources are often generated during assessments, particularly when conducting exercises or responding to real-world incidents. They frequently emerge as action items in **After-Action Reports** (**AARs**), evolving into documented lessons learned and practical guides for future readiness.

We can categorize internal readiness tools into a few key types that support day-to-day incident management, as shown in *Figure 12.1*.

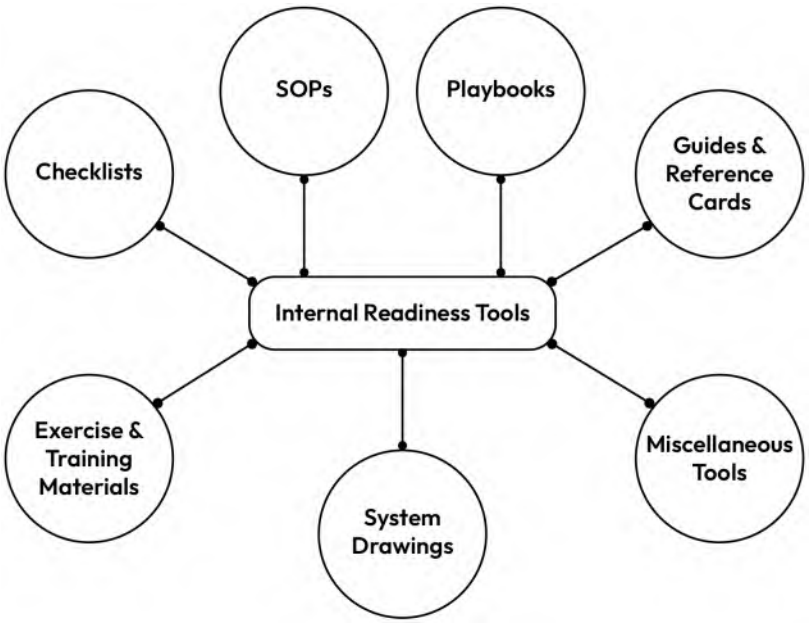


Figure 12.1 – Core categories of internal readiness tools used for ICS incident management

These include the following:

- **Checklists**: Concise reminders that ensure essential steps aren't overlooked
- **Standard Operating Procedures (SOPs)**: Detailed, repeatable instructions for recurring tasks
- **Playbooks**: Scenario-driven guides for specific incident types
- **Guides and Reference Cards**: Quick-access escalation trees, classification schemes, and diagrams
- **Exercise and Training Materials**: Tabletop injects, hot wash templates, and training aids
- **System Drawings**: Network topologies, **piping and instrumentation diagrams (P&IDs)**, and architecture diagrams
- **Miscellaneous Tools**: Contact lists, notes, and ad hoc job aids

Checklists

Checklists are concise, step-by-step reminders that ensure critical actions are not overlooked. They are common in business and project management, but in incident management for **CI**, they have a special advantage: they are often tested in exercises or real incidents. This means even staff with limited technical expertise can follow them under stress and still achieve reliable results.

By reducing reliance on memory, checklists improve speed, consistency, and accountability during crises. They act as a safety net, ensuring responders take the right steps in the right order.

For example, the Endpoint Security Checklist shown in *Figure 12.2* provides a simple, step-by-step set of actions designed to protect individual workstations from compromise:

Figure 12.2 – Endpoint Security Checklist example

It focuses on ensuring that key security controls, such as antivirus/EDR agents and local firewalls, are active and current, while also outlining immediate response measures such as disconnecting compromised machines, running malware scans, and preserving logs. By including notification of the SOC or Incident Commander, this checklist ensures that both technical and organizational responses are aligned, making it a practical tool even for non-expert staff to follow during an incident.

Some of the common checklists used in the industry include the following:

Physical security checklist

- Inspect access control systems (badges, biometric readers)

Ensure doors to control rooms and **Motor Control Centers** (**MCCs**) are locked

- Confirm security cameras are functioning and recording
- Log all visitors and contractor entries
- Report any unauthorized access attempts immediately

Network/OT device checklist

- Validate firewall rules against the approved baseline
- Check PLC/RTU firmware versions against vendor advisories
- Confirm backups are current and stored offline
- Inspect switch configurations for unauthorized changes
- Ensure secure remote access (VPN with MFA) is enforced

SCADA system recovery checklist

- Reboot HMI servers one at a time
- Validate historian data integrity
- Confirm alarm/event logs are functioning
- Run water/chemical dosing control checks before going live
- Sign-off from Operations and OT Security before resuming automated control

Other checklists that are common

- Startup/shutdown checklists: Validate that critical safety and cybersecurity measures are in place
- Incident response checklists: Initial containment, notification, and escalation actions
- Recovery checklists: Verification steps for restoring systems safely

Standard Operating Procedures (SOPs)

Standard Operating Procedures (SOPs) are detailed, step-by-step instructions that describe how to consistently perform a recurring task or process. Unlike checklists, which provide concise reminders, SOPs capture the full context, prerequisites, responsibilities, and escalation paths for operational activities. They are formal documents designed to standardize work across teams and ensure reliability, safety, and compliance. In some organizations, SOPs may also be referred to as **Knowledge Base (KB)** documents, since they serve as a reference library for how tasks are performed and problems are resolved.

In CI sectors (such as water utilities, power generation, chemical processing, and transportation), SOPs are the backbone of operations. They define how to safely and securely do the following:

- Start up, run, and shut down complex systems such as SCADA, PLCs, and HMIs
- Perform routine maintenance, calibrations, and inspections on critical assets
- Manage patching, backups, and access control in OT environments
- Coordinate response during abnormal conditions or failures (cyber or physical)

For example, an SOP might detail how an operator should validate water treatment chemical dosing systems during daily rounds, or how engineers should apply vendor firmware updates without disrupting production.

Figure 12.3 shows an example of an SOP used in OT systems, specifically the first page of a formal SOP for **ABC Company LLC — Water Utility**:

