UNIVERSITY OF PIRAEUS - DEPARTMENT OF INFORMATICS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

MSc «Cybersecurity and Data Science»

ΠΜΣ «Κυβερνοασφάλεια και Επιστήμη Δεδομένων»

MSc Thesis

Μεταπτυχιακή Διατριβή

Thesis Title: Τίτλος Διατριβής:	**Cybersecurity in Industrial Control Systems:** A roadmap for fortifying operations Κυβερνοασφάλεια σε βιομηχανικά συστήματα ελέγχου και διαχείρισης: Ο δρόμος προς την οχύρωση κρίσιμων λειτουργιών
Student's name-surname: Ονοματεπώνυμο Φοιτητή:	Stamatina Chairopoulou Σταματίνα Χαιροπούλου
Father's name: Πατρώνυμο:	Vasileios Βασίλειος
Student's ID No: Αριθμός Μητρώου:	MPKED21059 ΜΠΚΕΔ21059
Supervisor: Επιβλέπων:	Panagiotis Kotzanikolaou, Professor Παναγιώτης Κοτζανικολάου, Καθηγητής

Πειραιάς, Ιούνιος 2024

3 Member Examination Committee
Τριμελής Εξεταστική Επιτροπή

Panagiotis Kotzanikolaou **Professor**	**Michael Psarakis** **Associate Professor**	**Dr. Ioannis Stellios**
Παναγιώτης Κοτζανικολάου Καθηγητής	Μιχαήλ Ψαράκης Αναπληρωτής Καθηγητής	Ιωάννης Στέλλιος Διδάσκων ΠΜΣ

Contents

Index Pictures

Περίληψη

Η απρόσκοπτη ενοποίηση της τεχνολογίας πληροφοριών (IT) και της επιχειρησιακής τεχνολογίας (OT) έχει μεταμορφώσει τα βιομηχανικά περιβάλλοντα, εκθέτοντας τα παραδοσιακά απομονωμένα δίκτυα OT στο ευρύτερο οικοσύστημα πληροφορικής. Αυτή η σύγκλιση παρουσιάζει τόσο οφέλη όσο και προκλήσεις, απαιτώντας ισχυρές στρατηγικές κυβερνοασφάλειας προσαρμοσμένες στα μοναδικά χαρακτηριστικά των περιβαλλόντων OT. Η παρούσα διατριβή εμβαθύνει στο εξελισσόμενο τοπίο της κυβερνοασφάλειας των συστημάτων βιομηχανικού ελέγχου (ICS), διερευνώντας τις πολύπλευρες προκλήσεις, τις στρατηγικές και τις μελλοντικές κατευθύνσεις για την προστασία των κρίσιμων υποδομών από απειλές στον κυβερνοχώρο. Εξετάζει σχολαστικά τις περιπλοκές της σύγκλισης IT-OT, τονίζοντας την αντίθετη φύση του IT και του ICS/OT, τα οφέλη και τις προκλήσεις της ενσωμάτωσής τους και το εξελισσόμενο τοπίο κινδύνων που αντιμετωπίζουν τα OT περιβάλλοντα. Επιπλέον, η διατριβή παρουσιάζει την τρέχουσα κατάσταση των προτύπων, κανονισμών και των στρατηγικών συμμόρφωσης στον κυβερνοχώρο για το ICS, εντοπίζοντας βασικά πλαίσια σε περιφερειακούς, εθνικούς και διεθνείς τομείς και τονίζοντας τον κρίσιμο ρόλο της συμμόρφωσης στον μετριασμό των κινδύνων για την ασφάλεια στον κυβερνοχώρο. Η ανάπτυξη στρατηγικής άμυνας στον κυβερνοχώρο αποτελεί τον πυρήνα της διατριβής, διερευνώντας τους διαφορετικούς τύπους προγραμμάτων κυβερνοασφάλειας ICS και τον κεντρικό ρόλο των σχεδίων διαχείρισης κινδύνου στη διαφύλαξη των περιουσιακών στοιχείων του ICS. Παρουσιάζει ένα ολοκληρωμένο πλαίσιο για την αξιολόγηση κινδύνου, το οποίο περιλαμβάνει την καταγραφή των συστημάτων (υλικό, λογισμικό), την αξιολόγηση τρωτότητας, την εκτίμηση επιπτώσεων και τις στρατηγικές μετριασμού του κινδύνου. Η διατριβή εξετάζει επίσης τα σχέδια εφαρμογής της κυβερνοασφάλειας, τονίζοντας τη σημασία της διαχείρισης αλλαγών στην πλοήγηση στη μετάβαση σε ένα πιο ασφαλές περιβάλλον ICS. Οι στρατηγικές ενεργητικής άμυνας στον κυβερνοχώρο διερευνώνται σε βάθος, υπογραμμίζοντας τη σημασία της ευφυΐας και της κατανάλωσης απειλών, της ορατότητας μέσω της αναγνώρισης περιουσιακών στοιχείων, της ανίχνευσης απειλών, της απόκρισης συμβάντων και της χειραγώγησης απειλών και περιβάλλοντος. Επιπλέον, παρουσιάζετε η συμβολή των τελευταίας τεχνολογίας τεχνολογιών κυβερνοασφάλειας ICS, συμπεριλαμβανομένων προηγμένων συστημάτων ανίχνευσης απειλών, λύσεων κυβερνοασφάλειας που βασίζονται σε σύννεφο, αρχές ασφάλειας μηδενικής εμπιστοσύνης και την εφαρμογή τεχνητής νοημοσύνης, τεχνολογιών blockchain και ψηφιακών δίδυμων. Για να καταδείξει πώς δημιουργώντας στρατηγικές κυβερνοασφάλειας για την προστασία της υποδομής ζωτικής σημασίας, η διατριβή παρουσιάζει σε βάθος αναλύσεις μερικών από τις πιο διαβόητες επιθέσεις ICS. Οι μελέτες που αναλύθηκαν κατά την έρευνα αποκαλύπτουν ότι οι οργανισμοί θα μπορούσαν να έχουν ενισχύσει την προστασία τους εφαρμόζοντας αποτελεσματικά μέτρα ασφαλείας σε διάφορα επίπεδα της αμυντικής αρχιτεκτονικής ICS. Η διατριβή ολοκληρώνεται συνοψίζοντας βασικά ευρήματα, δίνοντας έμφαση στην επιτακτική ανάγκη υιοθέτησης μιας ολιστικής προσέγγισης κυβερνοασφάλειας σε περιβάλλοντα ICS και σκιαγραφώντας μελλοντικές κατευθύνσεις έρευνας για την αντιμετώπιση των αναδυόμενων προκλήσεων κυβερνοασφάλειας στο ταχέως εξελισσόμενο τοπίο των OT.

Abstract

The seamless integration of information technology (IT) and operational technology (OT) has transformed industrial environments, exposing traditionally isolated OT networks to the broader IT ecosystem. This convergence presents both benefits and challenges, necessitating robust cybersecurity strategies tailored to the unique characteristics of OT environments. This dissertation delves into the evolving cybersecurity landscape of industrial control systems (ICS), exploring the multifaceted challenges, strategies, and future directions for safeguarding critical infrastructure from cyber threats. It meticulously examines the intricacies of IT-OT convergence, highlighting the contrasting nature of IT and ICS/OT, the benefits and challenges of their integration, and the evolving risk landscape confronting OT environments. Furthermore, the dissertation delves into the state of cybersecurity standards, regulations, and compliance strategies for ICS, identifying key frameworks across regional, national, and international domains, and emphasizing the critical role of compliance in mitigating cybersecurity risks. Strategic cyber defense development forms the core of the dissertation, exploring the diverse ICS cybersecurity program types and the pivotal role of risk management plans in safeguarding ICS assets. It presents a comprehensive framework for risk assessment, encompassing asset identification, vulnerability assessment, impact assessment, and risk mitigation strategies. The dissertation also scrutinizes cybersecurity implementation plans, emphasizing the importance of change management in navigating the transition to a more secure ICS environment. Active cyber defense strategies are explored in depth, highlighting the significance of threat intelligence and consumption, visibility through asset identification, threat detection, incident response, and threat and environment manipulation. Additionally, the dissertation examines the benefits and challenges of applying cutting-edge technologies in ICS cybersecurity field, including Cloud Computing, AI/ML, Blockchain, Digital Twins and Deception Technology. To illustrate how by building cybersecurity strategies for protecting critical infrastructure, the dissertation presents in-depth analyses of a few of the most notorious ICS attacks. The case studies analyzed in this research reveal that organizations could have enhanced their protection by implementing effective security measures across different tiers of the ICS defense architecture**.** The dissertation concludes by summarizing key findings, emphasizing the imperative of adopting a holistic cybersecurity approach in ICS environments, and outlining future research directions to address emerging cybersecurity challenges in the rapidly evolving OT landscape.

1. Introduction

1.1 Industrial Revolution: Driving the Future of Industry 4.0 & Industry 5.0

In the ever-evolving industrial landscape, the distinction between information and data is becoming increasingly crucial. Every day, a multitude of technologies operate behind the scenes to facilitate modern existence. Two of the most important examples include Information Technology (IT) and Operational Technology (OT). In today's interconnected world, industrial processes have become highly dependent on complex computerized systems known as Industrial Control Systems (ICS). ICS play a critical role in the operation of many of the systems that keep our society running smoothly. Industrial control systems (ICS) and operational technology (OT) are the backbone of modern industrial infrastructure.

As the world undergoes the 4th industrial revolution, known as Industry 4.0, the boundaries between IT and OT are rapidly blurring. The division between them has traditionally hindered manufacturing processes. Addressing this divide is essential for achieving a holistic overview of shop floor operations and driving Industry to the 5th version. Industry 4.0 and Industry 5.0 underscore the need for IT and OT integration. The 4th Industrial Revolution (2010-2020) involved the convergence of digital, biological, and cyber-physical systems. This era has transformed sectors such as manufacturing, transportation, healthcare, and agriculture and has seen the emergence of breakthrough technologies, including the IoT (Internet of Things),artificial intelligence/machine learning (AI/ML), big data analytics, hybrid cloud computing, renewable energy, 3D printing, robotics, and biotechnology.

Today, at the dawn of the Industry 5.0 (2020-beyond) when inter-machine connectivity of Industry 4.0 will be extended to incorporate human-machine interaction as part of the process. The uniqueness of human creativity and critical thinking will not be able to be designed to machines, in the context of industry 5.0. Consequently, ongoing innovation is designed to continually improve processes by relieving operators of repetitive or predictable tasks by automation and, at the same time also integrate these operators into production processes. The 5th Industrial Revolution involves cyber-physical human intelligence, cognitive systems, and mass customization. The European Union defines Industry 5.0 as a vision for the future of industry, transcending efficiency, and productivity as sole objectives. It aims to strengthen the industry's societal contributions and its positive impact on society. Industry 5.0 uses new technologies to provide prosperity beyond jobs and growth while respecting the production limits of the planet. What sets Industry 5.0 apart is its emphasis on the purpose of industrialization and its focus on sustainability and resilience. It is important to emphasize that the introduction of Industry 5.0 does not mean that Industry 4.0 will be completely replaced. Industry 5.0 will extend the strengths of Industry 4.0 and help make companies even more agile and future-proof. With the Industry 5.0 unfolding and formerly futuristic technologies like edge computing and autonomous systems approaching mainstream, the associated security risks escalate sharply.

1.2 The Importance of Critical Infrastructures

The safe and smooth operation of critical infrastructures is the cornerstone of a functioning society. From energy grids that power our homes and businesses to transportation networks that facilitate the movement of goods and people, these infrastructures underpin the basic systems we rely upon daily. Any disruption to these vital services can have cascading effects, leading to economic losses, public safety hazards, and even threats to national security. Maintaining the integrity and resilience of critical infrastructures is essential to ensure societal stability, economic prosperity, and the well-being of our communities.

The complex chain of interconnected computer systems, both legacy and new, underpins many critical processes in the physical realm. However, this dependence makes these inherently vulnerable systems, prime targets for malicious actors, potentially leading to severe safety and the environmental impacts. More complex critical infrastructure examples include the generation, transmission, and distribution of electric power in a power grid system, critical manufacturing, oil and gas refineries and pipelines, water, and wastewater management systems among many others. The Cybersecurity & Infrastructure Security Agency (CISA) [1] lists 16 sectors deemed as critical infrastructure, as shown in Figure 1.

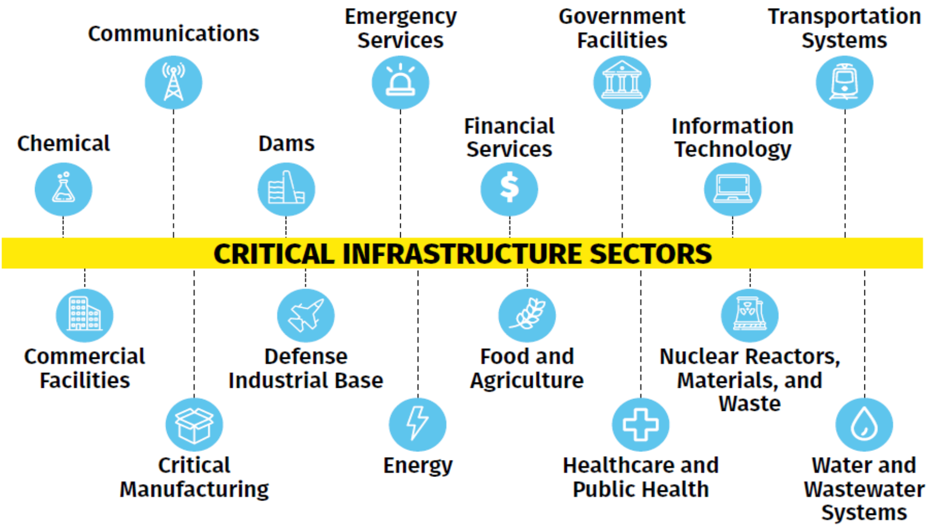


Figure 1 Critical Infrastructure Sectors

1.3 The Evolving Risk Landscape

The growing digitization and connectivity of ICS systems expose them to a new realm of threats, making Industrial Control System security a paramount concern. A security breach in an ICS could have serious consequences, including the disruption of critical infrastructure, environmental damage, lost revenue, and even loss of life.

With the spread of IT functions into OT environments, and the subsequently enhanced interconnectivity, some of the cybersecurity risks associated with IT systems have crept into OT networks as they become more accessible. In many industrial companies, there is now systemic interdependent cyber risk between the OT and IT sides of the house. While IT/OT convergence supports IT capabilities, it provides significantly less isolation to the OT environment and critical production from the outside world than legacy environments, exposing these systems to greater cyber risk.

There is an exponential growth of the ICS risk every year. The percentage of respondents who considered threats to the ICS as “high” in 2019 was 38% and rose to 40% in 2021, 41% in 2022, and 44% in 2023. This is driven by the rise of ransomware campaigns aimed at critical infrastructure and by scalable attack frameworks specifically intended for ICS. We are also observing more ICS adversaries using “living-off-the-land” attacks, as they are able to have an impact with less malware, thus becoming less detectable due to existing engineering systems being set against themselves.

The increasing integration of IT and OT systems in recent years has led to the belief that IT security tools can be effectively applied to ICS environments. This is supported by the observation that attackers often employ similar tactics and leave similar digital footprints in both IT and ICS systems, as moving laterally between Windows machines within the ICS or exfiltrating data via DNS.