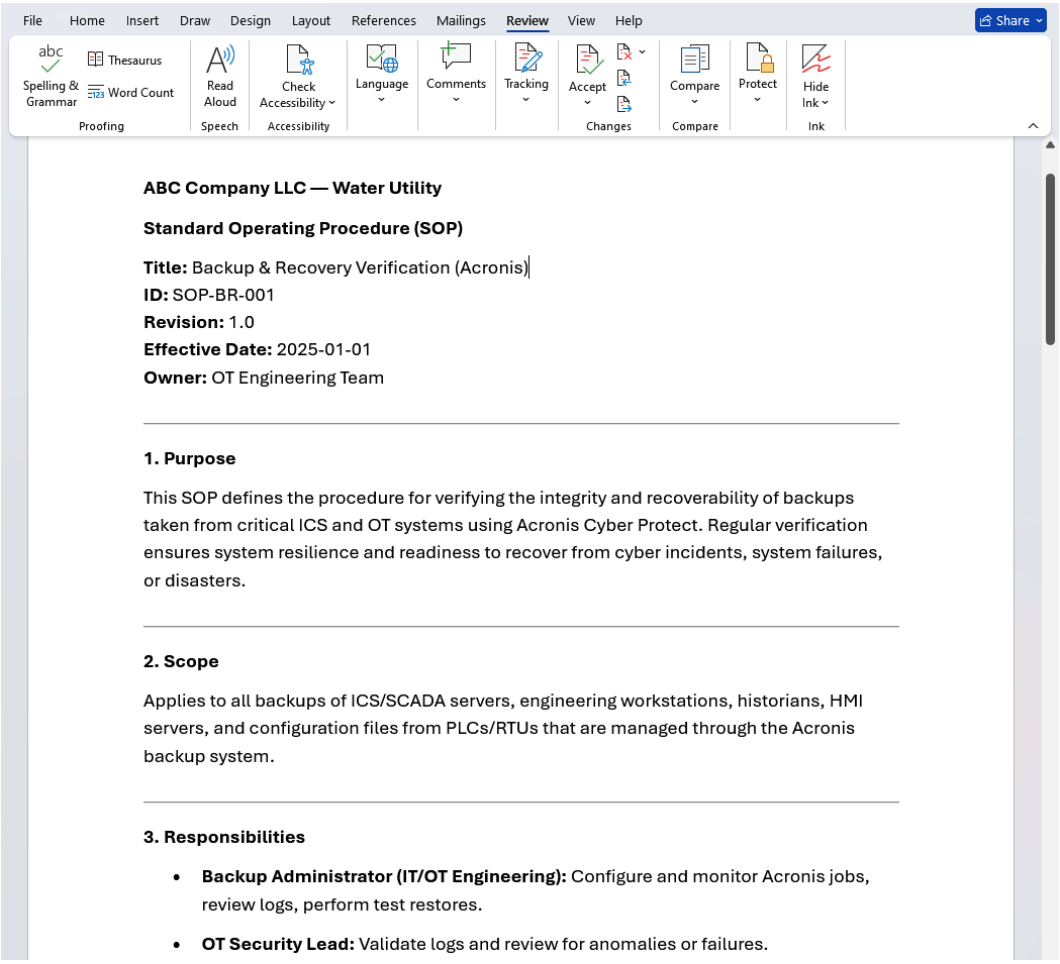


Figure 12.3 – Screenshot of an SOP for backup of OT systems

The SOP, titled **Backup & Recovery Verification (Acronis)**, includes key metadata such as ID, revision number, effective date (January 1, 2025), and the designated owner or department – in this case, **OT Engineering Team**. The opening sections outline the purpose, which is verifying backup integrity and recoverability using the backup tool, **Acronis Cyber Protect**; the scope, which applies to ICS/SCADA servers and related OT systems; and the responsibilities, which assign tasks to roles such as the Backup Administrator and OT Security Lead. In practice, this SOP may also define testing procedures for backups, reporting requirements for audits, and documentation protocols to ensure compliance. Such an SOP is especially valuable during incident response – for example, in a ransomware scenario where primary systems may be encrypted or compromised.

Having clearly documented backup verification processes ensures responders can rapidly restore, clean, and validate system states, minimizing downtime and maintaining operational continuity while also providing evidence for audits or post-incident reviews.

Other commonly used SOPs are as follows:

- **Patch and update management in OT**: Defines how to review advisories, schedule updates, test patches in staging, and apply them safely to ICS/SCADA systems
- **Establishing secure vendor remote access**: Standardizes how vendors are granted, monitored, and revoked access with VPN, MFA, and logging requirements
- **Change management for control systems**: Outlines steps for requesting, approving, and implementing changes to PLC logic, SCADA configurations, or firewall rules

Playbooks

The term playbook is often overused in discussions about incident management, but in the context of **CI**, it has a very specific and valuable meaning. A playbook is a scenario-specific guide that combines technical steps, decision points, and communication protocols to respond to a defined type of incident.

Unlike SOPs, which provide detailed instructions for recurring routine tasks, playbooks are situational. They outline what to do when something goes wrong – such as ransomware on an engineering workstation, a misconfigured firewall, or a vendor remote access compromise.

An effective playbook should be the following:

- **Practical and action-oriented**: Clear enough to be used under pressure, even by non-experts
- **Scenario-specific**: Focused on a single threat or failure type rather than generic instructions
- **Cross-functional**: Covering both technical response and communication/escalation
- **A living document**: Updated regularly after exercises, audits, and real-world incidents
- **Tested**: Validated through tabletop exercises and drills, so responders trust it when needed

Some of the commonly maintained playbooks are as follows:

- **Ransomware on engineering workstation**: Steps for isolating affected endpoints, preserving forensic data, and restoring from backups
- **Vendor remote access compromise**: Actions to disable compromised accounts, block IPs, coordinate with the vendor, and validate system integrity

- **Firewall misconfiguration**: Procedure for rolling back changes, verifying network segmentation, and restoring connectivity safely
- **Insider threat detection**: Response guide for when suspicious user activity suggests an insider may be tampering with systems or data
- **SCADA data historian corruption**: Playbook for restoring historian databases, validating integrity, and resuming reporting functions

Let us look at an example of a ransomware on engineering workstation playbook. *Figure 12.4* shows an example of an incident response playbook used in OT systems, specifically the first page of a formal playbook for **ABC Company LLC - Water Utility**:

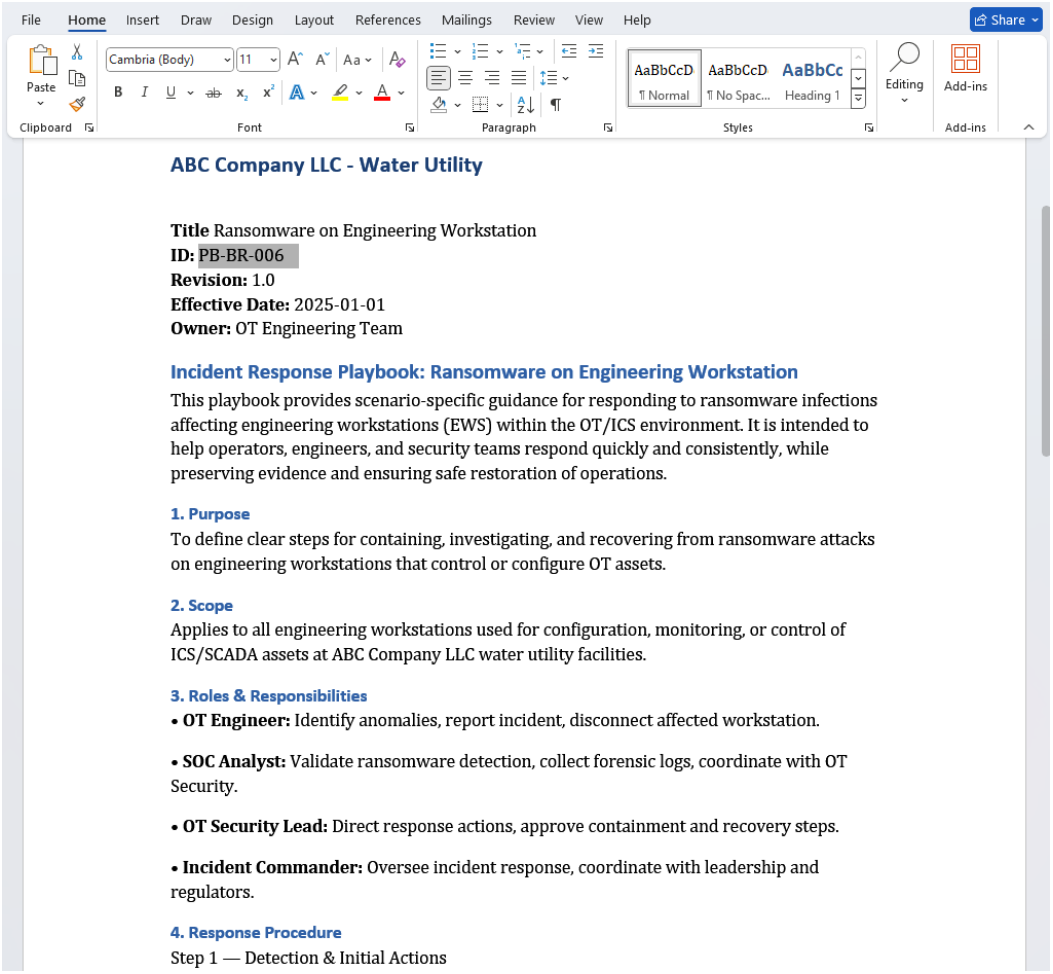


Figure 12.4 – Screenshot of the sample incident response playbook: Ransomware on Engineering Workstation

The playbook titled **Ransomware on Engineering Workstation** includes key information such as document ID, revision number, effective date, and the designated owner or department – in this case, **OT Engineering Team**. The opening sections outline the purpose, which is to define steps for containing, investigating, and recovering from ransomware attacks on engineering workstations; the scope, which applies to all workstations used for configuration, monitoring, or control of ICS/SCADA assets; and the roles and responsibilities, which assign tasks to personnel such as the OT Engineer, SOC Analyst, OT Security Lead, and Incident Commander. The response procedure, which is not visible in this screenshot, typically contains detection and initial actions, emphasizing immediate isolation and reporting requirements.