Yet, a crucial difference exists between IT and ICS environments. Standard IT security solutions often remain incompatible with ICS systems due to fundamental communication gap between IT tools and the specialized protocols used in OT environments. This incompatibility is evident in the ineffectiveness of the endpoint protection devices to safeguard programmable logic controllers (PLCs).

Significantly, numerous IT security tools rely on heuristics and machine learning models trained exclusively on "normal" IT customer environment data. This lack of specialized training and tuning for ICS environments renders them significantly less effective in detecting ICS-specific anomalies and attacks. Effective management and mitigation of cyber risks in the intricate ICS environment necessitates addressing the following critical challenges:

- ❖ **Myth: "Air-gapped ICS systems"**

  The belief that ICS systems are always air-gapped is a dangerous misconception. While air gaps may have been effective in the past, they are no longer feasible in today's interconnected digital landscape. Even if an organization isolates its ICS from its IT network, vulnerabilities remain through connections established for legitimate maintenance and support by vendors and integrators. These connections can unintentionally serve as entry points for cyber threats, even when the systems are isolated from an organization's enterprise network.

- ❖ **Malware and Zero-Day Vulnerabilities**

  Malicious software designed to infiltrate ICS networks, such as Triton, Industroyer, NotPetya and Stuxnet, has shown the devastating impact it can have on critical infrastructure (more details in chapter Vb). Attackers actively search for unknown vulnerabilities in ICS software and hardware to exploit them before they are patched. One best practice that an industrial organization should follow is leveraging an ICS threat intelligence tool to ensure detections for zero-day exploits before they get public.

- ❖ **Network Misconfigurations**

  In modern ICS environments, various subsystems and components are connected to optimize operations. This means that an issue in one part of the system can cascade to other areas. A network misconfiguration or process anomaly in one part of the network can quickly spread and impact critical processes. Network misconfigurations, such as improper firewall rules or insecure device settings, can inadvertently expose critical components of the ICS to unauthorized access or manipulation. Similarly, process anomalies, including unexpected deviations from normal system behavior, can disrupt industrial processes and cause downtime.

- ❖ **Human Factor: Phishing, Social Engineering & Disgruntled Employees**

  Cybercriminals can use tactics ranging from a basic phishing email to complex social engineering schemes to trick employees into revealing login credentials and gain unauthorized access to ICS systems. Moreover, disgruntled employees or contractors with access to ICS systems can pose a significant security risk. Continuously cleaning up old user accounts, applying the principle of least privilege and spot checking each system after third-party vendor access could reduce this risk.

1.4 Consequences of modern ICS cyberattacks

Modern ICS cyberattacks have the potential to cause widespread and devastating consequences, impacting not only the physical operations of critical infrastructure but also the broader economy, society, and even national security.

One of the most concerning consequences of ICS cyberattacks is the potential for physical damage to critical infrastructure, such as power grids, oil and gas pipelines, and transportation networks. Sabotaging the control systems of these systems could lead to large-scale blackouts, explosions, or derailments, with potentially catastrophic consequences.

In addition to physical damage, ICS cyberattacks can also have significant economic and societal impacts. The disruption of critical infrastructure can halt production, disrupt supply chains, and cripple critical services, leading to billions of dollars in economic losses and widespread disruption. The consequences of ICS cyberattacks extend beyond national borders, as they can disrupt global trade, energy markets, and financial systems. In today's interconnected world, a cyberattack on a critical infrastructure system in one country could have ripple effects across the globe, posing a serious threat to international security and stability.

In the light of these immense risks, it is crucial to prioritize cybersecurity for ICS systems. Organizations responsible for managing critical infrastructure must implement robust cybersecurity measures, including vulnerability assessments, incident response plans, continuous monitoring, and patching of systems, to protect their ICS systems and mitigate the risk of attacks. Finally, yet importantly, governments and international organizations should collaborate to develop and share best practices for ICS cybersecurity, strengthen international cooperation in incident response, and promote research and development of innovative security solutions tailored to the unique challenges of ICS environments.

Risks and challenges in Operational Technology systems are multifaceted, stemming from both external and internal sources. Identifying and managing these risks is crucial to ensuring the security and resilience of OT systems. The impact of risks in OT systems extends beyond compromising confidentiality and integrity, potentially affecting the safety and reliability of operational processes. Developing a robust security posture, encompassing the implementation of tailored security controls, continuous monitoring, incident response, and security awareness, is pivotal to mitigating risks and enhancing the resilience of OT systems. Security awareness and training play a crucial role in addressing the human factor in security, fostering an environment of knowledge and vigilance against the myriad of threats and vulnerabilities inherent to OT systems.

A holistic understanding and approach to the risks and challenges in OT is essential for developing and implementing effective security measures. The subsequent chapters will provide further insights and guidelines on the specific security considerations and best practices to fortify Operational Technology systems against the evolving landscape of threats and vulnerabilities.

1.5 Thesis Contribution and Structure

In today's increasingly interconnected world, ensuring the secure and reliable operation of critical infrastructure, such as power grids, transportation systems, and water treatment facilities, is paramount. These systems, heavily reliant on industrial control systems (ICS), face constant threats from cyberattacks, potentially causing widespread disruption and devastating consequences. Building an efficient and robust cybersecurity plan for ICS is no longer just an option but a crucial necessity. This thesis proposes a structured and agile methodology for building cyber resilience and enhancing the overall security posture of industrial companies. The recommended methodology can act as a comprehensive shield, safeguarding critical operations from unauthorized access, data breaches, and disruptions, ultimately protecting public safety and economic stability.

This thesis contributes significantly to the field of critical infrastructure cybersecurity by presenting a comprehensive roadmap for defense against the ever-changing threat landscape. Unlike existing approaches, this roadmap, structured upon established regulatory frameworks and risk-based management principles, by providing actionable steps for implementing layered network defenses. It further empowers critical infrastructure operators by offering flexibility in choosing passive or active safeguards, aligning with their specific needs. This comprehensive and adaptable approach equips operators to address current and future cybersecurity challenges, ensuring the continuity and integrity of essential services. This thesis also advocates for a novel approach to ICS defense. It proposes leveraging cutting-edge technologies like machine learning for anomaly detection, blockchain for secure data management, and deception technology for misdirection, as complementary practices following risk management and cybersecurity development phases. By strategically integrating these tools, the research aims to:

- **Enhance threat detection and response:** Cutting-edge tools can identify subtle anomalies or suspicious behavior that might evade traditional methods.

- **Strengthen security posture:** Blockchain can offer tamper-proof data storage and communication, while deception technology can divert attackers from critical systems.
- **Provide a layered defense:** These technologies complement existing practices, creating a more robust defense against evolving cyber threats in ICS environments.

A breakdown structure of the thesis is presented below, by outlining each chapter.

- ❖ **Chapter 1 – Introduction :** This chapter explores the evolution of the Industrial Revolution, delving into Industry 4.0 and the emerging Industry 5.0, ultimately emphasizing their profound impact on critical infrastructure and the imperative of ensuring safe and seamless operations to safeguard our society. It also outlines the evolving cybersecurity risk landscape and the devastating consequences of the emerging sophisticated cyberattacks against critical infrastructures.
- ❖ **Chapter 2 – Industrial Architecture :** This chapter delves into the evolving industrial network architecture and its paradigm shift towards IT/OT convergence. It analyzes the potential benefits and challenges associated with this convergence, highlighting its significant impact on modern industrial systems.
- ❖ **Chapter 3 – ICS Cybersecurity Standards and Compliance :** This chapter navigates the landscape of regional and international standards and regulations governing/applying cybersecurity controls for ICS, subsequently outlining a step-by-step approach to building a robust compliance strategy.
- ❖ **Chapter 4 – Unveiling the Hidden Pathways of ICS cyberattacks :** This chapter dissects the ICS cyber kill chain, analyzes "living-off-the-land" attacks, explores real-world examples through case studies of ICS cyberattacks, and extracts valuable lessons learned.
- ❖ **Chapter 5 – Cyber Defense Development :** This chapter delves into the critical components of building a robust cyber defense for industrial control systems. It outlines the different types of ICS cybersecurity programs, unpacks the essential elements of constructing a Risk Management Plan, and defines the phases of 'Sliding Scale of Cyber Security' model. Additionally, it emphasizes the importance of developing a Change Management policy and building the Active Defense key processes for achieving comprehensive protection.
- ❖ **Chapter 6 – Beyond Traditional Security: Leveraging Cutting-Edge Technologies :** This chapter investigates the potential of cutting-edge technologies, such as cloud computing, Industrial Internet of Things (IIoT), Artificial Intelligence/Machine Learning (AI/ML), blockchain, digital twins, and deception techniques through honeypots, for enhancing the security of Industrial Control Systems (ICS).
- ❖ **Chapter 7 – Conclusions & Future Work :** This chapter charts the path towards a more secure critical domain by advocating for the adoption of essential security controls while emphasizing the crucial need for balanced prioritization within ICS/OT security.

2. Industrial Architecture

2.1 Scope of Industrial Control Systems (ICS)

ICS are complex systems with interconnected hardware and software parts that have been developed for the purpose of monitoring, managing, operating, or automating industrial processes. ICS are usually a variety of parts including sensors, programmable logic controllers (PLCs), human-machine interfaces (HMIs), and communications networks. These components cooperate in the handling of the control of different process flows, for example, the treatment of water systems as well as the movement of railway trains in a transport system, processing of goods packaging, the movement of belt conveyors, the measurement of power generation and consumption in a power grid, building automation system, and so on.

In spite of the fact that the ICS-OT terms are sometimes used synonymously, ICS is actually a significant part of the OT domain and consists of systems used to monitor and control industrial processes. Generally, these systems use the industry-specific protocols and hardware created for industrial conditions. However, OT is a large umbrella term that covers all hardware and software used to manage and control processes in the industry including ICS. ICS consists of SCADA systems, DCS, and other technologies to the extent their operation is concerned. Given that these devices are supposed to be reliable, secure, and resilient, they mostly demand specialized professionalism for their implementation and maintenance. In fact, all types of ICS are forms of OT, but all types of OT are not ICS. Some examples of types of ICS systems include:

- **Supervisory Control and Data Acquisition (SCADA):** are the most common type of industrial control systems that consist of software and hardware components. They allow industrial organizations to control processes locally or at remote locations, monitor, gather, and process real-time data, interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software, and record events into log files. SCADA systems have several advantages of cost reduction, ease of use, and performance efficiencies, but the cyberattack and data breaches have increased greatly in the recent times due to the remote access and internet connectivity. In worst cases, hacks to these systems can let an adversary gain such a capacity as controlling the water supply system of a city, shutting down electricity or causing dangerous mistakes in nuclear reactors. The last illustrations show why securing ICS has become highly needed.
- **Distributed Control Systems (DCS)**: are employed in complex industrial processes to control and manage various components of a system. They are commonly used in sectors such as manufacturing, oil and gas, and power generation.
- **Programmable Logic Controllers (PLC)**: are ruggedized computers used to control machinery and automate processes. PLCs are programmed devices that efficiently manage those critical processes with precise timing. They are commonly found in manufacturing and industrial environments.

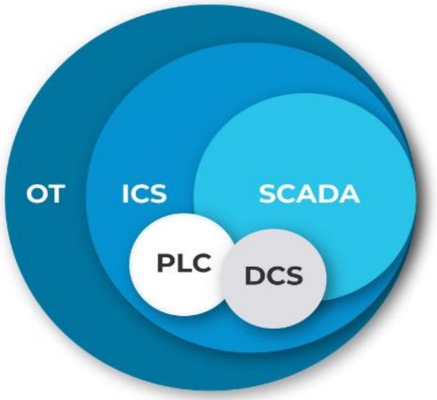


Figure 2 Layers of ICS environment, [2]

Building management systems (BMS) are another type of industrial control system (ICS). They are used to monitor and regulate various aspects of building systems, such as HVAC *(*Heating, ventilation, and air conditioning)*,* lighting, and security systems. BMS can improve operational efficiency, comfort, and safety, and reduce operating costs and environmental impact. However, they are also vulnerable to cyberattacks, which can cause a wide range of problems, such as shutdowns, data theft, and patient safety risks.

Safety Instrumented Systems (SIS) are often implemented as PLCs, provide critical processes with robust safety measures. They act independently of normal process control, triggering lifesaving interventions like stopping machinery or shutting down gas flow when dangerous conditions arise. This overriding functionality ensures safety even if normal operations become hazardous. Traditionally separated systems, SIS, prioritize safety by monitoring parameters and initiating alarms or shutdowns to prevent harm. While theoretically isolated from the ICS network, SIS often exhibit greater connectivity for operational convenience, exposing them to network threats. SIS also have default "backdoor accounts", that are crucial for administrative control. However, if discovered by a perpetrator could be exploited to gain access without the need for any authorization. While critical for emergency access, these accounts pose a significant security risk. Newer models address this concern with stronger authentication methods, but older models, like the one exploited, require stricter network isolation and monitoring to mitigate abuse. Blocking activity without understanding the impact can be detrimental, as maintaining operational functionality is crucial. Therefore, a balanced approach is necessary, prioritizing both security and operational needs through robust network isolation and careful monitoring of SIS connections.

2.2 IT/OT Convergence

2.2.1 Difference and Convergence between IT and ICS/OT

Initially, IT and OT systems were designed to work apart, separate from each other by different teams with different objectives, and with no connectivity between them. These principles, however, have changed significantly over the past ten years, mainly evoking for the rise of technology and digital transformation. Nowadays, organizations from all industries have found it necessary to apply a variety of newer cyber-physical systems and technologies that have to interconnect IT and OT. Such merging of previously independent environments have resulted in an unequivocal creation of business opportunities, which encompasses benefits including higher efficiency and sustainability to innovation. However, in the process of convergence this poses new risks, issues, especially IT and OT cybersecurity.

IT and OT networks many times need to interact with one another to exchange data and information. However, ensuring that communication between segmented OT networks and other parts of an organization's IT infrastructure can be challenging. The OT (Operational Technology) sector generally lags behind IT, in terms of security practices, including integration with IT systems (IT/OT convergence). According to ICS CERT advisories, common vulnerabilities like buffer overflows, weak session management, hardcoded credentials, and inadequate access control persist in many ICS applications and devices.

One of the practical examples of IT/OT convergence is IIoT devices, which is made possible by networks of sensors, instruments, and machines connecting to the IT networks, mostly using cloud. Also, there is the example of IoT devices in general which brings together things such as smart meters, wearable devices, and even smart dustbins and home appliances.

Unlike the IoT which is oriented on consumers' demand, the IIoT imposes attention on a more advanced level in the sense that it involves increasing efficiency in production, communication between machines (M2M), and automatic industrial processes operations. The IIoT tools enable manufacturing industries to achieve higher levels of productivity, performance, and predictive maintenance through analytics, artificial intelligence, and real-time data collection. As businesses increasingly realize its potential the IIoT is set to revolutionize how industries function.

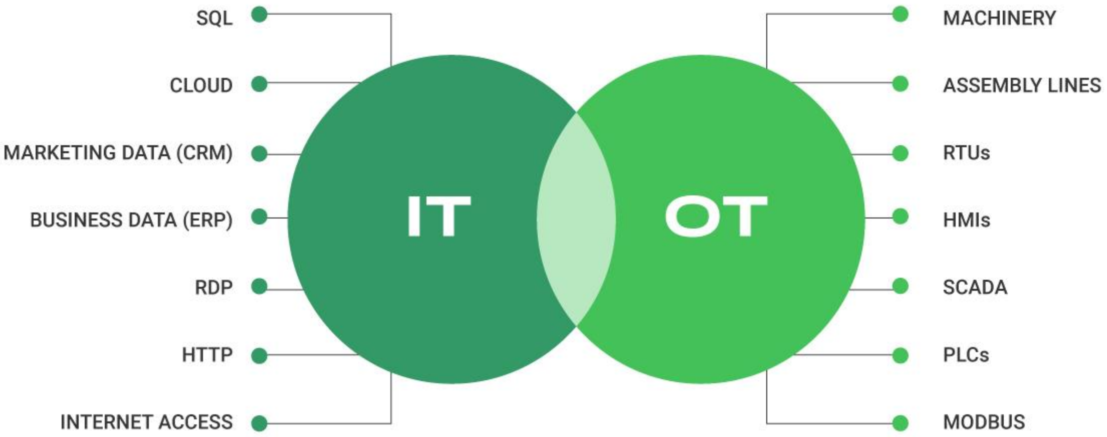


Figure 3 Convergence of IT and OT components

2.2.2 The New Age of Operational Technology

Traditionally, the role of IT teams for an organization has been to oversee the application of the technology involved in the day-to-day business operations, the related equipment as well as the processes involved in the storage, transfer, and security of the ensuing data. As opposed to this, OT operators stabilize industrial control systems (ICS) – the systems, devices, and processes that give an effect on physical environments. Unlike many security groups which are involved in fighting a wide spectrum of diverse cyber threats, including users with repeat offenses, etc., the OT community is facing significant challenges pertaining to the growing threats against critical infrastructures that require being perceived, comprehended, and addressed before collateral effects.

The IT/OT convergence era has given organizations a possibility to significantly speed up their digital transformation programs. With the convergence of the IT and OT systems, organizations can automate their processes even more to minimize human error, enhance productivity, and simplify their operations. They will also have a better understanding of their operations and will be able to make data informed decisions with improved data availability. But the emergence of converged IT/OT has also created an interconnectedness increasing the problems that companies face.

With an increased interconnection of IT devices and systems with OT environments, and the expanding extended internet of things (XIoT), more organizations will see such implications. The term XIoT describes all the connected assets that form the backbone of the CPS (cyber-physical systems) in industrial, healthcare, and commercial environments. It is the by-product of the digital revolution and therefore is growing the interconnection of the internet and systems which govern the physical processes.

While being introduced more than 15 years ago, the concept of cyber-physical systems (CPS) is now approaching the mainstream mostly because digital transformation is gaining momentum and OT environments are getting integrated with IT systems, and other IoT devices. Cyber-physical systems cover OT assets and systems, as well as numerous connected devices. Gartner defines cyber-physical systems as engineered systems that integrate sensing, computing, controlling, networking, and analyzing to interact with the physical world, producing better operations, resilient, reliable systems, and a deeper understanding of the physical things they control. This cyber-physical fabric covers everything from OT assets like PLCs, to BMS devices like HVAC controllers and elevators, to IoT devices like security cameras and vending machines, to healthcare and IoMT (Internet of Medical Things) devices like infusion pumps and MRI machines. Other examples of CPS are robots, smart buildings, and autonomous vehicles. Now we are at a stage where our world is very digital dependent.

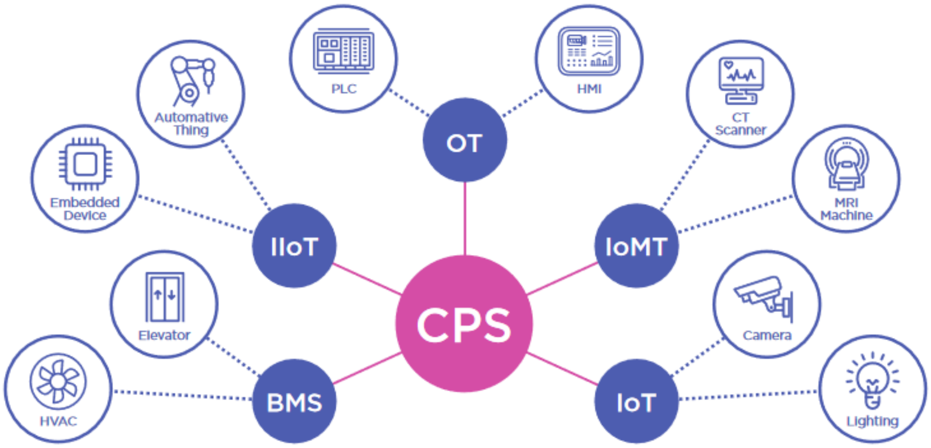


Figure 4 Evolution from OT to CPS: Outcome of IT and OT Convergence, (source: [3])

2.2.3 Architecture of Integrating OT and modern IT

The Purdue Model stemmed from the 1990s Purdue Enterprise Reference Architecture (PERA) framework, represents a widely recognized conceptual model for segmenting ICS networks. The architectural framework was developed by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing and was meant to be resilient, while encoding it into standards, such as ANSI/ISA-95 and IEC 62264. It delivers foundational language for control systems security regulatory controls, such as IEC 62443 and NIST SP800-82 benchmarks.

The Purdue Model segments devices and equipment into hierarchical functions that show the interconnections and interdependencies of the main components of a typical ICS. The Purdue Model delineates security boundaries between users, ICS networks, and business networks, and shows how these boundaries have blurred in recent years as IT/OT Convergence gained importance.

Current Purdue architecture breaks down OT and IT into six functional levels that run from Level 0 to Level 5 across three zones, as shown in Figure 5.

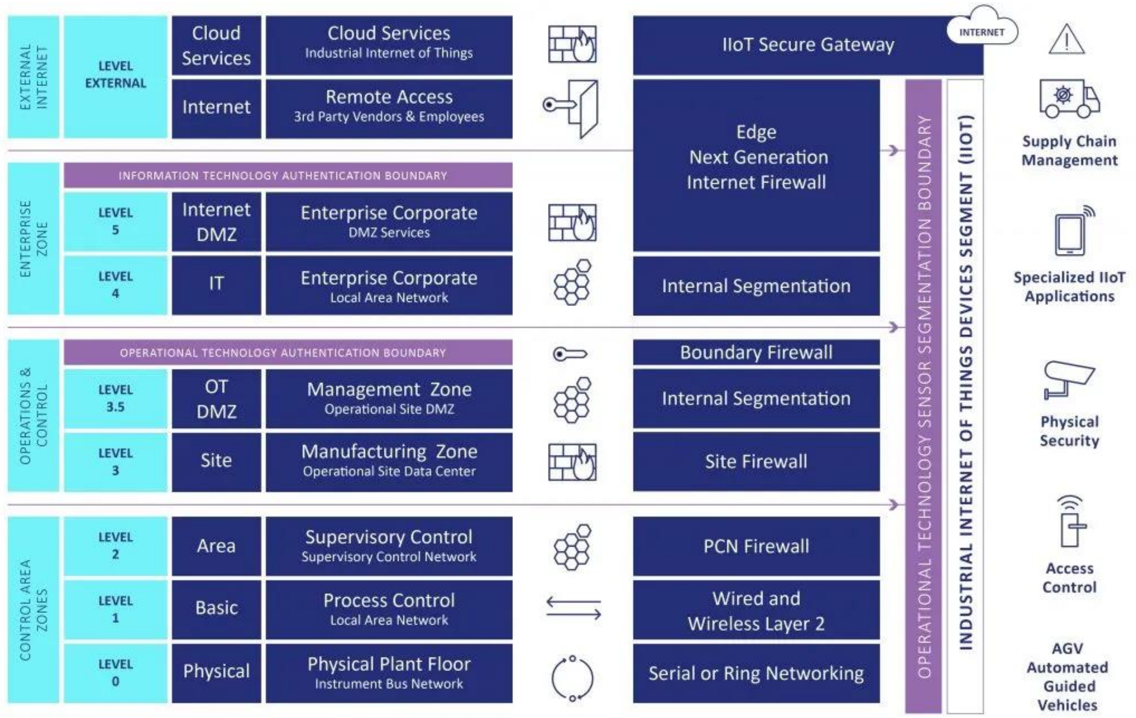


Figure 5 Purdue Model including IIoT and Cloud – Operational Technology Cyber Security Alliance (source:[4])

2.2.4 Benefits and Challenges of the IT-OT Convergence

Facing an incrementing cyber threat landscape, companies reliant on industrial processes for their core business are at a critical juncture. While digitalization and hyperconnectivity are essential for growth, they create new vulnerabilities and magnify existing ones. To mitigate these risks while harnessing innovation, organizations must seek partners who enable synchronized advancement of both cybersecurity and OT.

Implementing necessary changes within organizations while managing ICS and OT security poses unique challenges for defenders. Securing OT systems, achieving stakeholder alignment, and fostering IT-OT collaboration are central hurdles.

IT-OT convergence refers to the merging of distributed computing power, data processing, and OT systems responsible for industrial operations. This integration, driven by business demands for process automation and business intelligence, necessitates balancing these advancements with robust OT security.

Regardless of their preferred terminology IT/OT "Convergence" or "Collaboration", industrial organizations must now confront the undeniable security challenges arising from the interconnectedness of IT and OT networks. This critical nexus point demands immediate recognition and proactive management to mitigate inherent risks across both domains. The air gap, if it ever truly existed, is long gone…

While IT/OT convergence enhances supply chain integration and visibility, it simultaneously expands the attack surface and facilitates the exploitation of vulnerabilities by cybercriminals. This risk is exacerbated by the inadequate cyber protection of OT infrastructure in many organizations. Traditional IT security tools are often incompatible with OT environments due to the potential disruption of critical processes, leading to production losses or safety hazards. Consequently, inherent vulnerabilities within industrial control systems present significant cyberattack opportunities.

Benefits

Bringing systems together presents one of the major advantages of the IT and OT systems convergence since the organization gets the capability of streamlining its processes hence the organization operates in a more efficient way. When an organization's IT and OT systems are linked, it is simpler to apply IT analytics to OT systems.

This is especially the case for example of a manufacturing facility, where IT can track how long each step of the manufacturing process takes, and hence to identify production bottlenecks. These inefficiencies can be eliminated by purchasing faster equipment or adding additional staff.

At the same time, the opposite is also true. The IT analytics system can recognize that a machine in the factory floor is operating at a very low production rate. In such a case, the IT system can help in scaling up the production to utilize the maximum potential of the machine or cut down the operational cost by trading in the machine with another.

The convergence of IT and OT systems could also offer benefits in the context of operational efficiency. This convergence might enable organizations to extend established IT best practices, like patch management, to their OT environment. This could ensure all OT devices, including IIoT hardware, operate with the latest firmware, potentially enhancing overall system security and stability.

Nonetheless, the legacy OT equipment usually comes with patching and update difficulties that make it more susceptible to security breaches. In that regard, organizations must perform thorough OT system inventories and introduce network segmentation that separates legacy systems thus minimizing the spread of the attacks. By facilitating live tracking of OT devices, following the IT practices, enhances security, and support proactive vulnerability management. Importantly, centralized asset tracking advantages are more than just loss prevention simplicity.

IT-OT convergence can further enhance operational service-level agreement (SLA) compliance by leveraging IT systems to monitor industrial machinery usage. These systems can proactively alert staff to upcoming maintenance requirements based on real-time usage data, ensuring timely interventions, and minimizing downtime.

The convergence of IT and OT systems offers organizations significant advantages, as outlined below:

- ✓ Reduced downtime: Integrating the systems can help identify issues proactively before they cause unplanned outages or shutdowns. This improves reliability and continuity.
- ✓ Efficiency gains: Bringing the data together from various systems can help optimize workflows, assets, and energy use across the facility. This drives cost savings.
- ✓ Regulatory compliance: An integrated view of operations and associated data can help ensure adherence to safety, reporting, and other regulations.
- ✓ Better asset utilization: Insights from connected systems allow companies to maximize the use and lifespan of critical equipment through improved maintenance and reduced unplanned downtime.
- ✓ Supply chain management: By linking OT production systems with IT business systems like inventory, logistics, etc. facilitate massive integration across the supply chain. This improves agility and efficiency.

The key is bringing the contextual data about actual operations, processes, and assets together with the analytical capabilities of IT systems. This provides the visibility and insights needed to optimize production, assets, and ultimately profitability. But it does require overcoming technological and organizational barriers between traditional IT and OT teams.

Implications and Challenges

In the modern era, the advent of interconnected systems and digital technologies has led to new security challenges. Our greater reliance on digital infrastructure and the increased connectivity across industries creates vulnerabilities that can be easily exploited by malicious actors. The increased connectivity and criticality of these systems create greater challenges for their adaptability, resilience, safety, and security.

The complexity and large scale of today’s systems make security management and incident response even more difficult. Industry 4.0 and 5.0 rely heavily on global supply chains, suppliers, and partnerships.

The integration of IT with OT opens the floodgates for potential intruders to exploit interconnected systems, and potentially disrupt essential services like energy grids and manufacturing plants. As the Industrial Internet of Things (IIoT) becomes integral to industrial operations, each connected device becomes a potential entry point for cyber threats. The intricate web of devices, if not properly secured, can cascade vulnerabilities across the entire IT/OT ecosystem. Compromise to a single component can have far-reaching implications for the entire supply chain.

Many of the challenges in IT/OT Convergence are people/process problems rather than technical ones. Threats are increasingly complex and unpredictable, and malicious actors do not necessarily have to specifically target industrial enterprises to have a devastating impact. Indeed, there are already many examples of ransomware, not designed to target industrial enterprises having a considerable impact on production.

Despite the potential efficiency gains promised by IT/OT convergence, three primary challenges hinder seamless integration: security risks, technological hurdles, and human factors. Each of these areas present significant issues requiring careful consideration and mitigation strategies.

❖ **Security Risks “IT security is not OT/ICS security”**

Security concerns constitute a major hurdle in IT/OT convergence. Unforeseen vulnerabilities arise when previously isolated systems merge, potentially leading to significant repercussions. This necessitates a delicate balancing act between IT's data-centric approach and OT's real-time operational focus, necessitating a comprehensive reevaluation of existing security protocols.

It is essential to dispel the prevailing myth that IT security practices can be seamlessly applied to ICS systems. While leveraging existing IT security knowledge is valuable, blindly applying traditional methods to ICS can incur detrimental consequences. Moreover, differing priorities between IT and OT cybersecurity, with IT focusing on confidentiality and data integrity, and OT emphasizing real-time functionality, safety, and availability, create potential conflicts. To improve its security posture, the industrial field must address several key challenges outlined below.

- **Lack of Secure Remote Access.** The lack of proper access control in many industrial control systems (ICS) makes it easier for cybercriminals to gain unauthorized access to critical systems, posing a significant security risk. Organizations also face the challenge of managing remote access for internal and third-party users who need to access ICS for maintenance or other purposes. Without secure remote access measures in place, organizations have limited visibility and control over operations, which can lead to downtime and safety concerns. Additionally, if remote access is not configured properly, it can bypass network segmentation measures, further compromising security.
- **Lack of Segmentation.** Establishing robust network segmentation in industrial environments can be challenging and resource intensive. It necessitates continuous adjustment and maintenance, leaving room for human error. Insufficient segmentation leaves OT networks vulnerable to lateral movement by attackers who breach one part of the network.