In practice, this type of playbook serves as a living document, updated after exercises or incidents, and provides operators and security staff with actionable guidance during a crisis. By documenting containment, recovery, and communication steps in advance, playbooks help ensure consistent, cross-functional response, reduce downtime, and build confidence that CI operations can be safely restored after a disruptive cyber event.

Guides and reference cards

These are quick-access tools that improve speed, consistency, and coordination during incidents. They provide responders with concise, standardized information that can be acted upon without delay. Examples include escalation trees, which identify who to contact and in what order; network and asset diagrams, which highlight zones, conduits, and critical systems; and classification guides, which define incident severity levels and outline the appropriate response triggers.

In an incident response scenario – for example, a ransomware attack – these guides reduce uncertainty and prevent wasted time. An escalation tree ensures that decision-makers and technical experts are engaged immediately. Network and asset diagrams help responders quickly understand the affected systems and prioritize recovery. Classification guides ensure incidents are categorized consistently, allowing the right playbooks and resources to be activated without hesitation. Together, these references ensure responders act decisively, minimizing confusion and downtime when every minute counts.

Figure 12.5 shows an example of a decision-making tree for ransomware isolation in ICS networks, used in our fictitious **ABC Company LLC — Water Utility**.

Figure 12.5 – A quick access card, part of a visual reference for calling OT Support for operators

The document includes a structured flow that guides responders through identifying affected networks, assessing criticality, taking containment actions, and initiating recovery. This visual playbook emphasizes isolating compromised assets quickly while maintaining critical water treatment operations, ensuring both containment and operational continuity.

Another important type of reference diagram in OT security is the network diagram. These may range from simple high-level drawings that show the overall ICS/IT boundary to detailed schematics that illustrate switches, firewalls, and individual asset connections. Network diagrams can be created in different forms – for example, logical diagrams highlight trust zones and data flows, while physical diagrams focus on hardware placement and cabling.

Figure 12.6 shows an example of a network architecture drawing, emphasizing the use of network segmentation to separate business IT systems, DMZ layers, and control networks.

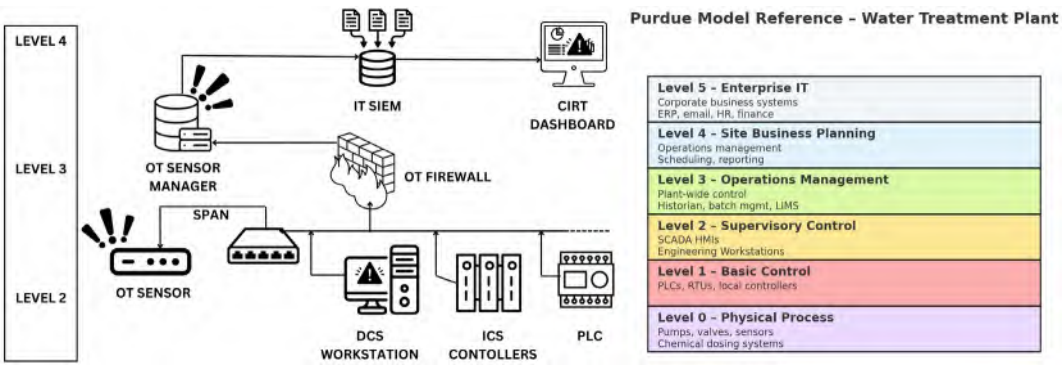


Figure 12.6 – Example of a network architecture diagram for OT security, showing segmentation between corporate IT, DMZ layers, and control networks

Such diagrams are particularly valuable during an incident: they are used by OT Engineers, security teams, and Incident Commanders to quickly identify affected segments, trace data paths, and determine the safest way to isolate compromised systems without disrupting critical operations.

Several other system diagrams provide essential context for both operations and incident response. For instance, **Piping and Instrumentation Diagrams (P&IDs)** show how chemicals, pumps, and valves interact in treatment processes. **Process Flow Diagrams (PFDs)** depict the overall process design, material flow, and major equipment relationships and are useful for understanding where disruptions might propagate. **Electrical single-line diagrams** map power distribution across control rooms, substations, and motor control centers. **Logical zone and conduit diagrams** illustrate trust boundaries and communication paths across OT/IT networks. Finally, **asset topology maps** document the placement of key devices and critical nodes.

These documents collectively serve as blueprints for *situational awareness*. During incident response, they allow teams to isolate compromised segments, validate operational integrity, and restore systems with confidence. As part of a preparedness library, system diagrams should be kept **current, version-controlled**, and **cross-referenced with SOPs, playbooks, and checklists**.

Start small and build one checklist, one SOP, and one playbook targeting your top three risks. Expand gradually through exercises and lessons learned.

Digital repositories such as intranets, SharePoint, or secured file servers are an effective way to organize and centralize critical resources, including checklists, SOPs, playbooks, and reference documents. They provide structure, enable quick searching, and make version control easier to manage.

As shown in *Figure 12.7*, resources can be neatly arranged into folders by type, with clear labeling, ownership, and metadata such as modification dates:

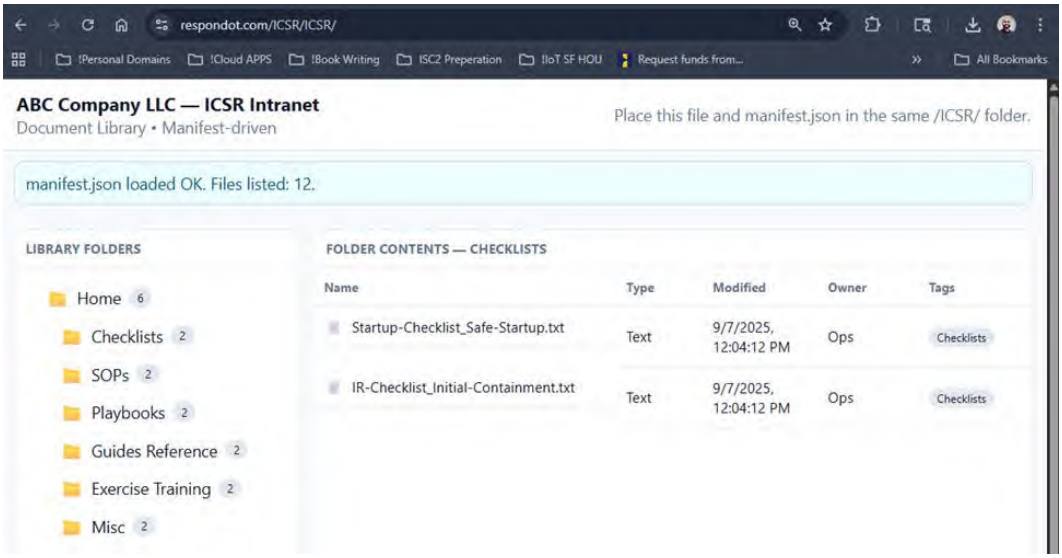


Figure 12.7 – Example of a digital repository (such as SharePoint) used to organize and store resources for an emergency operations center

This allows responders to quickly locate the right document during an incident without wasting valuable time navigating cluttered systems.

However, while these repositories improve efficiency, they should never be relied upon exclusively. In the event of a cyberattack or outage, digital access may be disrupted. Maintaining offline copies, whether in printed binders or easily exportable formats, ensures critical procedures remain accessible under any circumstance.

Finally, regulatory bodies often require organizations to demonstrate that materials are up to date and readily accessible during audits. A well-maintained repository not only supports response readiness but also provides tangible evidence of compliance, making audits smoother and reducing the risk of penalties.

While checklists, SOPs, playbooks, and system diagrams provide the structure for how to respond, exercises need a way to simulate real-world disruptions that test those resources in action. This is where **injects** come in.

We defined **injects** in earlier chapters, but here it's worth emphasizing that they are an essential resource during any tabletop, functional, or full-scale exercise. A well-crafted inject ensures participants are challenged to do the following:

- Make decisions with incomplete or evolving information
- Coordinate across technical and leadership roles
- Validate playbooks, checklists, and procedures in practice
- Reveal gaps in planning, communication, or technical response

Injects are used by the facilitator of an exercise to move the scenario forward, challenge participants, and create opportunities for learning. They are not meant to *trick* participants but to simulate realistic disruptions that force decision-making under pressure.

The following are best practices for using an inject:

- **Introduce at the right time**: The facilitator presents the inject according to the exercise timeline (e.g., "T+35 minutes"). Timing matters, as injects are used to escalate or pivot the exercise when participants are ready.
- **Frame the scenario**: The facilitator reads or distributes the inject narrative (e.g., "Logs show an operator accessing restricted PLC programming files outside of normal shift hours…"). This sets the scene for participants.
- **Encourage discussion**: The facilitator prompts participants with questions such as the following:
    - What actions would you take first?
    - Who would you notify?
    - Do we have the right checklist or SOP to handle this?
    - What if this escalated further?
- **Observe and capture gaps**: The goal is not just to "solve" the inject but to see whether participants follow existing playbooks, improvise, or encounter roadblocks. These observations become valuable lessons learned.
- **Drive learning outcomes**: After the discussion, the facilitator summarizes: Were the right roles activated? Did communication flow as expected? Did procedures exist, and were they clear?

In the example shown in *Figure 12.8*, the **Insider Threat Activity** inject pushes participants to consider both technical and organizational responses:

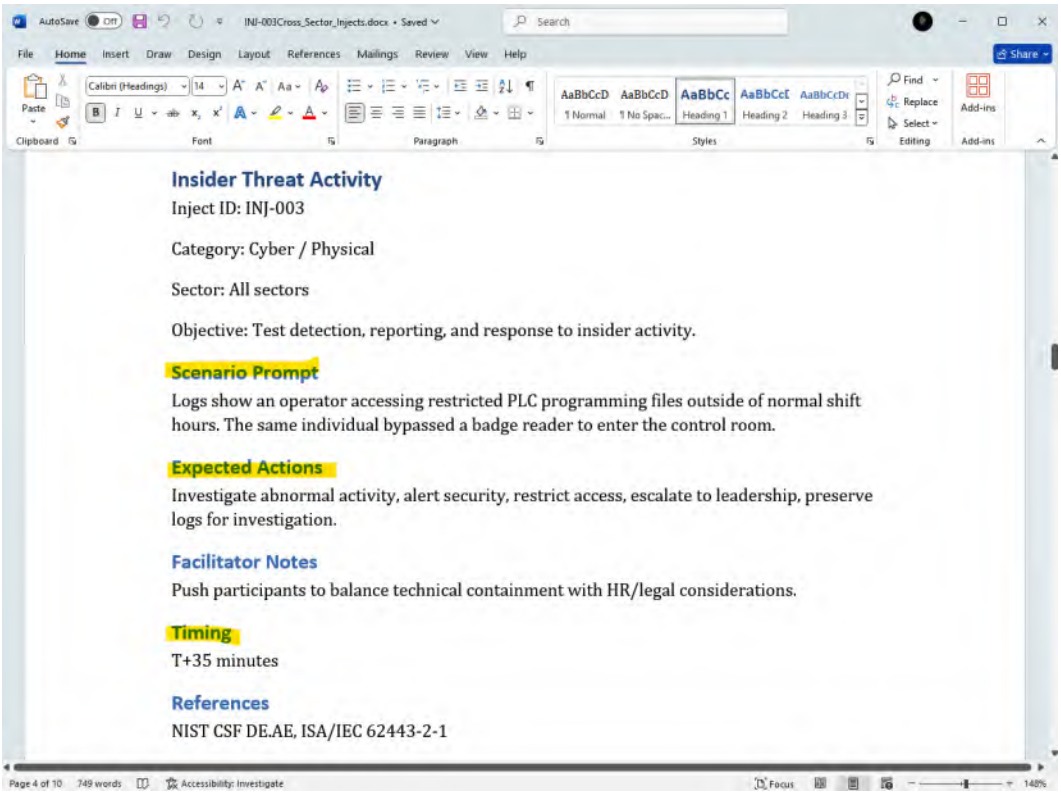


Figure 12.8 – Insider Threat Activity inject used in an exercise

It forces them to balance technical containment (restricting access, preserving logs) with HR and legal implications (addressing insider behavior, engaging leadership). This way, injects ensure exercises are not abstract conversations but realistic tests of readiness.

While every organization is unique, with its own environment, processes, and risk profile, the value of well-designed injects remains universal. Organizations can always create their own tailored injects to match their context, but there is also a set of cross-sector injects that prove useful across industries. These injects address the most common forms of threats and add immense value by helping teams practice responses to scenarios that are frequently encountered in the real world. These can be viewed or downloaded online: `https://durgeshkalya.com/icsbookresources/`. To help facilitators design realistic and meaningful exercises, the following

examples highlight common injects that reflect real-world challenges frequently encountered across IACS environments. Each inject represents a scenario that can be tailored to your facility's risk profile, operational setup, and maturity level.

- **Ransomware on engineering workstation**: Simulates malware infection that encrypts configuration files and halts engineering activity, testing backup integrity and containment response
- **Phishing email compromise**: Explores how credential theft through deceptive emails can lead to unauthorized system access or financial fraud
- **Insider threat activity**: Focuses on intentional or accidental misuse of access privileges by authorized personnel
- **SCADA/HMI loss of visibility**: Examines how operators respond when monitoring systems go dark, requiring manual coordination and safety validation
- **Vendor remote access compromise**: Tests procedures for managing third-party connectivity and remote maintenance security
- **Backup/recovery test failure**: Highlights the importance of validating recovery systems before an incident occurs
- **Supply chain/software update Trojan**: Demonstrates the cascading effects of compromised software or firmware updates
- **Physical security breach with cyber implications**: Integrates physical intrusion scenarios with potential cyber exposure or equipment tampering

Each of these injects can be implemented in tabletop or functional exercises to test specific decision-making pathways, communication flow, and procedural readiness.

For step-by-step instructions, sample narratives, and discussion prompts, refer to the file named *Chapter 12: Exercise Inject Reference Guide*, available in the online resource library: `https://durgeshkalya.com/icsbookresources/injects.html`

For reference, additional inject libraries and examples are publicly available through **CISA's Tabletop Exercise Packages (CTEP)**:

`https://www.cisa.gov/resources-tools/resources/election-security-cisa-tabletop-exercise-packages-cteps`

External readiness tools

While internal tools provide the *how*, federal and state resources deliver the *why* and *what* of incident management and response. They define the frameworks, regulations, and guidance that shape how incident management is approached across CI sectors. By leveraging these resources, organizations ensure their programs are not only operationally effective but also aligned with broader national and global security strategies. The following subsection discusses these in detail.