- **Lack of Patching.**The high uptime requirements of many industrial environments often lead to limited maintenance windows, making these systems more susceptible to known attacks. This lack of regular maintenance leaves vulnerabilities unaddressed, increasing the likelihood of breaches and downtime.

Different natures between IT and ICS/OT necessitate distinct approaches to security incident response, safety protocols, cybersecurity controls, engineering methodologies, support structures, system design principles, threat detection mechanisms, and network architectures.

❖ **Technological Hurdles**

- **Legacy Systems.** Legacy ICS systems are often vulnerable to cyberattacks due to the lack of security features and compatibility with modern systems. This can lead to data breaches, downtime, and even physical damage. Many industrial control systems, built decades ago when security wasn't a top priority, lack essential features like encryption and authentication, making them vulnerable to cyberattacks. Incompatibilities often pose a challenge for communication between IT and OT environments. OT devices may not use IT-compatible communication protocols or be limited to one-way communication. ICS environments are intricate and diverse, often these systems are procured by different vendors. This complexity can make consistent security implementation challenging.
- **Outdated Software.** Often, critical infrastructures are equipped with both new and legacy devices in the environment. These devices, many times, underlying outdated software that are no longer supported by vendors, which results in CVEs and other vulnerabilities.
- **Lack of device Visibility.** The incompatibility of legacy systems and proprietary communication protocols with traditional IT solutions makes it difficult for IT security teams to gain a complete inventory of OT assets. This makes it impossible to identify and assess threats and vulnerabilities. The first step in accelerating network segmentation is to identify all connected devices in the environment.
- **Scalability.** The proliferation of edge devices and the vast amount of data they produce that can strain IT infrastructure. Without careful planning, edge devices may overwhelm IT systems by generating more data than they can effectively process.

❖ **Human Factors - Fostering Cooperation between IT security teams and OT personnel**

Achieving successful IT/OT convergence necessitates a multifaceted approach. Firstly, it requires cultivating a skilled workforce with expertise in both domains, fostered through innovative training initiatives. Secondly, organizations must embrace a paradigm shift in their mindset, promoting a collaborative environment where IT and OT specialists develop mutual appreciation for each other's roles and engage in cross-training to bridge knowledge gaps. This unification of IT security and operational professionals, dismantling siloed security structures, empowers industrial organizations to bolster their defenses against escalating cyber threats within an increasingly complex and concerning threat landscape.

All these challenges are then heightened by the rapid pace of technological evolution, which creates a technological gap as organizations grapple to synchronize disparate systems. The increasing proliferation of IT capabilities into OT/physical systems can provoke behavioral changes in the structure of the enterprise with underlying security implications.

The once hidden realm of OT has opened itself to the outside . . .

3. ICS Cybersecurity Standards and Compliance

3.1 Cybersecurity Standards and Regulations on ICS

Due to the newly emerged threat landscape and sensitive nature of industrial controls systems (ICS), governments and regulatory bodies all over the world have required cybersecurity standards and regulations to secure critical infrastructure.

Critical infrastructure has faced major cybersecurity challenges in 2023, with adversaries deploying sophisticated ransomware attacks on critical systems, potentially disrupting train operations and exploiting vulnerabilities in maritime networks, posing significant operational risks to navigation and safety. Governments and organizations took steps to enhance cybersecurity measures, collaboration, and regulatory frameworks to address these evolving threats and protect essential infrastructure.

Cybersecurity compliance arises from the necessity to safeguard critical infrastructure, networks, data, and operations from cyberattacks. This is achieved by adhering to established cybersecurity standards, regulations, and best practices. National security laws and international standards have become significant drivers for corporations to implement and operate intrusion detection systems, actively defending against evolving threats.

The regulations of the US and Europe governments in this area define the OT cybersecurity of industrial infrastructure for the decade to come from 2020 through 2030 and further. The requirements are designed so that they will be relevant in the years to come and allow for adaptability to counter threats that are continuously evolving and manage risk in different environments. Instead of specifying the tools and technologies that must be implemented, the new guidelines are outcome oriented. The operators will be required to determine the goals, analyze risks, and develop and carry out plans aimed at achieving their desires.

The aim of such an approach is to be flexible. Despite the fact that the requirements are directed at certain vital industrial sectors including energy and transportation, any organization can use the guidelines to protect its industrial operations.

A breakdown and assessment of the adequacy of existing regulations, standards, and directives under the national or international scope, contributes to building resilience and business continuity in OT environments and the critical infrastructure sector.

3.1.1 Regional Regulations & Standards

Reducing critical vulnerabilities and increasing resilience is one of the EU's key objectives. Adequate protection must be ensured and the negative effects of violence on the community and the citizens must be limited to the extent possible. Cybersecurity efforts were shaped by existing and future directives, such as regulations, that incentivized organizations to strengthen security and comply with guidelines such as the NIS Directive [5] and the EU Cybersecurity Act [6]. However, compliance across industries remains a challenge, requiring constant efforts to increase adoption and remediation.

➢ **NIS2 Directive (EU)**

The NIS regulation is the regulation on network and information systems. The first regulation, now called NIS1, was adopted by the EU Parliament in July 2016 and came into force on May 10, 2018. At the time, it was the world's first cybersecurity legislation.

The NIS1 Directive introduced a framework for member states to implement national cybersecurity measures. It did not directly mandate specific cybersecurity standards across the board. Instead, it encouraged member states to adopt a risk-based approach and outlined core security measures that essential organizations such as critical infrastructures were expected to follow**.** NIS2 builds upon this foundation by expanding the definition and group of the so-called essential companies and imposing stricter security requirements on these designated sectors.

It applied to two groups: operators of essential services (OES) (water, transportation, and energy infrastructure) and digital service providers (DSP) (cloud computing (IaaS, PaaS, SaaS), online marketplace, online search engine).

In Europe, the Russian invasion of Ukraine in 2022 helped spur the European Union to update its Network and Infrastructure Security Directive of 2016. Enacted in January 2023, the EU's NIS2 Directive 2022/2555 [7] aims to strengthen the security and resilience of network and information systems across member states. While EU members have until October 2024 to transpose the directive into national law, affected organizations must comply within a year. As the deadline approaches, immediate action is crucial for organizations to embrace these upcoming changes.

The updated NIS2 Directive is a modernized framework and the first piece of EU-wide legislation on cybersecurity. The NIS2 Directive defines 10 critical infrastructure sectors and establishes a common level of cybersecurity across the EU. NIS2 aims for a more aligned cybersecurity management approach to mitigate inconsistencies in cybersecurity resilience across sectors, outlining several key measures to manage risks posed to networks and information systems. NIS2 is in direct response to the growing threat landscape; at the heart of the new legislation is that organizations within critical infrastructure sectors must improve their resilience, detection, and incident response capabilities.

The Directive provides legal measures to boost the overall level of cybersecurity in the EU by focusing on preparedness and cooperation within critical sectors. Under the Directive, operators of essential services must take appropriate security measures, notify relevant national authorities of serious incidents, and mitigate security risks in their supply chains by assessing the product quality and cybersecurity practices of suppliers and service providers. Management bodies are required to take an active role in supervision and implementation, bolstering the importance of the CISO as an educator and best practices guide for senior executives. To do so they must provide associated plans for how they intend to comply. Updates to the Directive expand its scope to include new critical sectors, and additional considerations for determining “essential” vs. “important” entities. Non-compliance may result in fines, management liability, temporary bans against managers, and more. Fines for non-compliance could amount to €10 million or 2% of global turnover for essential entities and €7 million or 1.4% of global turnover for important entities.

- **Critical Entities Resilience − CER Directive (EU)**

The European Commission, in 2020, proposed strengthening EU regulations on critical infrastructure resilience and network and information system security. To address online and offline threats, including cyberattacks, crime, public health risks, and natural disasters, two key directives entered into force on January 16, 2023: the Critical Entities Resilience Directive (CER) [8] and the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). On 25 July 2023, the Commission Delegated Regulation [9] establishes a non-exhaustive list of essential services in all the sectors and sub-sectors of the CER Directive. The list is to be used by the competent authorities for the purpose of carrying out a risk assessment and thereafter the risk assessment is to be used for the purpose of identifying critical entities. Critical entities provide essential services in upholding key societal functions, supporting the economy, ensuring public health and safety, and preserving the environment.

Until October 17, 2024, Member States must transpose the requirements of the CER Directive into national law. Also, pursuant to the CER Directive, Member States shall adopt a national strategy for enhancing the resilience of critical entities and carry out a risk assessment by 17 January 2026. Taking into account the outcomes of the risk assessment, Member States shall identify critical entities by 17 July 2026. Even if the deadline for identifying critical entities is set for July 17, 2026, the compliancy requirements should be taken seriously, because non-compliance could lead to penalties. The directive itself does not set limits on fines, leaving the determination to national implementation.

The CER Directive addresses a gap in existing EU regulations, which previously only covered specific aspects of resilience in certain sectors. The CER Directive establishes a comprehensive framework across all sectors, encompassing both natural and man-made threats. Critical entities are now obligated to regularly (at least every four years) assess their vulnerabilities and develop strategies to mitigate disruption to essential services.

➢ Cyber Resilience Act − CRA (EU)

The Cyber Resilience Act (CRA) [10] is a cyber-security regulation for the EU that was announced in the 2020 EU Cybersecurity Strategy, and complements other legislation in this area, specifically the NIS2 Framework. The CRA was proposed on 15 September 2022 by the European Commission for improving cybersecurity and cyber resilience in the EU through common cybersecurity standards for products with digital elements in the EU. On 1st December 2023, the European Commission reached political agreement on the CRA, the EU reached political agreement on the CRA, the first legislation globally to regulate cybersecurity for digital and connected products that are designed, developed, produced, and made available on the EU market. The CRA agreement must now receive formal approval by European Parliament and the Council prior to being enforced.

The newly adopted Critical Entities Resilience Act (CRA) joins the Data Act**,** Digital Operational Resilience Act (DORA), CER, NIS2, and Data Governance Act, solidifying the EU's data and cybersecurity agenda. It complements forthcoming certification schemes like EU Cloud Service Scheme (EUCS) and EU ICT Products Scheme (EUCC), and responds to the alarming surge in cyberattacks, particularly the tripling of software supply chain attacks. This surge, coupled with the growing presence of digital and connected products in our daily lives, necessitates robust measures to mitigate these evolving risks. Indicative cyberattacks that exploited the security of products with digital elements are the following:

- The Pegasus spyware, which exploited vulnerabilities in mobile phones.
- The WannaCry ransomware, which exploited a Windows vulnerability that affected computers across 150 countries.
- The Kaseya VSA supply chain attack, which used network administration software to attack over 1000 companies.

The recently adopted CRA aims to bolster cybersecurity within the European Union by setting mandatory requirements for a range of hardware and software products with digital components (industrial control systems, sensors, smart meters, smart robots etc.), including products whose "intended and foreseeable use includes direct or indirect data connection to a device or network.

This legal framework seeks to address the increasing prevalence of cyberattacks and the associated vulnerabilities found in many products. By introducing a framework of cybersecurity standards throughout the entire product lifecycle, the CRA aims to ensure better design, development, and maintenance of these products, ultimately fostering informed decision-making and a more secure digital environment for businesses and consumers. The CRA applies to:

i. **Products with digital elements (PDEs):** These include any software or hardware designed to connect to a device or network, such as smart appliances or home security systems.

ii. **Remote data processing solutions for PDEs:** This encompasses cloud services or other systems necessary for the PDE's function, like a mobile app allowing users to control their smart devices remotely.

iii. **Individual software or hardware components of PDEs sold separately:** This applies to all components except spare parts that are placed on the EU market separately.

The CRA mandates a range of obligations for manufacturers and importers of PDEs, including:

- Designing PDEs to meet certain essential cybersecurity requirements through risk assessment and protection against known vulnerabilities.
- Submitting PDEs to conformity assessments.
- Notifying identified vulnerabilities (within 24 hours) to the relevant national cybersecurity authority, the entity that maintains the vulnerable PDE and, potentially, ENISA.
- Notifying severe security incidents to ENISA, the relevant national cybersecurity authority, and users of the PDE.
- Conducting due diligence on imported PDEs.

Manufacturers are now obliged to take security seriously throughout a product's life cycle. Under the CRA, manufacturers of in-scope products will be required to conduct mandatory security assessment requirements, implement vulnerability-handling procedures, and provide necessary information to users. The CRA will apply to products placed on the market in the EU, irrespective of where the products are manufactured. Products designated as critical will be subject to more onerous obligations. The CRA also proposed high fines for non-compliance, up to €15 million or 2.5% of annual turnover.

The Council, on December 20, 2023, expressed its intent for swift adoption of the final CRA text in Q1 2024. Obligations will be implemented in phases. While a 36-month transition period is granted for most provisions, allowing manufacturers to adapt products, vulnerability and incident reporting by manufacturers will commence 21 months after entry into force.

3.1.2 International Regulations & Standards & Frameworks

- **ISA/IEC 62243 *Standard***

The IEC 62443 standards emerged from a collaborative effort by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) to address the growing cybersecurity threats to industrial automation and control systems. In 2022, the ISA formed a dedicated committee, ISA99, to establish cybersecurity standards for industrial systems. ISA99 brought together experts from various sectors to develop comprehensive standards that could be applied across industries. The initial work of ISA99 resulted in the ISA-99 standards, which laid out the foundation for securing industrial automation and control systems. In 2010, the IEC adopted the ISA-99 standards as IEC 62443. IEC 62443 has been updated and expanded to address the evolving cybersecurity threats and technological advancements in industrial automation. Today, IEC 62443 is one of the most comprehensive and widely recognized standards for industrial cybersecurity worldwide.

The ISA/IEC 62443 standards are the most comprehensive and exhaustive industrial cybersecurity standards available to the industrial and manufacturing sector, which addresses the cybersecurity challenges of industrial automation and control systems (IACS) and OT environments. The IACS technologies are central to critical infrastructure and OT environments. Apart from geographically dispersed operations, IACS includes control systems used in manufacturing and processing plants and facilities, including those found across the utilities, pipelines, petroleum production, and distribution facilities. ISA/IEC standards establish a unified cybersecurity benchmark across various critical infrastructure sectors utilizing Industrial Automation and Control Systems (IACS).

The ISA/IEC 62443 series addresses industrial automation and control system (IACS) cybersecurity comprehensively, defining requirements and processes for secure implementation and maintenance. These standards go beyond establishing best practices by providing a framework for assessing security performance. Their holistic approach bridges the gap between operational technology and information technology, fostering collaboration between cybersecurity and process safety disciplines.

The standard recommends a multi-layered defense strategy, known as 'defense in depth'. This strategy involves implementing multiple levels of security controls throughout the system to provide redundancy, ensuring that if one measure fails or a vulnerability is exploited, other protective layers remain intact.

ISA/IEC 62443 is a functional standard – the series sets objectives for security performance but does not define how these objectives should be met. The series is referenced throughout the NIST Cybersecurity Framework (CSF) [11], and most recently, within the CISA Cybersecurity Performance Goals (CPGs) [68]. The CPGs extensively reference ISA/IEC 62443-2-1 and ISA/IEC 62443-3-3 in almost every category, including account security, device security, data security, governance and training, vulnerability management, supply chain/third party, and response and recovery.