Federal and state ICS resources

CISA ICS-CERT offers vulnerability advisories, alerts, and mitigation recommendations specific to industrial systems. These advisories are trusted across industry because they aggregate vendor input, lab validation, and federal analysis. Details can be found here: `https://www.cisa.gov/news-events/cybersecurity-advisories`.

ICS4ICS is a FEMA-inspired model for structured ICS incident management, adapted for OT environments to provide a common structure for response. Here are the relevant links.

- `https://www.ics4ics.org/exercises`
- `https://gca.isa.org/blog/ics4ics-will-improve-management-of-ics-cybersecurity-incidents`

Regional and state-level support

CISA also provides regional support. It operates through 10 regional offices across the United States, each staffed with **Protective Security Advisors** (**PSAs**) and **Cybersecurity Advisors** (**CSAs**) who provide localized assistance to CI owners and operators. They offer services such as risk assessments, tailored technical assistance, training, exercises, and real-time incident response support. These regional teams serve as trusted liaisons, helping CI organizations navigate both preparedness and emergent threats with region-specific expertise and coordination. For more localized support and direct contacts, see the CISA Regions page: `https://www.cisa.gov/about/regions`.

InfraGard Members Alliances (**IMAs**), commonly known as *InfraGard Chapters*, are non-profit organizations affiliated with local FBI Field Offices across the United States. There are over 70 IMAs nationwide, each staffed by volunteers from CI sectors and supported by a dedicated FBI Private Sector Coordinator. These chapters serve as the frontline of public-private information sharing hosting local meetings, educational events, and regional programming that are tailored to specific threat environments and industries. More information can be found here: `https://www.infragardnational.org/about-us/infragard-chapters/`.

The **Homeland Security Information Network – Critical Infrastructure (HSIN-CI)** is a collaboration platform for private and public sector operators to share situational awareness and incident updates: `https://www.dhs.gov/homeland-security-information-network-hsin`

The **Federal Emergency Management Agency (FEMA)** provides frameworks such as the **Homeland Security Exercise and Evaluation Program (HSEEP)** and the standardized ICS forms, covered in the next section, widely used in cross-sector response.

ICS forms

ICS forms are standardized templates developed by FEMA to help responders document incident objectives, actions, and resources. They create a common structure and make it easier for teams from different agencies or organizations to work together. During an incident, these forms guide communication, decision-making, and documentation in a consistent way. The following are a few important ICS forms that are commonly used during incident response and planning. These examples also show how they are applied in real situations.

The **ICS 201 Incident Briefing Form** is usually the first form completed at the start of an incident. It captures what is known about the situation, the immediate actions taken, and the initial set of priorities. When new personnel arrive, this form helps them understand the current conditions and the overall picture without needing long explanations.

The **ICS 213 General Message Form** is used to send messages or document requests between teams. It keeps communication organized and creates a written record. It is very helpful during long or complex events where information can easily be lost if it is not documented properly.

ICS 214 Activity Log records actions, observations, and decisions throughout the incident. Every section and individual responder can maintain an ICS 214. It becomes extremely valuable during after-action reviews and for understanding how events unfolded over time. In OT environments, this form helps track technical changes, troubleshooting steps, and operational decisions.

The **ICS 215 Operational Planning Worksheet** form supports the planning process. It helps identify the resources needed for the next operational period and outlines what the teams are expected to accomplish. It brings structure to the planning cycle and helps leadership make informed decisions about priorities and resource allocation.

ICS 215A Incident Action Plan Safety Analysis is a companion form that identifies hazards associated with planned operations and outlines mitigation measures. It helps ensure that safety considerations are included before tasks are assigned. This is especially important in industrial and OT environments where safety risks and cybersecurity concerns overlap.

Many organizations use a **Resource Request form** to request personnel, equipment, vendors, or specialist support. It provides a formal way to track requests, approvals, and deployments. It keeps the process transparent and avoids confusion during busy operations.

These are only a few examples. ICS includes many more forms that support planning, logistics, finance, and demobilization. For a complete list and additional details, you can visit the FEMA ICS Forms Library at the link provided here: `https://training.fema.gov/emiweb/is/icsresource/icsforms/`.

ICS Job Aids are role-specific reference guides that give responders clear, step-by-step tasks during an incident: `https://training.fema.gov/emiweb/is/icsresource/jobaids/`

ICS Training Courses are exercise scripts, injects, and evaluation templates designed to prepare staff and validate readiness through practice: `https://training.fema.gov/emiweb/is/icsresource/trainingmaterials/`

Local Emergency Planning Committees (LEPCs)

A **Local Emergency Planning Committee** (**LEPC**) is a community-based group authorized under the federal **Emergency Planning and Community Right-to-Know Act (EPCRA)** (also known as **SARA Title III**) to support emergency planning, especially for hazardous chemicals, and to provide the public with access to information about chemical hazards in their communities.

LEPCs typically include elected officials, first responders (police, fire, EMS), health and environmental professionals, facility representatives, community groups, media, and other stakeholders. They provide a vital bridge between industry, emergency responders, government, and the public. For your ICS-/OT/CI audience, the LEPC is a valuable asset, not just for hazardous-material planning but also for integrating industrial/OT facilities into the broader community response framework. Recognizing the LEPC and engaging with it helps your organization align its incident-management and emergency preparedness plans with the local public-sector structures already in place. More information can be found here: `https://www.epa.gov/epcra/local-emergency-planning-committees`.

While federal and state resources provide the regulatory foundation and structured frameworks for incident response, organizations must also align with industry standards and peer-driven best practices to ensure consistency and resilience. These standards define the technical *how* of implementing security, and **Information Sharing and Analysis Centers** (**ISACs**) extend this by enabling collaboration across sectors.

Industry standards, best practice groups, and ISACs

Industry standards and collaborative groups play a central role in guiding how organizations protect and manage their systems. Standards and frameworks, which were covered in *Chapter 8*, *Incident Management Frameworks*, such as NIST CSF and ISA/IEC 62443, establish structured best practices for security and resilience, while ISACs create trusted channels for sharing real-time threat intelligence across peers in the same sector. Together, they help organizations build consistency, stay ahead of emerging threats, and learn from collective experience. The notable standard bodies are discussed next.

NIST Cybersecurity Framework (CSF) is a risk-based guide for managing cybersecurity across critical sectors: `https://www.nist.gov/cyberframework`

ISA/IEC 62443 are international standards for OT security covering system development life cycles and technical safeguards: `https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards`

The **Center for Internet Security (CIS)** is a nonprofit that offers industry-specific cybersecurity resources such as CIS benchmarks, SecureSuite tools, and threat insights, which are tailored to help organizations meet their unique security and regulatory needs: `https://www.cisecurity.org/industry`.

While primarily focused on cybersecurity rather than incident management, CIS benchmarks and controls are widely adopted across industries and provide a strong foundation for securing systems. Many industrial organizations use CIS as a baseline, adapting its guidance to operational technology environments.

ISACS

Information Sharing and Analysis Centers (ISACs) are trusted, sector-focused organizations that facilitate the sharing of timely, actionable threat intelligence, vulnerabilities, incidents, and best practices among CI owners, operators, and relevant government partners. ISACs are vital for strengthening collective cybersecurity and operational resilience by enabling collaboration across organizations that face similar risks, particularly in sectors that rely heavily on industrial control systems and operational technology. Through information sharing, alerts, advisories, exercises, and coordinated response efforts, ISACs help members better prepare for, detect, respond to, and recover from cyber and physical threats. The following are some of the ISACs operating across the United States and globally that support critical infrastructure and industrial sectors.

United States ISACs (Critical Infrastructure & Industry-Focused)

Here are some US-specific ISACS:

- **Financial Services Information Sharing and Analysis Center (FS-ISAC)**: A global consortium serving the financial sector by sharing cyber threat intelligence to protect banks, credit unions, and financial services firms worldwide. Website: `https://www.fsisac.com/`
- **Multi-State Information Sharing and Analysis Center (MS-ISAC)**: Operated by the CIS, MS-ISAC is a central cybersecurity resource that provides threat alerts, incident support, and risk assessment to U.S. state, local, tribal, and territorial governments. Website: `https://www.cisecurity.org/ms-isac`
- **Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)**: Provides dedicated cyber threat intelligence and resilience support for state, local, tribal, and territorial election officials as part of MS-ISAC membership. Website: `https://www.cisecurity.org/ei-isac`
- **National Defense Information Sharing and Analysis Center (ND-ISAC)**: Focuses on the Defense Industrial Base (DIB) sector, enabling suppliers and defense companies to share cyber and physical threat insights and mitigation strategies. Website: `https://ndisac.org/`
- **Electricity Information Sharing and Analysis Center (E-ISAC)**: Operated under the North American Electric Reliability Corporation (NERC), E-ISAC delivers threat intelligence and coordination for bulk power system owners/operators. Website: `https://www.cisecurity.org/ei-isac`
- **IT-ISAC**: A community of information technology companies sharing cyber threat intelligence, best practices, and operational insights to strengthen cyber defenses across IT domains. Website: `https://www.it-isac.org/`
- **Retail & Hospitality ISAC (RH-ISAC)**: Serves the retail, hospitality, gaming, travel, and consumer sectors by facilitating threat intelligence sharing and security collaboration. Website: `https://www.rhisac.org/`
- **Water ISAC**: Information sharing hub for the water and wastewater sector, focused on strengthening cyber and physical security preparedness and incident response.
- **Website**: `https://www.waterisac.org/`

- **Maritime Transportation System ISAC (MTS-ISAC)**: Facilitates cybersecurity and threat info sharing among maritime stakeholders to reduce risk across ports, shipping, and maritime networks. Website: `https://www.mtsisac.org/`
- **Real Estate ISAC (RE-ISAC)**: Supports commercial real estate and facilities security teams by sharing intelligence on threats affecting buildings, tenants, and visitors. Website: `https://www.reisac.org/`
- **Research & Education Network ISAC (REN-ISAC)**: Provides cybersecurity threat info and automated data sharing tools to universities, colleges, and research institutions. Website: `https://www.ren-isac.net/`
- **Tribal Information Sharing and Analysis Center (Tribal-ISAC)**: Enables tribal governments and enterprises to share threat intelligence, best practices, and coordinated defense information. Website: `https://www.tribalisac.org/`

Global ISACs

Here are some global ISACs:

- **Health-ISAC**: While based in the U.S., Health-ISAC has a global membership and delivers cybersecurity intelligence and collaboration across healthcare organizations internationally. Website: `https://health-isac.org/`
- **European Energy – Information Sharing & Analysis Centre (EE-ISAC)**: A European ISAC that connects utilities, solution providers, and institutions to share cyber resilience information across the EU energy sector. Website: `https://www.ee-isac.eu/`
- **CI-ISAC Australia**: Australia's cross-sector critical infrastructure ISAC focused on collective threat intelligence sharing and resilience within the Australian context. Website: `https://ci-isac.org.au/`
- **CI-ISAC International**: A global initiative extending ISAC capabilities to sovereign nations and promoting federated threat intelligence sharing worldwide. Website: `https://ci-isac.org/`
- **Japan ISACs (multiple by sector)**: Examples include Financials ISAC Japan, ICT ISAC Japan, Power/Electricity ISAC, Medical ISAC Japan, and Transportation ISAC Japan.

Sector-specific regulations

The **Maritime Transportation Security Act** (**MTSA**) has sector-specific rules, such as the *Facility Security Officer Cyber Job Aid*, that support compliance and give facility personnel a practical response reference.

The **MTSA Cybersecurity Regulatory References** (**CFR**) have the following parts:

- **33 CFR Part 101 – Cybersecurity (New Subpart F)**: Establishes minimum cybersecurity requirements for U.S.-flagged vessels, facilities, and OCS facilities regulated under MTSA. Includes mandates for **Cybersecurity Plans, Cybersecurity Officers** (**CySO**), phased implementation, reporting, and more: `https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F`
- **33 CFR Parts 104, 105, and 106 – Existing MTSA Security Plans**:
    - Part 104: Vessel Security Plans: `https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-104`
    - Part 105: Facility Security Plans
    - Part 106: Outer Continental Shelf (OCS) Facility Security Plans: `https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-105`

These remain part of the framework that now incorporates cybersecurity via Subpart F.

The **NVIC 01-20 – Guidance on Cyber Risks** under MTSA is the *Navigation and Vessel Inspection Circular* from the U.S. Coast Guard that interprets cybersecurity inclusion in **Facility Security Assessments** (**FSA**) and **Plans** (**FSP/VSP**). It encourages integrating cyber annexes or governance programs: `https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf`

For the accompanying **Frequently Asked Questions** (**FAQs**), visit this link: `https://www.dco.uscg.mil/Portals/9/Cyber%20NVIC%2001-20%20FAQs_updated%2029%20APR%2022.pdf`

The **U.S. Coast Guard** (**USCG**) issues FAQs to support regulated entities—such as maritime facilities, vessel operators, and security officers in interpreting new or complex requirements. For example, the Cyber NVIC 01-20 FAQs explain how cyber risks should be incorporated into **Facility Security Plans** (**FSPs**) and **Vessel Security Plans** (**VSPs**), offering real-world interpretations, use cases, and compliance tips.

The **North American Electric Reliability Corporation** (**NERC**) represents Critical Infrastructure Protection CIP Reliability and cybersecurity standards for North American electric utilities: `https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx`

The **Chemical Facility Anti-Terrorism Standards** (**CFATS**) is a U.S. DHS regulation for securing high-risk chemical facilities: `https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/laws-regulations`

As of July 28, 2023, Congress allowed the CFATS program's authority to expire, leaving CISA without a legal mandate to enforce its requirements. Facilities are no longer obligated to report chemicals, submit CSAT data, undergo inspections, or implement site security plans. In the meantime, CISA promotes voluntary security through its ChemLock program, while industry groups stress CFATS's past success in significantly improving facility security.

Compliance, governance, and industry regulations

Based on the industry and sector, an organization may or may not have regulatory requirements. However, most organizations in CI fall under some form of regulation. The following presents the industry sectors (CI sectors) and some of the regulations they are subject to:

CI Sector	**Examples of Applicable Regulations / Standards**
Energy (Electricity, Oil, Gas)	NERC CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection) DOE Cybersecurity Capability Maturity Model (C2M2) TSA Pipeline Security Guidelines
Water and Wastewater	EPA America's Water Infrastructure Act (AWIA) AWWA Cybersecurity Guidance NIST Cybersecurity Framework (CSF)
Transportation Systems	TSA Security Directives FAA Regulations (for aviation) USCG Maritime Transportation Security Act (MTSA)
Chemical	CFATS (Chemical Facility Anti-Terrorism Standards) EPA Risk Management Program (RMP)
Healthcare and Public Health	HIPAA (Health Insurance Portability and Accountability Act) HITECH Act FDA Cybersecurity Guidelines
Financial Services	GLBA (Gramm-Leach-Bliley Act) FFIEC Guidelines NYDFS Cybersecurity Regulation

Information Technology	NIST SP 800-series CISA Best Practices FISMA (Federal Information Security Management Act)
Communications	FCC Regulations CISA Sector-Specific Guidelines
Defense Industrial Base	DFARS (Defense Federal Acquisition Regulation Supplement) CMMC (Cybersecurity Maturity Model Certification)
Food and Agriculture	FDA FSMA (Food Safety Modernization Act) USDA Guidelines
Emergency Services	FEMA NIMS (National Incident Management System) DHS Guidelines
Government Facilities	FISMA FedRAMP DHS Protective Security Requirements

Table 7.2: Common CI sectors and examples of key regulations or standards

Understanding these regulations and requirements is essential, as they play a critical role during incident management. Additionally, they should be incorporated into the **Incident Response Plan (IRP)**.