The ISA/IEC 62443 series adopts a risk-based, methodical approach to enhance the reliability, integrity, and security of IACS. This standards-based framework offers several advantages: it reduces the probability of successful cyberattacks, simplifies system complexity by establishing common stakeholder requirements, and fosters comprehensive security throughout the IACS lifecycle. The standards define a unified set of terminology and requirements for asset owners, product suppliers, and service providers, outlining a comprehensive framework for designing, planning, integrating, and managing secure IACS.

Zones and Conduits

IEC 622443-3-2 addresses security risk assessment and network design. It suggests how organizations should segment their network into zones and conduits, grouping systems which are similar in functionality and restricting access to limit threat exposure and propagation. This standard defines as a security zone a group that pertains to functionally, logically, and physically related systems with shared security needs. Also, conduits are specified as the communication channels that link zones with similar security requirements.

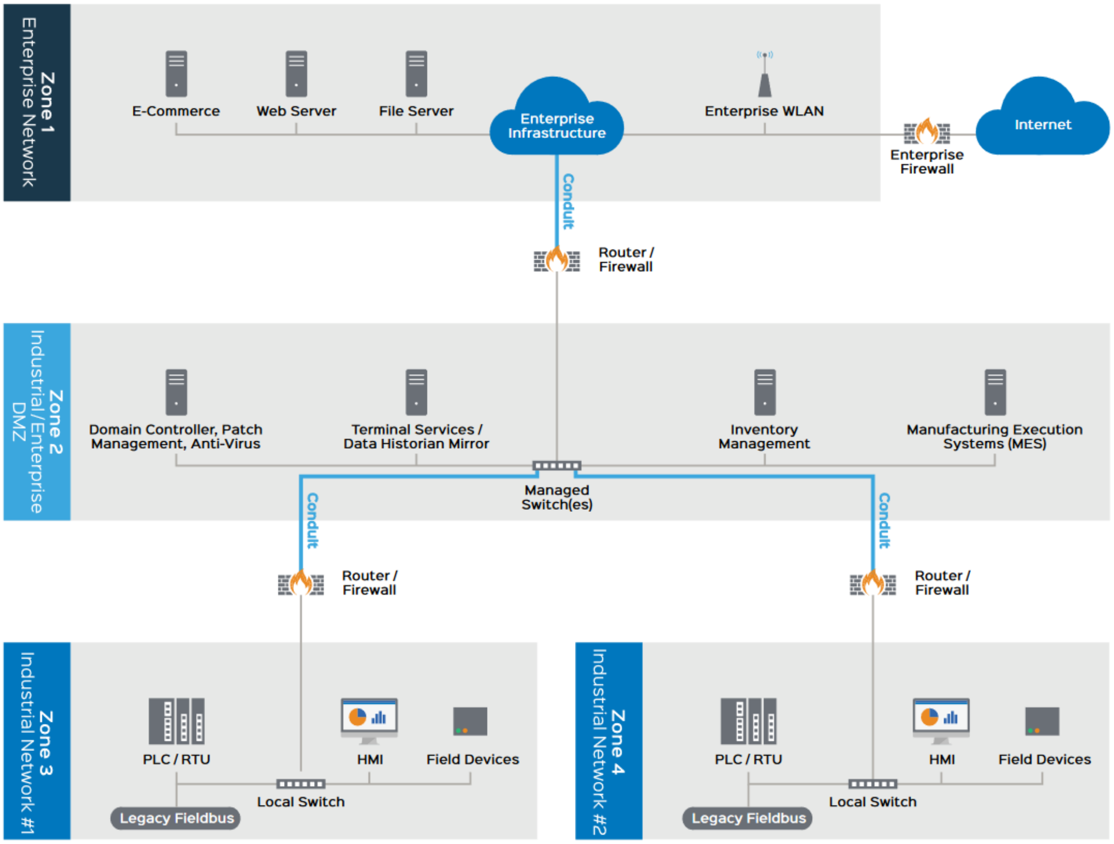
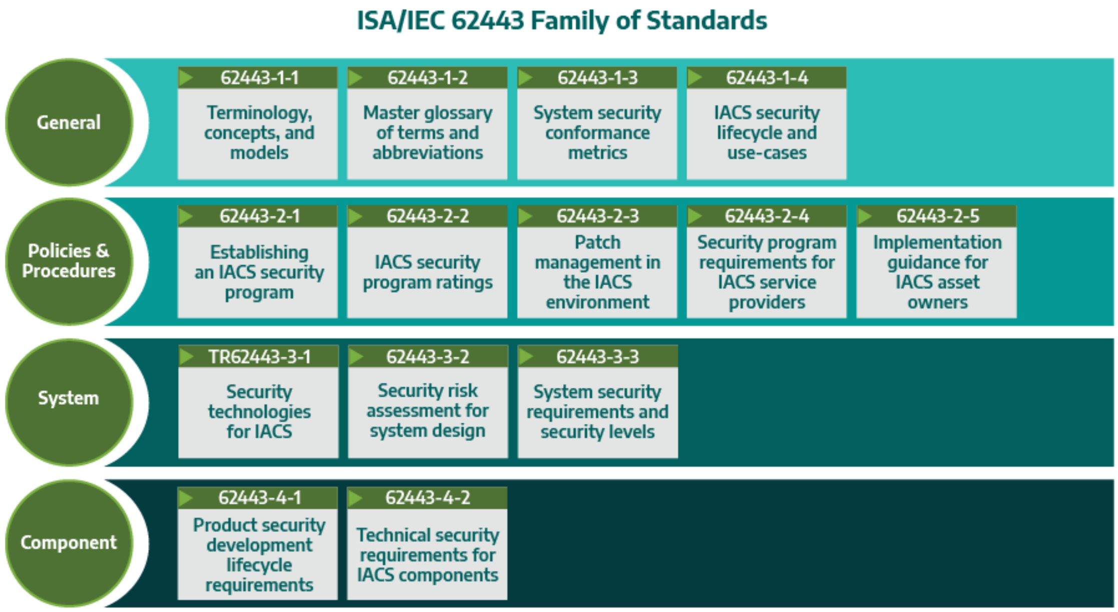


Figure 6 Source: ISA [12]

Breakdown of the IEC 62443 standards

The IEC 62443 series comprises 14 standards, technical reports (TR), and technical specifications (TS). They can further be classified into four groups – General, Policies and Procedures, System, and Component. The first two groups describe concepts, use cases, policies, and procedures associated with ICS security. In contrast, the two latter groups focus on the technical requirements for networks and system components. The four parts of the IEC 62443 series of standards are organized into:

1. General: covers topics that are common to the entire series
2. Policies and procedures: focus on methods and processes associated with IACS security
3. System: is about requirements at the system level
4. Component and requirements: provide detailed requirements for IACS products



ISA/IEC 62443 Family of Standards

General	62443-1-1 Terminology, concepts, and models	62443-1-2 Master glossary of terms and abbreviations	62443-1-3 System security conformance metrics	62443-1-4 IACS security lifecycle and use-cases	
Policies & Procedures	62443-2-1 Establishing an IACS security program	62443-2-2 IACS security program ratings	62443-2-3 Patch management in the IACS environment	62443-2-4 Security program requirements for IACS service providers	62443-2-5 Implementation guidance for IACS asset owners
System	TR62443-3-1 Security technologies for IACS	62443-3-2 Security risk assessment for system design	62443-3-3 System security requirements and security levels		
Component	62443-4-1 Product security development lifecycle requirements	62443-4-2 Technical security requirements for IACS components			

Figure 7 ISA/IEC 62443 Overview, [13]

Compliance and Certification

Compliance with this standard demonstrates a systematic, risk-based approach to IACS security, facilitating certification and stakeholder/client assurance. Current verifiable standards fall into two main categories:

- **Security Standards**: ISA/IEC 62443-3-3 and ISA/IEC 62443-4-2 define security levels for IACS products referring to systems, subsystems, and related components Additionally, 62443-4-2 classifies components by type (software, embedded devices, networking equipment, and control devices).
- **Process Standards**: ISA/IEC 62443-2-4 and ISA/IEC 62443-4-1 define processes and procedures for organizations. 62443-2-4 covers service procedures (maintenance, updates, installation, deployment etc.) while 62443-4-1 addresses product development procedures.

Security Requirements and Levels

One of the key features of the IEC 62443 standards is the incorporation of security levels (SL) to assess the cybersecurity risks posed to OT and ICS systems. This capability empowers both industrial organizations and asset owners and operators to gain a comprehensive understanding of their assets, their interconnectivity within the infrastructure, potential security vulnerabilities, and the need to address them promptly to prevent adversaries from exploiting them. The IEC 62443 standards classify security levels into five grades, ranging from 0 to 4, with SL 0 representing the lowest level of risk and SL 4 signifying the highest or most vulnerable level. This model dictates that SL 4 systems demand more stringent compliance measures compared to SL 0 systems. The varying SL grades indicate the ability of the system to withstand cyberattacks from different classes of adversaries. To meet the security requirements of each SL, it is crucial for industrial systems to implement robust protective measures that safeguard uptime, safety, and intellectual property.

Security Level (SL)	Description
0	No specific requirements or security protection requirements
1	Requires protection against casual or coincidental violations
2	Requires protection against intentional violation using simple means with low resources, generic skills, and low motivation
3	Requires protection against intentional violation using sophisticated means with moderate resources, specific skills, and moderate motivation
4	Requires protection against intentional violation using sophisticated means with extended resources, specific skills, and high motivation

Figure 8 Source: IEC62443-3-3, (source: [14])

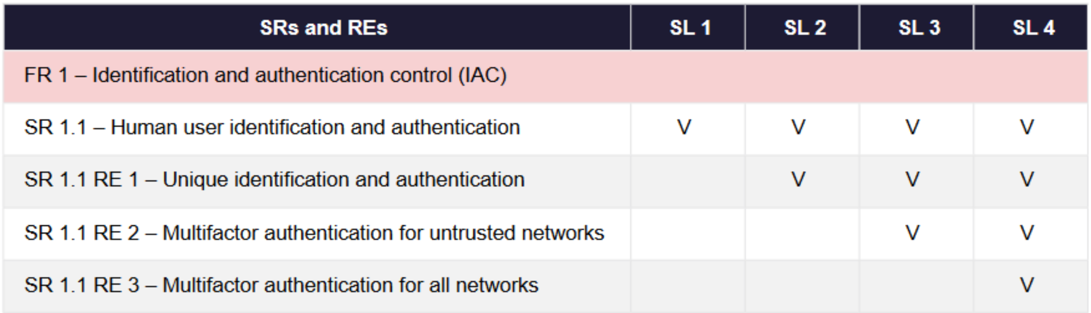
To measure a Security Level (SL), System Requirements (SR) are specifically defined for each Foundation Requirement (FR). Furthermore, for each System Requirement (SR), Requirement Enforcements (RE) are specified to satisfy each Security Level (SL). The ISA/IEC 62443 standard provides practical guidelines on how to implement protective measures against cybersecurity incidents based on defined security levels, broken down into seven basic requirements, called Foundational Requirements (FR).

- *FR1 – Identification and Authentication Control (IAC):* Reliably identify and authenticate all users (human, software processes, and devices) attempting to access the IACS.
- *FR2 – Use Control (UC)*: Enforce the assigned privileges of authenticated users (humans, software processes, or device) ensuring they can only perform authorized actions and that their activity is monitored.
- *FR3 – System Integrity (SI)*: Protect the integrity of the industrial automation and control system from unauthorized modifications that could impact its operations or data.
- *FR4 – Data Confidentiality (DC)*: Ensure confidentiality of information on communication channels and data repositories. Prevent unauthorized disclosure.
- *FR5 – Restricted Data Flow (RDF)*: Segment the control system via zones and conduits to limit the unnecessary flow data.
- *FR6 – Timely Response to Events (TRE)*: Respond to security violations. Notify the proper authority reporting needed evidence of the violation. Take timely corrective action when incidents occur.
- *FR7 – Resource Availability (RA)*: Maintain the availability of the control system against degradation or denial of essential services, ensuring authorized user access and utilization when needed.

SR - System Requirement: any system requirements as a part of system hardening against bounded 7 foundation requirements (as explained above).

RE - Requirement Enhancement: each SR has a baseline requirement and zero or more requirement enhancements (REs) within envelopes of foundational system requirements to strengthen security.

The standard defines Security Levels (SLs) using threat definitions and maps them to specific Foundational Requirement (FR) levels. Due to the dynamic nature of the industrial control system (ICS) threat landscape, SLs can be further tailored to individual security zones, considering unique threats, operational changes, and IIoT integration. While providing targets, SLs should remain adaptable to evolving global threats.



SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user identification and authentication	V	V	V	V
SR 1.1 RE 1 – Unique identification and authentication		V	V	V
SR 1.1 RE 2 – Multifactor authentication for untrusted networks			V	V
SR 1.1 RE 3 – Multifactor authentication for all networks				V

Figure 9 Example of ISA/IEC 62443 Security Levels

When native technical solutions are insufficient to achieve acceptable risk levels within an IACS zone or conduit, compensating countermeasures (e.g., policies, procedures) can be implemented to meet security requirements. These complementary measures strengthen existing technological safeguards to reduce the risk to a tolerable level. Alternatively, compliant technical solutions can be deployed.

While the ISA/IEC 62443-3-3 security framework may appear complex, businesses can navigate it efficiently. Leaders can empower relevant teams by creating a clear roadmap for OT security improvement. This process starts with a risk analysis. By understanding the gap between the current site’s security posture and the standard, the security teams can pinpoint weak areas for improvement. This may involve revising processes, implementing new technology, or investing in employee training. By adopting a phased approach, actions can be prioritized, based on available resources, ensuring sustainable progress towards compliance.

The adoption of any level of ISA/IEC 62443 is optional and driven by individual network risk assessments. It empowers organizations to build a robust OT security foundation. Each organization by tailoring risk assessments to its unique risk needs, can define the security level necessary to safeguard their ICS and achieve business and regulatory compliance. As a cornerstone for securing OT, following ISA/IEC standards offers a clear path to organization to address existing security gaps and ultimately strengthen the overall industrial automation environment.

➢ NIST CSF 2.0

NIST Cybersecurity Framework (CSF) 2.0 [11], an update to the standardized cyber risk management approach for diverse sectors, released on *26 February 2024*. Developed by the National Institute of Standards and Technology (NIST), this framework establishes cybersecurity best practices benchmarks. Organizations can utilize their own timelines to update configurations or maturity assessments based on the previous framework version.