Various components of the regulations can apply during incidents, such as the following:

- Mandatory government or agency reporting (e.g., CISA, DHS, DOE, etc.)
- Time-bound breach notification requirements
- Preservation of evidence for legal and regulatory reviews
- Coordination with sector-specific **Information Sharing and Analysis Centers (ISACs)**
- Documentation and audit trail requirements
- Compliance with recovery timelines or service restoration thresholds

Including these aspects in the IRP ensures the organization meets its compliance obligations while responding effectively to incidents.

Global resources

European Union Agency for Cybersecurity (ENISA) offers technical guidance to support EU member states in implementing the NIS2 Directive, including risk management measures, national cybersecurity strategies, and certification schemes. The agency also publishes best practice guides and maintains the European Vulnerability Database: `https://www.enisa.europa.eu/#contentList`.

You can find the ENISA vulnerability database here: `https://euvd.enisa.europa.eu/`

The **UK National Cyber Security Centre (NCSC)** acts as the UK's technical authority for cyber threats, offering operational guidance for OT/ICS systems, incident communication protocols, and assessment frameworks such as **GovAssure**: `https://www.ncsc.gov.uk/`

Australia's **Australian Cyber Security Centre (ACSC)**, part of the Australian Signals Directorate, provides a comprehensive **Information Security Manual (ISM)**, incident guidelines, asset protection advice, and threat intelligence services for both IT and OT environments: `https://www.cyber.gov.au/report-and-recover`

The **Operational Technology Information Sharing and Analysis Center (OT-ISAC)** provides threat intelligence, best practices, and alerts for ICS and OT operators globally. It encourages information sharing between sectors and regions to mitigate cyber risks: `https://www.otisac.org/`

Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) publishes ICS security guidelines, critical infrastructure protection measures, and sector-specific incident management frameworks: `https://www.cyber.go.jp/eng/index.html`

The **ICS-CERT division of US CISA** provides guidance, alerts, and best practices for industrial control systems. Resources include alerts on vulnerabilities, ICS security assessments, and incident response templates: `https://www.cisa.gov/topics/industrial-control-systems`.

Industry white papers

Industrial incident management is shaped by what has already gone wrong somewhere else. **Industry white papers** reflect real incidents, regulatory expectations, and operational lessons learned across critical infrastructure. They provide practical guidance that helps teams avoid guesswork during high-stress situations and align response actions across safety, operations, engineering, and cybersecurity when time and clarity matter most. The resources are listed here:

Government and standards organization white papers

- **NIST SP 800-82 Revision 3: Guide to Operational Technology (OT)** provides comprehensive federal guidance on securing OT/ICS environments, threat profiles, risk management, and

security controls tailored to industrial systems: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf. This is the official NIST cybersecurity special publication (OT/ICS focus): https://csrc.nist.gov/pubs/sp/800/82/r3/ipd.

- **NIST SP 1800-10: Protecting Information and System Integrity in Industrial Control System Environments** presents practical cybersecurity implementation scenarios and use cases for manufacturing ICS environments. Download NIST SP 1800-10 (PDF) here: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-10.pdf.
- The **CISA: Post-Quantum Considerations for Operational Technology** white paper explores emerging threats and quantum-era security considerations: https://www.cisa.gov/topics/industrial-control-systems
- The **CIS Critical Security Controls v8.1 for ICS** is a guide on applying CIS controls to industrial control systems for defense-in-depth and practical cybersecurity operations: https://www.cisecurity.org/insights/white-papers/cis-critical-security-controls-v8-1-industrial-control-systems-ics-guide

Organizational/industry white papers

These are produced by professional cybersecurity organizations, industrial vendors, and think tanks, useful for context, frameworks, and implementation strategies.

- **SANS Institute: State of ICS/OT Security 2025** is an industry survey-based white paper on current ICS/OT security posture trends and strategic insights: https://www.sans.org/white-papers/state-of-ics-ot-security-2025
- **SANS Institute: State of ICS/OT Cybersecurity 2024** presents trend analysis with threat insights and defense recommendations for the prior year: https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity
- The **International Society of Automation (ISA) Executive Cybersecurity White Paper** provides a practical overview of ICS cyber risk and executive considerations for governance and risk reduction: https://www.isa.org/getmedia/4b3f6d2e-8d9e-45ed-a563-6ddfc42d0ae3/ISA_WP_Executives-Cybersecurity.pdf
- **Fortinet: A Solution Guide to Operational Technology Cybersecurity** provides operational guidance on OT/ICS cybersecurity architecture and risk mitigation controls. Fortinet OT Cybersecurity Guide (PDF): https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-solution-guide-to-ot-cybersecurity.pdf

- **Tenable: Secure Industrial Control Systems with Configuration Control** is a technical white paper examining threat vectors and configuration control approaches for ICS environments: `https://www.tenable.com/whitepapers/secure-industrial-control-systems-with-configuration-control`
- **Claroty CSP White Papers (Multiple)** provide numerous OT/ICS white papers covering remote access, vulnerability exposure management, and regulatory alignment: `https://claroty.com/resources/white-papers`

Standards and framework-aligned resources

- **BSI/ISO/IEC Reference White Papers** guide you on functional safety and cybersecurity integration. These often align with ISO/IEC and IEC 62443 standards: `https://www.bsigroup.com/siteassets/pdf/en/insights-and-media/insights/white-papers/uk-ks-stan-thght-ict-nst-nsp-sth-01functionalsafetywhitepaper-0025.pdf`
- The **ISA Global Cybersecurity Alliance (ISAGCA)** white papers are related to ISA/IEC 62443 (risk assessments, zero trust, certification, lifecycle security, etc.): `https://isagca.org/resources`

Used correctly, these resources help teams respond with intent rather than improvisation. They support clearer decision-making, more consistent coordination, and defensible actions during incidents that carry real operational and safety impact. In practice, they become reference points that strengthen plans, exercises, and execution, especially when conditions are dynamic and consequences are high.

Summary

This chapter underscored the reality that strong incident management for industrial control systems depends on two dimensions of preparedness: building robust internal resources and leveraging external guidance.

You explored checklists and SOPs that make responses repeatable, playbooks and reference diagrams that give teams structure under stress, and internal readiness tools that form the operational backbone. Meanwhile, federal, state, and industry resources—such as FEMA's ICS forms, CISA's advisories, and standards such as NIST CSF and ISA/IEC 62443—ensure alignment with regulatory expectations and best practices.

Equally important, you explored exercise injects: the catalysts that transform static plans into live tests of readiness. Injects challenge teams to make decisions, reveal gaps, and validate that checklists, SOPs, and playbooks actually work in practice.