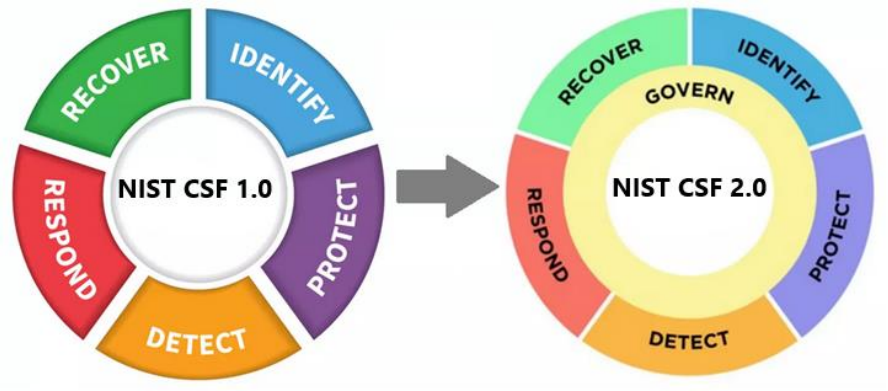


Figure 10 NIST CSF versions evolution

The new version 2.0 of the popular NIST Cybersecurity Framework has expanded beyond the original framework's five functions of an effective cybersecurity program — identify, protect, detect, respond, and recover — and added a sixth, govern. CSF 2.0 is a significant revision of the previous version, with several new features and improvements. The key updates in the CSF 2.0 are broken down into six parts: changes in the scope of application, emphasizing the importance of governance, integration with OT/ICS-related standards, updates to the CSF 2.0 implementation guide, updates to cybersecurity supply chain risk management, and cybersecurity metrics and evaluation.

- **Expanding the Scope of CSF 2.0**

The Cybersecurity Framework 2.0 (CSF 2.0) has undergone modifications to broaden its scope and enhance applicability. The revised title "Cybersecurity Framework" reflects the framework's broader applicability beyond critical infrastructure organizations. NIST intends to make the framework more inclusive of smaller businesses and higher education institutions, aligning with the U.S. Congress's request. CSF 2.0 also places a strong emphasis on international collaboration, showcasing its global adoption and plans to actively participate in international cybersecurity standards development.

- **Emphasizing the Importance of Governance**

In CSF 1.1, the core consisted of five functions: “Identify”, “Protect”, “Detect”, “Respond”, and “Recover”. In CSF 2.0, a “Govern” function has been added. This new governance function, positioned more like a central feature of the framework, differs from the previous five functions. The “Govern” function involves understanding the organization’s setting, creating a cybersecurity strategy, and managing supply chain risks, defining roles and responsibilities, setting up policies and procedures, and overseeing the cybersecurity strategy. This function emphasizes the need for organizations to have a strong cybersecurity governance framework in place, which includes things like risk management, incident response, and compliance. In other words, it informs how an organization will implement the other five functions.

- **Integrating OT/ICS Standards into the Framework**

NIST is actively promoting the creation of mappings that align CSF 2.0 with other cybersecurity resources. Such mappings will facilitate the integration of CSF 2.0 with specific guidelines, such as the "Internet of Things (IoT) Cybersecurity Capabilities Baseline" and the "Guide to Operational Technology (OT) Security" (SP 800-82 Rev. 3) [15]. Additionally, these mappings will establish a clear connection between CSF 2.0 and the principles of Zero Trust Architecture (NIST SP 800-207) [16]. By creating these functional and category-level mappings, CSF 2.0 will enhance its compatibility with other resources, expanding its practical applications**.**

- ➢ NIST SP 800-82r3 [15]

  Amidst a backdrop of intensifying threats and perilously close near-miss attacks directly targeting operational technology (OT), the National Institute of Standards and Technology (NIST) recently unveiled the third iteration of the NIST SP 800-82 document, titled "Guide to Operational Technology (OT) Security". NIST published the first draft of Special Publication (SP) 800-82r3 (Revision 3) in April 2021, with a second draft being released one year later. Now, Revision 3 of the OT security guide has been finalized. The guidance focuses on OT cybersecurity program development, risk management, cybersecurity architecture, and applying the NIST Cybersecurity Framework (CSF) to OT. The document also aligns with other OT security guides and standards, and provides tailored security control baselines for low-, moderate- and high-impact OT systems. The new release underscores an expanded focus on OT, distinct from its prior emphasis on industrial control systems (ICS). Significantly, the NIST SP 800-82r3 publication incorporates critical updates covering the gamut of OT threats and vulnerabilities, while also advancing the field of **OT risk management**, recommended practices, and architectural considerations (Zero Trust). The document also serves as a beacon for OT asset owners and operators, delivering the most current advancements in OT security protocols. It not only imparts the latest developments in security practices tailored for OT environments but also provides them with critical security capabilities and tools, thus fortifying their defense against potential cyber threats. Furthermore, NIST SP 800-82r3 introduces an all-encompassing overhaul of OT risk management, emphasizing the necessity for a proactive stance in cybersecurity. The recommended practices put a premium on bolstering the security stance of OT networks, featuring upgraded authentication protocols and the implementation of network segmentation. The updated architectures prioritize resilience, advocating the incorporation of layered defenses and continuous monitoring mechanisms, thereby aligning with prevalent industry standards and best practices.

- **Adding Implementation Guidance to CSF 2.0**

  CSF 2.0 has introduced action-oriented samples to make the framework more accessible and applicable. These samples provide templates for creating organizational action plans, simplifying the implementation of CSF principles for organizations of all types. The concise and practical examples in CSF 2.0 reinforce the framework's effectiveness and provide guidance for those unfamiliar with cybersecurity standards.

- **Cybersecurity Supply Chain Risk Management**

  NIST has recognized the increasing importance of managing supply chain and third-party cybersecurity risks. CSF 1.1 introduced a category and content to address these risks, but CSF 2.0 takes a more explicit approach by incorporating supply chain management into the

Govern function and creating new functions to specifically focus on supplier risk assessment. NIST is also updating its Secure Software Development Framework to further strengthen supply chain cybersecurity measures. These changes reflect NIST's commitment to addressing the challenges of managing supply chain and third-party cybersecurity risks. CSF 2.0 document’s spotlight on supply chain risks covers how various types of technologies rely on a complex ecosystem for outsourcing, which involves geographically diverse routes for both private and public sector organizations that offer a variety of services. In the updated CSF, NIST points to Cybersecurity Supply Chain Risk Management (C-SCRM) [17] as a systemic process to manage exposure to cybersecurity risks by developing appropriate "strategies, policies, processes and procedures."

- **Cybersecurity Metrics and Evaluation**

  Cybersecurity metrics and evaluation are crucial for assessing an organization's cybersecurity maturity and tracking its progress. CSF 2.0 provides a unified framework for measuring and evaluating cybersecurity, allowing organizations to tailor it to their unique risk profiles and systems. CISA has released voluntary cross-sector cybersecurity performance goals aligned with CSF 2.0, offering a benchmark for improving cybersecurity posture. NIST is also updating its "Guide for Performance Measurement of Information Security" (SP 800-55r2) to provide guidance on measuring and implementing cybersecurity programs.

The CSF 2.0 is a living document, which means that it is continually being updated to reflect changes in the cybersecurity landscape. This means that organizations should regularly review the framework and make changes as needed to address new risks and threats. The CSF 2.0 is not a one-size-fits-all solution. Organizations should tailor the framework to their specific needs and requirements. There are a number of resources available to help organizations implement the CSF 2.0, including the NIST website, the NIST Cybersecurity Framework Self-Assessment Tool, and the NIST Cybersecurity Framework Implementation Guide.

The NIST framework is a widely adopted set of cybersecurity standards and practices that are utilized by the US federal government and organizations worldwide. The applied changes to the existing NIST framework are significant due to their far-reaching impact on cybersecurity practices. Many vendor security products are developed to adhere to NIST standards, and the federal government invests billions of dollars to ensure the framework remains current, reliable, and industry-leading. Regular updates to NIST policies are crucial to prevent a significant portion of global security from becoming outdated and vulnerable to increasingly sophisticated and frequent cyberattacks.

➢ ISO/IEC 27001 *Standard*

ISO/IEC 27001 is a widely recognized international standard for establishing and maintaining an ISMS (Information Security Management System), empowering critical infrastructure organizations to become proactive risk managers and identify weaknesses promptly. The standard is published by the International Organization for Standardization (ISO) and is designed to help organizations protect their sensitive information and systems from potential threats. ISO 27001 outlines a number of key principles and requirements for implementing an effective ISMS, including:

- Conducting a risk assessment to identify potential threats and vulnerabilities and implementing measures to mitigate them.
- Implementing strong security controls, such as access controls and encryption, to protect against unauthorized access to sensitive information.

- Regularly monitoring and reviewing the effectiveness of the ISMS to ensure that it remains effective and up to date.
- Having a plan in place for responding to and recovering from security incidents.

OT/ICS and critical infrastructure domains can significantly benefit from implementing ISO/IEC 27001, a comprehensive framework for managing cybersecurity. ISO/IEC 27001 mandates a risk-based approach to cybersecurity. This means that organizations must identify, assess, and prioritize cybersecurity risks before implementing mitigation measures. This approach is essential for OT/ICS and critical infrastructure domains, as these systems are often more vulnerable to cyberattacks than traditional IT systems. By identifying and addressing the most critical risks, organizations can reduce their overall cybersecurity risk.

ISO/IEC 27001 also provides a comprehensive framework for managing cybersecurity, covering all aspects of the organization's security lifecycle, from policy development to incident response. This comprehensive approach is necessary for OT/ICS and critical infrastructure domains, as these systems encompass a wide range of hardware, software, and data. By having a holistic view of their cybersecurity, organizations can ensure that they are protecting all their assets.

The standard's guidelines and principles can be effectively adapted to address specific cybersecurity challenges faced by critical infrastructure domains, including:

- **Power Grids:** ISO/IEC 27001 can be applied to secure SCADA systems, communication networks, and data centers that form the backbone of power grids. It can help identify and mitigate cyber threats, protect sensitive data, and ensure the resilience of power grid operations.
- **Water and Wastewater Utilities:** ISO/IEC 27001 can be employed to safeguard operational technology (OT) systems, supervisory control, and data acquisition (SCADA) networks, and data centers that manage water distribution and wastewater treatment processes. It can help prevent disruptions to critical infrastructure services and protect sensitive water data.
- **Transportation Systems:** ISO/IEC 27001 can be implemented to secure railway signaling systems, communication networks, and passenger information systems. It can help prevent cyberattacks that could disrupt transportation networks and compromise passenger safety.
- **Communication Networks:** ISO/IEC 27001 can be utilized to protect core network infrastructure, data centers, and customer-facing systems. It can help prevent data breaches, maintain network security, and ensure the reliability of communication services.
- **Healthcare Infrastructure:** ISO/IEC 27001 can be applied to secure electronic health records (EHRs), medical devices, and communication networks within healthcare facilities. It can help protect patient privacy, maintain operational continuity, and prevent disruptions to healthcare services.
- **Financial Services:** ISO/IEC 27001 can be implemented in banks, financial institutions, and payment processing systems. It can help safeguard sensitive financial data, prevent cyberattacks, and maintain trust in the financial system.

By implementing this comprehensive framework, organizations can effectively manage and protect the confidentiality, integrity, and availability of sensitive information, including financial data, employee data, and customer data. Similar to IEC 62443, ISO/IEC 27001 enhances compliance with regulatory requirements, including those mandated by the DHS (U.S Department of Homeland Security) and the GDPR. Ultimately, by adopting this holistic cybersecurity framework, organizations can safeguard sensitive data from cyber threats and maintain a secure operational environment.

- **MITRE ATT&CK for ICS**

The variety of standards reflect different approaches and enables security professionals to choose which standard emphasizes what they consider to be most critical. While some frameworks focus on increasing network hygiene to mitigate the chances and impact of a cyberattack, others may focus on threat detection or quick recovery. One of the important threat detection frameworks is MITRE ATT&CK for ICS [18]. As described by MITRE, “This is a knowledge base useful for describing the actions an adversary may take while operating within an ICS network”. Based on real actions exhibited by threat actors, MITRE ATT&CK for ICS is a variant of the enterprise and mobile ATT&CK matrices and is updated frequently to account for what is seen in the wild. This framework is used worldwide across multiple disciplines including intrusion detection, threat hunting, security engineering, threat intelligence, red teaming, and risk management.

MITRE ATT&CK ICS is a standard framework for identifying the various TTPs (Tactics, Techniques and Procedures) that adversaries use to gain their foothold and pivot into ICS/OT networks. This specialized framework differs from MITRE ATT&CK Enterprise framework by focusing on adversaries aiming to disrupt critical operational processes, steal sensitive information, or trigger safety hazards through targeted attacks on ICS infrastructure.

On October 31st, 2023, MITRE released *version 14* of its ATT&CK framework. The new release made some major changes by including enhancements to the detection content, new industrial control system (ICS) assets, and the addition of structured detections for mobile.

A recent SANS study (Q4 2023) revealed that only 22% of ICS facilities leverage the MITRE ATT&CK ICS framework to identify advanced ICS-specific threat detection capabilities. This powerful tool can empower organizations to adopt a proactive approach to ICS cybersecurity, moving beyond reactive measures. By leveraging threat intelligence specific to their sector and utilizing technical analysis, security teams can identify active adversary capabilities as also key data sources and relevant tools in order to proactively build mitigation strategies and bolster their ICS defenses.

OT and ICS cyber defenders can effectively utilize MITRE ATT&CK for ICS in several ways, including but not limited to:

- Accelerating response times and prioritizing risks when dealing with attacks on industrial systems.
- Enhancing detection capabilities by providing valuable insights on what to monitor for.
- Employing hypothesis-driven threat hunting to uncover concealed or emerging threats that match patterns identified in the framework.
- Safeguarding ICS security plans by keeping up with evolving attack methods tracked by ATT&CK, thus ensuring their effectiveness in the future.

3.1.3 Key Regulations/Standards per Critical Infrastructure Sector

- **NERC CIP Standard (USA - Electric Power Grid)**

Initially this standard was developed in 2003 by NERC with the intention of creating an industrial safety standard for companies in the electricity sector, the initial version was named as NERC CSS (*Cyber Security Standards*), after successive improvements and evolutions the most current version is known as NERC-CIP, and although its origin is North American, it is currently implemented in several Latin American countries such as Mexico, Colombia, Ecuador, Brazil, Chile and Peru.

The North American Electric Reliability Corporation (NERC) [19] Critical Infrastructure Protection (CIP) standards are mandatory security standards that apply to utility companies connected to the North American power grid. The CIP standards were adopted in 2006 and establish a baseline set of cybersecurity measures aimed at regulating, enforcing, monitoring, and managing the security of the Bulk Electric System (BES) in North America. The CIP standards were initially approved by the Federal Energy Regulatory Commission (FERC) in 2008 to ensure appropriate security controls are in place to protect BES and its users and customers from all threats that may affect its timely and effective functioning.

There are thirteen standards in NERC CIP [20], each covering a particular type of control or capability to help build OT security programs.

Standard	Requirement
CIP-002: BES Cyber System Categorization	To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of security requirements
CIP-003: Security Management Controls	To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems
CIP-004: Personnel and Training	To require an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems
CIP-005: Electronic Security Perimeter(s)	To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP) in support of protecting BES Cyber Systems
CIP-006: Physical Security of BES Cyber Systems	To specify a physical security plan in support of protecting BES Cyber Systems
CIP-007: System Security Management	To manage system security by specifying select technical, operational, and procedural requirements
CIP-008: Incident Reporting and Response Planning	To specify incident response requirements to mitigate the risk to the reliable operations of the BES Cyber Systems
CIP-009: Recovery Plans for BES Cyber Systems	To specify recovery plan requirements in support of the continued stability, operability, and reliability of the BES Cyber Systems
CIP-010: Configuration Change Management and Vulnerability Assessments	To prevent and detect unauthorized changes to BES Cyber Systems
CIP-011: Information Protection	To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements
CIP-012: Communications between Control Centers	To protect the confidentiality and integrity of real-time assessment and real-time monitoring data transmitted between Control Centers.

CIP-013: Supply Chain Risk Management	Implement security controls for supply chain risk management to mitigate cybersecurity risks to the reliable operation of the BES Cyber System
CIP-014: Physical Security	To protect the physical assets of BES Cyber Systems

Figure 11 NERC CIP, Requirements per Standard

The NERC CIP compliance standards include many of the same common cybersecurity practices as other frameworks, such as NIST CSF or IEC 62443. However, they are more prescriptive and are enforceable by fines for non-compliance on the BES operators which are subject to them. Beyond the power utilities, which are the focus of NERC CIP, industrial organizations worldwide need to understand these standards and prepare for similar requirements in their industries. NERC frequently updates the CIP standards to address new risks, so utilities must stay agile. Emerging attack techniques like ransomware pose a growing menace to industrial control systems. While the CIP standards provide a strong foundation, continued vigilance and collaboration between public and private sectors is needed to enhance grid cybersecurity. Compliance with NERC CIP standards will remain crucial for securing operational technology and critical infrastructure from motivated, adaptive adversaries.

➢ TSA (Transportation and Security Administration) Directive (USA)

The TSA (Transportation and Security Administration) began issuing a series of Security Directives on cybersecurity for critical pipelines and LNG facilities in spring of 2021 following the high-profile cyberattack on Colonial Pipeline. These Directives apply to owners and operators of oil and gas pipelines, liquified natural gas (LNG) facilities, rail transit systems and the aviation sector as deemed "critical" by TSA. At a high level, they require owners and operators to develop and implement a cybersecurity incident response plan, complete a vulnerability assessment to identify potential risks in their systems and report security breaches to CISA within a specific timeframe.

The initial Security Directive, Security Directive-Pipeline-2021-01 [21], which went into effect on May 28, 2021, was the TSA's first set of mandatory cybersecurity rules for critical pipelines and LNG facilities. Previously, the agency had issued only nonbinding guidance, including its 2018 Pipeline Security Guidelines [22]. The TSA has since issued four additional Security Directives on pipeline and LNG facility cybersecurity and has provided notice to owners and operators it deems subject to these directives.

The directive was revised on 26th July 2023 with industry input, expanding requirements and focusing on performance-based measures. The new Security Directive Security Directive Pipeline 2021-02D [23], largely builds on its predecessor directive's flexible approach and adds more detailed requirements related to cybersecurity program testing, reporting, and documentation. The Security Directive became effective the day after it was issued. The TSA regulations outline four key objectives to safeguard critical infrastructure: separating OT and IT networks, securing access to critical systems, and implementing continuous monitoring for threats. To achieve these goals, operators must create a TSA-approved plan, develop a comprehensive incident response strategy, and establish a continuous program for assessing cybersecurity vulnerabilities.

TSA has incorporated elements of both the *CISA Cyber Performance Goals* and the *NIST CSF 2.0* into its security directives. Compliance with these directives necessitates substantial financial investments requiring pipeline owners and operators to allocate resources and upgrade their cybersecurity infrastructure, develop incident response plans, and train personnel to monitor and protect their systems, detect vulnerabilities, and swiftly respond to cyber incidents. Leading regulations like NIS2 (Europe) and TSA (USA) highlight five key practices for securing the

Industrial Control Systems (ICS): incident response planning, continuous network monitoring, building robust architectures, secure remote access, and risk-based vulnerability management.

- **IACS UR (Unified Requirements) E26 & E27 (International - Maritime)**

  In April 2022, the International Association of Classification Societies (IACS) released two new Unified Requirements (UR) E26 and E27, relating to cyber resilience on board marine vessels. These URs specify requirements focused on the capability to reduce the occurrence and mitigate the effects of cyber incidents due to cyberattacks (hereinafter referred to as “cyber resilience”). The aim of the two URs is to set a minimum set of requirements for cyber resilience capabilities that a newly built vessel is to be delivered with to support cyber-secure operations.

  - IACS UR E26 [24]– Cyber Resilience of Ships

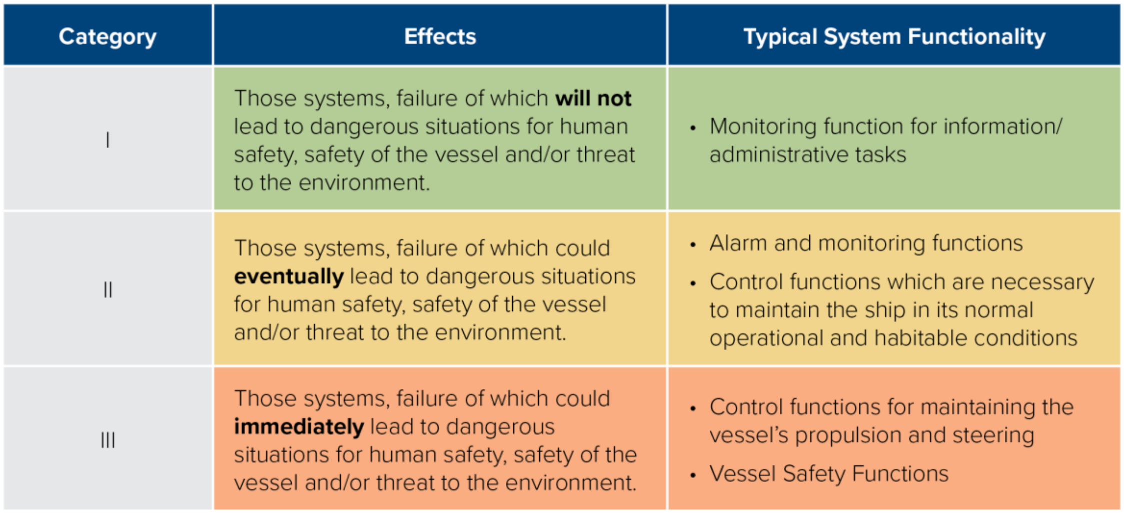
    UR E26 aims to ensure the secure integration of both Operational Technology (OT) and Information Technology (IT) equipment into the vessel’s network during the design, construction, commissioning, and operational life of the ship. This UR targets the ship as a collective entity for cyber resilience and covers five key aspects: equipment identification, protection, attack detection, response, and recovery. UR E26 includes 19 requirements that classification societies need to be aware of from design to operation depending on the stage of the ship’s lifecycle. Each stakeholder is responsible for meeting the predefined tasks per cyber requirement.

  - IACS UR E27 [25]– Cyber Resilience of On-Board Systems and Equipment

    UR E27 aims to ensure system integrity is secured and hardened by third-party equipment suppliers. This UR provides requirements for cyber resilience of onboard systems and equipment and provides additional requirements relating to the interface between users and computer-based systems onboard, as well as product design and development requirements for new devices before their implementation onboard ships.

The new unified requirements (UR) will be mandatory and uniformly implemented by IACS member societies on ships contracted for construction on or after 1 July 2024, complementing “UR E22 On Board Use and Application of Computer based systems”. Thus, the ship owners, designers, shipyards, integrators, and suppliers should expect new rules or guidelines from classification societies for conducting engineering reviews and surveys onboard vessels built after 1 July 2024. The new URs stand voluntary for existing fleets.

The foundation of the new requirements is based on the IMO’s RESOLUTION MSC.429(98)/Rev.1 [26] and guidance described in MSC-FAL.1/Circ.3/Rev.1 [27], including the five key functional aspects for cybersecurity: **Identify, Protect, Detect, Respond,** and **Recover**. Both requirements apply to all Computer Based Systems (CBS) on board vessels, including those that are not critical to safety, following the categorization included in the UR E22 [28], as shown in the table below.



Category	Effects	Typical System Functionality
I	Those systems, failure of which **will not** lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	• Monitoring function for information/ administrative tasks
II	Those systems, failure of which could **eventually** lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	• Alarm and monitoring functions • Control functions which are necessary to maintain the ship in its normal operational and habitable conditions
III	Those systems, failure of which could **immediately** lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	• Control functions for maintaining the vessel's propulsion and steering • Vessel Safety Functions

Figure 12 System Categories based UR E22, Source [29]

These regulations outline specific requirements that organizations must follow regarding the management and protection of their OT assets. Compliance with these measures is mandatory and failure to comply can result in penalties or loss of licensing. Assigning directives by regulatory bodies or industry-specific organizations also helps provide guidance on specific aspects of cybersecurity for OT environments. These measures serve as a roadmap for organizations to enhance their security posture and align their practices with industry best practices.

Standards are set by international organizations and industry consortiums to define best practices, frameworks, and technical specifications for securing OT environments. Standards such as *ISO 27001*, *IEC 62443*, *IEC 63452*, and *NIST SP 800-82* provide organizations with a structured approach to implementing security controls, risk management, and incident response processes in OT environments. Compliance with these standards helps organizations demonstrate their commitment to cybersecurity and provides a benchmark for measuring their security posture.

Looking ahead to 2024, the critical infrastructure sector needs further refining of its regulatory frameworks to address emerging challenges, adaptability to evolving threats, and foster a culture of cybersecurity resilience. Continued international cooperation remains vital, along with a focus on developing standardized practices to ensure interoperability and collective defense against cyber threats across international critical infrastructure sectors.

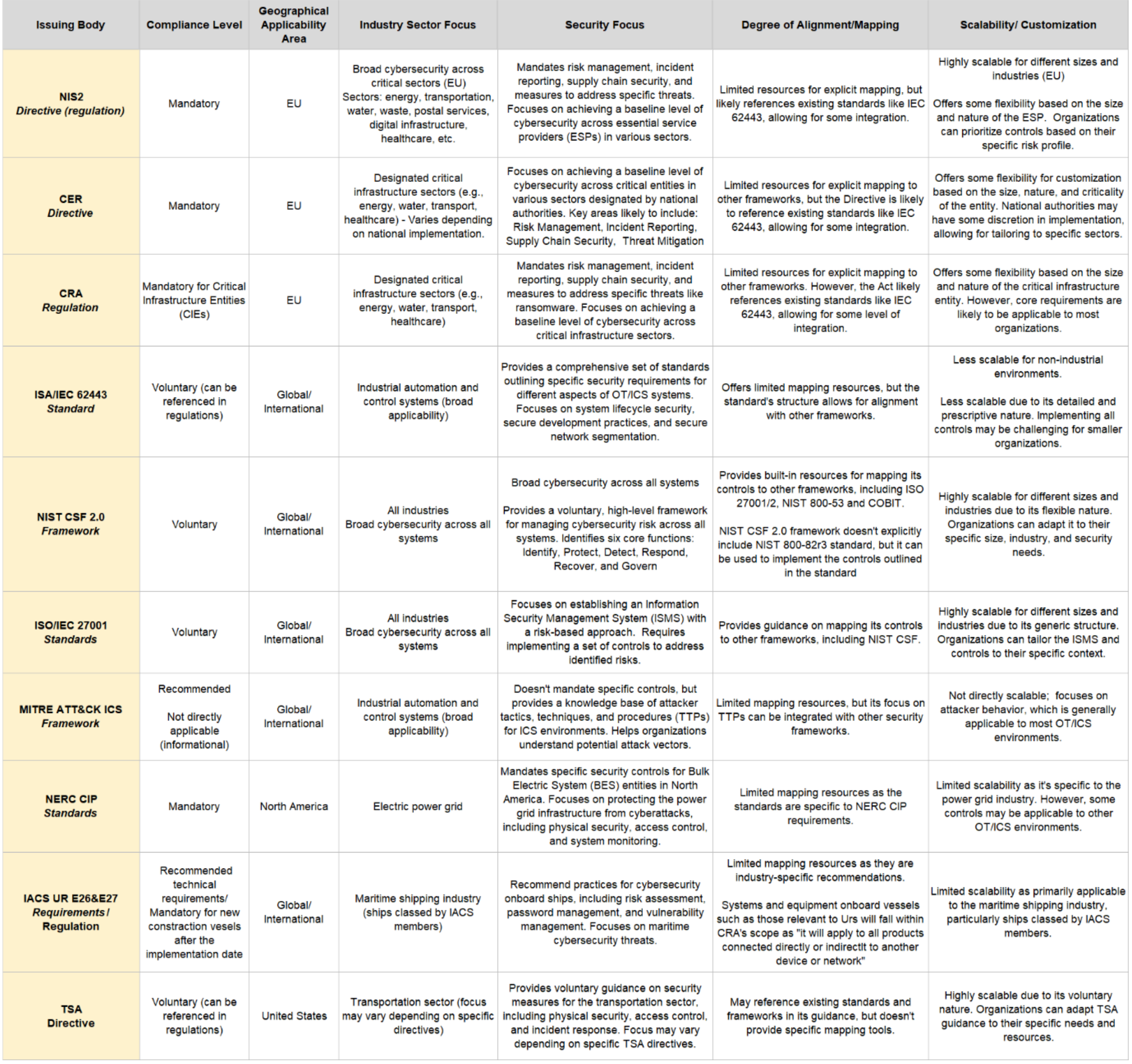
With every passing year, new cybersecurity legislation comes into force. Each set of guidelines or laws can be a large hurdle for organizations to overcome. At the same time, organizations are constantly having to keep up to date with the latest threats and technology in order to make sure their defenses against attacks and potential breaches are robust.

The consolidated table presented in Figure 13, compares the issuing bodies of regulations, frameworks, and standards referred to in this chapter, against some specific features (characteristics/metrics). The definitions of the chosen characteristics are articulated below:

1. **Compliance Level:** Mandatory, voluntary, or recommended adoption of the issuing body.
2. **Geographical Applicability Area**: In which geographical scope the issuing body applies.
3. **Industry Sector focus:** Whether the regulation/framework/standard applies to specific industries like power, water, manufacturing, etc.
4. **Security Focus:** Important security controls or compliance mandates stipulated by the issuing body. Main areas as outlined in the publication. This metric could be further broken down into

subcategories relevant to OT/ICS security, such as: physical security, network security, data security, incident response.

5. **Degree of Alignment/Mapping:** provides resources or guidance for mapping its controls to other frameworks.
6. **Scalability/Customization**: Evaluate the suitability of the regulation/framework for site's size and complexity, considering the potential need to scale the cybersecurity program in the future.