Taking the next step

Now that you have worked through the full spectrum of incident management concepts, from understanding threats to adopting ICS structures, to planning and running exercises, you are equipped to put this knowledge into practice within your organization. The following are some of the practical next steps that you can take:

- Build or refine your resource repository: start with one checklist, one SOP, and one playbook addressing your top three risks
- Run a tabletop exercise using injects from this book to validate those tools
- Engage with external partners (CISA, InfraGard, FEMA, or your sector's ISAC) to align your efforts with broader resilience programs

Get this book's PDF version and more

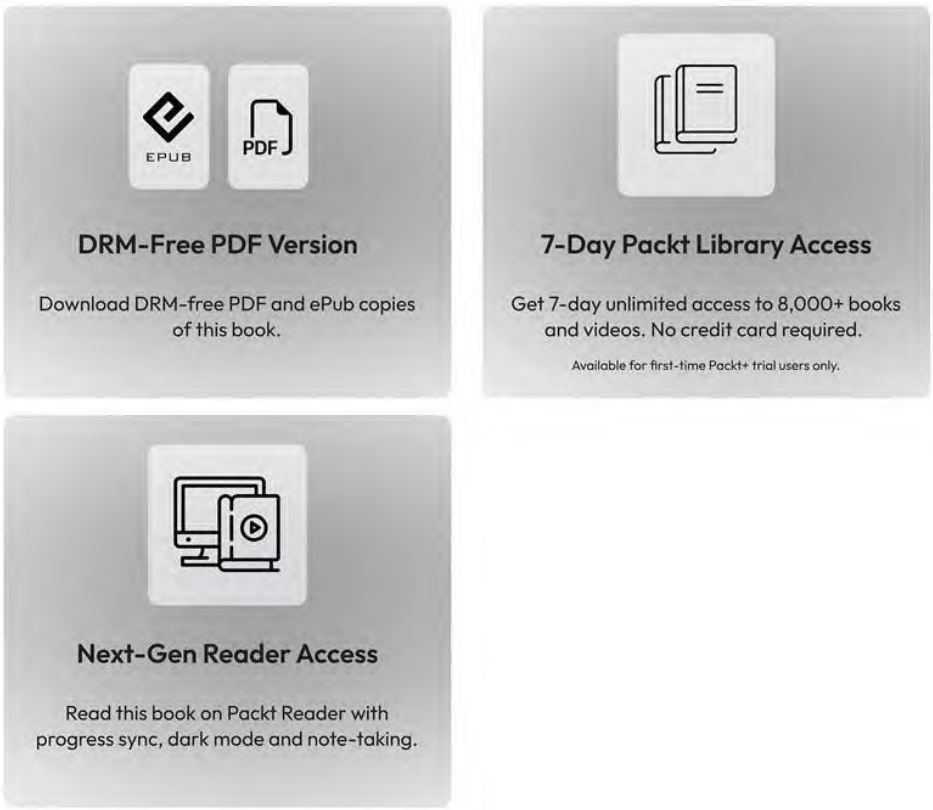
Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

13

Unlock Your Exclusive Benefits

Your copy of this book includes the following exclusive benefits:



Follow the guide below to unlock them. The process takes only a few minutes and needs to be completed once.

Unlock this Book's Free Benefits in 3 Easy Steps

Step 1

Keep your purchase invoice ready for *Step 3*. If you have a physical copy, scan it using your phone and save it as a PDF, JPG, or PNG.

For more help on finding your invoice, visit `https://www.packtpub.com/en-us/unlock?step=1`.

Note: If you bought this book directly from Packt, no invoice is required. After *Step 2*, you can access your exclusive content right away.

Step 2

Scan the QR code or go to `packtpub.com/unlock`.

On the page that opens (similar to *Figure 13.1* on desktop), search for this book by name and select the correct edition.

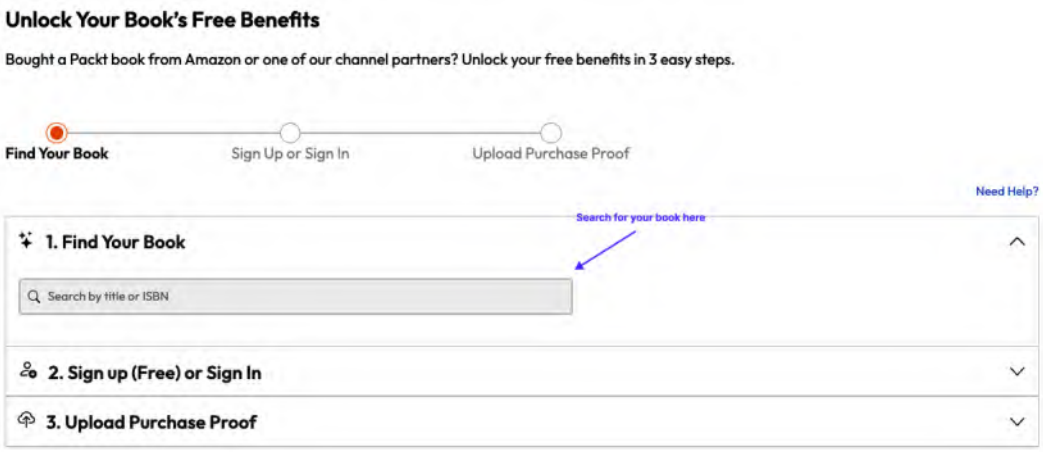


Figure 13.1: Packt unlock landing page on desktop

Step 3

After selecting your book, sign in to your Packt account or create one for free. Then upload your invoice (PDF, PNG, or JPG, up to 10 MB). Follow the on-screen instructions to finish the process.

Need Help

If you get stuck and need help, visit `https://www.packtpub.com/unlock-benefits/help` for a detailed FAQ on how to find your invoices and more. This QR code will take you to the help page.

Note: If you are still facing issues, reach out to `customercare@packt.com`.

Index

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

packt.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

At www.packt.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Other Books You May Enjoy

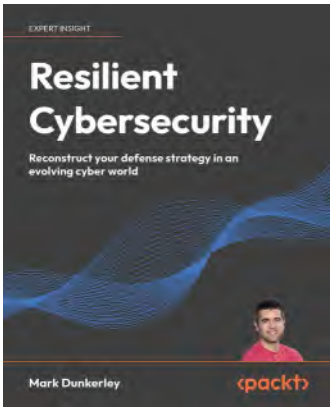
If you enjoyed this book, you may be interested in these other books by Packt:

Securing Industrial Control Systems and Safety Instrumented Systems

Jalal Bouhdada

ISBN: 978-1-80107-881-8

- Explore SIS design, architecture, and key safety network protocols
- Implement effective defense-in-depth strategies for SISs
- Evaluate and mitigate physical security risks in industrial settings
- Conduct threat modeling and risk assessments for industrial environments
- Navigate the complex landscape of industrial cybersecurity regulations
- Understand the impact of emerging technologies such as AI/ML, remote access, the cloud, and IIoT on SISs
- Enhance collaboration and communication among stakeholders to strengthen SIS cybersecurity



Resilient Cybersecurity

Mark Dunkerley

ISBN: 978-1-83546-251-5

- Build and define a cybersecurity program foundation
- Discover the importance of why an architecture program is needed within cybersecurity
- Learn the importance of Zero Trust Architecture
- Learn what modern identity is and how to achieve it
- Review of the importance of why a Governance program is needed
- Build a comprehensive user awareness, training, and testing program for your users
- Review the importance of why a GRC program is needed
- Gain a thorough understanding of everything involved with regulatory and compliance

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `authors.packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Share your thoughts

Now you've finished *Incident Management for Industrial Control Systems*, we'd love to hear your thoughts! If you purchased the book from Amazon, please `click here to go straight to the Amazon review page` for this book and share your feedback or leave a review on the site that you purchased it from.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.