Issuing Body	Compliance Level	Geographical Applicability Area	Industry Sector Focus	Security Focus	Degree of Alignment/Mapping	Scalability/ Customization
NIS2 ***Directive (regulation)***	Mandatory	EU	Broad cybersecurity across critical sectors (EU) Sectors: energy, transportation, water, waste, postal services, digital infrastructure, healthcare, etc.	Mandates risk management, incident reporting, supply chain security, and measures to address specific threats. Focuses on achieving a baseline level of cybersecurity across essential service providers (ESPs) in various sectors.	Limited resources for explicit mapping, but likely references existing standards like IEC 62443, allowing for some integration.	Highly scalable for different sizes and industries (EU) Offers some flexibility based on the size and nature of the ESP. Organizations can prioritize controls based on their specific risk profile.
CER ***Directive***	Mandatory	EU	Designated critical infrastructure sectors (e.g., energy, water, transport, healthcare) - Varies depending on national implementation.	Focuses on achieving a baseline level of cybersecurity across critical entities in various sectors designated by national authorities. Key areas likely to include: Risk Management, Incident Reporting, Supply Chain Security, Threat Mitigation	Limited resources for explicit mapping to other frameworks, but the Directive is likely to reference existing standards like IEC 62443, allowing for some integration.	Offers some flexibility for customization based on the size, nature, and criticality of the entity. National authorities may have some discretion in implementation, allowing for tailoring to specific sectors.
CRA ***Regulation***	Mandatory for Critical Infrastructure Entities (CIEs)	EU	Designated critical infrastructure sectors (e.g., energy, water, transport, healthcare)	Mandates risk management, incident reporting, supply chain security, and measures to address specific threats like ransomware. Focuses on achieving a baseline level of cybersecurity across critical infrastructure sectors.	Limited resources for explicit mapping to other frameworks. However, the Act likely references existing standards like IEC 62443, allowing for some level of integration.	Offers some flexibility based on the size and nature of the critical infrastructure entity. However, core requirements are likely to be applicable to most organizations.
ISA/IEC 62443 ***Standard***	Voluntary (can be referenced in regulations)	Global/ International	Industrial automation and control systems (broad applicability)	Provides a comprehensive set of standards outlining specific security requirements for different aspects of OT/ICS systems. Focuses on system lifecycle security, secure development practices, and secure network segmentation.	Offers limited mapping resources, but the standard's structure allows for alignment with other frameworks.	Less scalable for non-industrial environments. Less scalable due to its detailed and prescriptive nature. Implementing all controls may be challenging for smaller organizations.
NIST CSF 2.0 ***Framework***	Voluntary	Global/ International	All industries Broad cybersecurity across all systems	Broad cybersecurity across all systems Provides a voluntary, high-level framework for managing cybersecurity risk across all systems. Identifies six core functions: Identify, Protect, Detect, Respond, Recover, and Govern	Provides built-in resources for mapping its controls to other frameworks, including ISO 27001/2, NIST 800-53 and COBIT. NIST CSF 2.0 framework doesn't explicitly include NIST 800-82r3 standard, but it can be used to implement the controls outlined in the standard	Highly scalable for different sizes and industries due to its flexible nature. Organizations can adapt it to their specific size, industry, and security needs.
ISO/IEC 27001 ***Standards***	Voluntary	Global/ International	All industries Broad cybersecurity across all systems	Focuses on establishing an Information Security Management System (ISMS) with a risk-based approach. Requires implementing a set of controls to address identified risks.	Provides guidance on mapping its controls to other frameworks, including NIST CSF.	Highly scalable for different sizes and industries due to its generic structure. Organizations can tailor the ISMS and controls to their specific context.
MITRE ATT&CK ICS ***Framework***	Recommended Not directly applicable (informational)	Global/ International	Industrial automation and control systems (broad applicability)	Doesn't mandate specific controls, but provides a knowledge base of attacker tactics, techniques, and procedures (TTPs) for ICS environments. Helps organizations understand potential attack vectors.	Limited mapping resources, but its focus on TTPs can be integrated with other security frameworks.	Not directly scalable; focuses on attacker behavior, which is generally applicable to most OT/ICS environments.
NERC CIP ***Standards***	Mandatory	North America	Electric power grid	Mandates specific security controls for Bulk Electric System (BES) entities in North America. Focuses on protecting the power grid infrastructure from cyberattacks, including physical security, access control, and system monitoring.	Limited mapping resources as the standards are specific to NERC CIP requirements.	Limited scalability as it's specific to the power grid industry. However, some controls may be applicable to other OT/ICS environments.
IACS UR E26&E27 ***Requirements /*** **Regulation**	Recommended technical requirements/ Mandatory for new constraction vesels after the implementation date	Global/ International	Maritime shipping industry (ships classed by IACS members)	Recommend practices for cybersecurity onboard ships, including risk assessment, password management, and vulnerability management. Focuses on maritime cybersecurity threats.	Limited mapping resources as they are industry-specific recommendations. Systems and equipment onboard vessels such as those relevant to Urs will fall within CRA's scope as "it will apply to all products connected directly or indirectlt to another device or network"	Limited scalability as primarily applicable to the maritime shipping industry, particularly ships classed by IACS members.
TSA **Directive**	Voluntary (can be referenced in regulations)	United States	Transportation sector (focus may vary depending on specific directives)	Provides voluntary guidance on security measures for the transportation sector, including physical security, access control, and incident response. Focus may vary depending on specific TSA directives.	May reference existing standards and frameworks in its guidance, but doesn't provide specific mapping tools.	Highly scalable due to its voluntary nature. Organizations can adapt TSA guidance to their specific needs and resources.

Figure 13 ICS Cybersecurity Issuing Bodies: A Feature Comparison

3.2 Cybersecurity Compliance Strategy

Mandatory compliance is required by national or international laws or regulations, whereas voluntary compliance is a set of standards to help organizations maintain secure systems. Despite compliance with regulatory requirements, companies may still face legal action and public scrutiny in the event of a data breach.

Government and cybersecurity experts collaborate to create voluntary frameworks, acting as best practice guides for businesses of all sizes. These frameworks outline common controls, fostering industry-wide consistency. Aligning cybersecurity hygiene with accepted frameworks increases the likelihood of meeting industry regulations. A well-structured compliance plan will help critical infrastructures maintain industry regulations and protect their networks from costly and destructive cyberattacks. By understanding diverse regulatory compliance requirements, the industrial sector can develop comprehensive and tailored strategies that align with their industry requirements and cybersecurity objectives.

Cybersecurity controls pertain to policies, procedures, technologies, and organizational practices that are designed to protect critical infrastructure from cyberattacks. These controls can be implemented at various layers of the infrastructure, from the physical security of IT and OT systems to the processes for identifying and responding to threats. The state of practice for cybersecurity controls in critical infrastructure is constantly evolving as new threats and technologies emerge. However, there are a few common practices that are widely used by organizations that operate critical infrastructure.

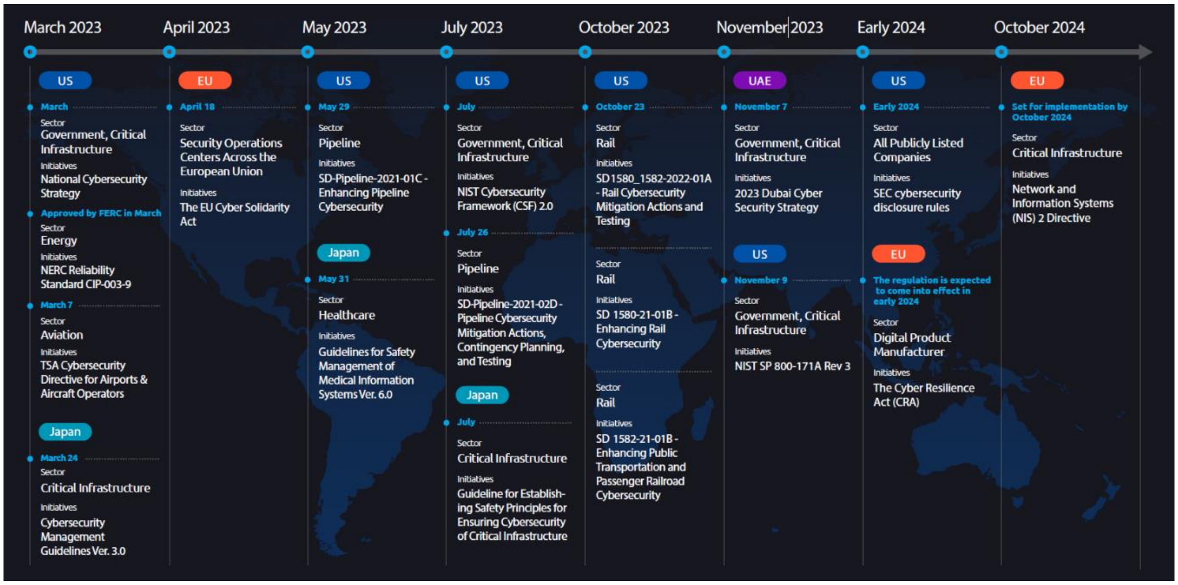
Just as the adage “prevention is better than cure” rings true in healthcare, it holds equal importance when addressing cybersecurity threats. Implementing a robust cybersecurity compliance program is a pivotal step for any organization aiming to safeguard itself from cyberattacks. Following the below nine key steps, the industry can effectively embark on the journey of compliance strategy.

Define Requirements	- Identify all relevant regulations and standards - Understand the specific requirements of each regulation
Data Protection	- Ensure encryption protocols are in place for data in transit and at rest - Implementing strong access control measures - Conduct regular backups of critical data
Risk Assessment	- Perform regular risk assessments - Identify vulnerabilities in the systems - Develop a plan to address and mitigate identified risks

Policies & Procedures	- Document all cybersecurity policies and procedures - Enforce policies and procedures align with relevant regulation requirements - Regularly update policies and procedures to reflect changes in regulations
Incident Response Plan	- Develop and document an incident response plan - Ensure the plan includes steps for identifying, containing, and recovering from a breach, as well as notifying affected parties - Regularly test and update the plan as needed
Training & Awareness	- Conduct regular cybersecurity training for employees, contractors, and stakeholders - Ensure the training covers company policies and compliance requirements - Update training materials regularly to address new threats and regulatory changes
Vendor Management	- Ensure that third-party vendors and partners also adhere to required cyber security standards - Embed clear compliance requirements into all vendor contracts - Conduct regular audits to verify adherence to compliance standards by vendors
Audit & Monitoring	- Establish regular monitoring of networks & systems to identify potential issues - Perform regular audits to ensure compliance with security standards - Maintain detailed records of all audit findings for future reference

Figure 14 Key steps for an industrial site to build a compliance strategy to adhere to regulations

Effective compliance programs should not be static documents but living, breathing entities. To maintain the effectiveness of the compliance program, it's crucial to be reviewed and updated regularly. This ensures that the program remains aligned with the latest regulations as the regulatory landscape shifts. In addition to these common practices for cybersecurity compliance, organizations should also adopt emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), Zero Trust Architecture (ZTA), Cloud Security, Supply Chain Security, to fortify their cybersecurity posture.



March 2023

US

March
Sector
Government, Critical Infrastructure
Initiatives
National Cybersecurity Strategy

Approved by FERC in March
Sector
Energy
Initiatives
NERC Reliability Standard CIP-003-9

March 7
Sector
Aviation
Initiatives
TSA Cybersecurity Directive for Airports & Aircraft Operators

Japan

March 24
Sector
Critical Infrastructure
Initiatives
Cybersecurity Management Guidelines Ver. 3.0

April 2023

EU

April 18
Sector
Security Operations Centers Across the European Union
Initiatives
The EU Cyber Solidarity Act

May 2023

US

May 29
Sector
Pipeline
Initiatives
SD-Pipeline-2021-01C - Enhancing Pipeline Cybersecurity

Japan

May 31
Sector
Healthcare
Initiatives
Guidelines for Safety Management of Medical Information Systems Ver. 6.0

July 2023

US

July
Sector
Government, Critical Infrastructure
Initiatives
NIST Cybersecurity Framework (CSF) 2.0

July 26
Sector
Pipeline
Initiatives
SD-Pipeline-2021-02D - Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing

Japan

July
Sector
Critical Infrastructure
Initiatives
Guideline for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure

October 2023

US

October 23
Sector
Rail
Initiatives
SD1580_1582-2022-01A - Rail Cybersecurity Mitigation Actions and Testing

Sector
Rail
Initiatives
SD 1580-21-01B - Enhancing Rail Cybersecurity

Sector
Rail
Initiatives
SD 1582-21-01B - Enhancing Public Transportation and Passenger Railroad Cybersecurity

November 2023

UAE

November 7
Sector
Government, Critical Infrastructure
Initiatives
2023 Dubai Cyber Security Strategy

US

November 9
Sector
Government, Critical Infrastructure
Initiatives
NIST SP 800-171A Rev 3

Early 2024

US

Early 2024
Sector
All Publicly Listed Companies
Initiatives
SEC cybersecurity disclosure rules

EU

The regulation is expected to come into effect in early 2024
Sector
Digital Product Manufacturer
Initiatives
The Cyber Resilience Act (CRA)

October 2024

EU

Set for implementation by October 2024
Sector
Critical Infrastructure
Initiatives
Network and Information Systems (NIS) 2 Directive

Figure 15 New Global Cybersecurity Initiatives for Critical Infrastructure, Source: TXOne [30]

4. Unveiling the Hidden Pathways of ICS cyberattacks

4.1 SANS Framework - ICS Cyber Kill Chain

An essential step in understanding cyber risk, and understanding how to manage that risk, lies in gaining some understanding of how cyberattacks work. Developed in 2011 by Lockheed Martin, the Cyber Kill Chain [31] model aids in identifying and responding to cyberattacks. Inspired by military kill chains, this widely adopted model assists security professionals in IT and enterprise networks by outlining the various stages of an attacker's intrusion process. Military Kill Chain Model: In military terminology, a kill chain is a phase-based model that classifies offensive activities based upon the stages of an attack and uses the deconstruction of the attack to prevent it.

The Cyber Kill Chain is a concept that represents the stages or steps involved in a cyberattack. It serves as a framework for understanding and analyzing the different phases of an attack, from the initial reconnaissance to the achievement of the attacker's objective. There are different variations of the Cyber Kill Chain, but commonly identified steps include:

1. **Reconnaissance:** The attacker gathers information about the target, such as its network infrastructure, vulnerabilities, and security posture.
2. **Weaponization:** The attacker creates or selects tools and exploits vulnerabilities identified during the reconnaissance phase.
3. **Delivery:** The attacker delivers the weaponized payload to the target system, often through phishing emails, malicious websites, or other means.
4. **Exploitation:** The attacker uses the payload to exploit further vulnerabilities and gain access to the target system.
5. **Installation:** The attacker installs malware or other malicious software on the target system to establish persistence and control.
6. **Command and Control (C2):** The attacker establishes communication channels with the compromised system to issue commands and exfiltrate data.
7. **Actions on Objective:** The attacker performs actions, such as stealing data, disrupting operations, or installing ransomware.
8. **Monetization:** The attacker might convert stolen data or compromised systems into financial gain or other benefits (a form of ransom or selling sensitive information on the dark web).

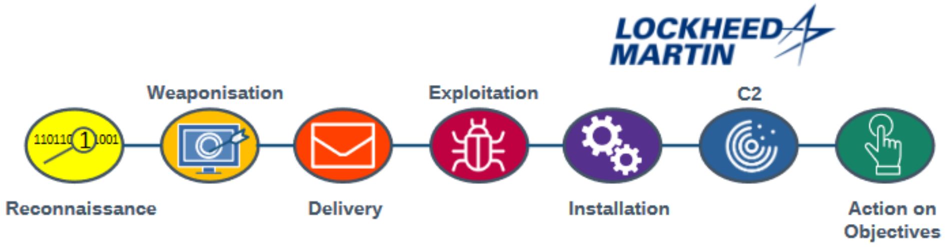


Figure 16 Cyber Kill Chain [32]

This Cyber Kill Chain does not equally represent the framework of the ICS customized cyberattacks, but it served as a valuable foundation on which Michael Assante and Robert M. Lee developed the ICS Cyber Kill Chain [33] in 2015. The ICS Cyber Kill Chain outlines the stages an attacker follows to execute a high-confidence attack against an ICS process. This framework aims to predict and control the potential for physical equipment damage.

The ICS Kill Chain diverges from its IT counterpart due to the Inherent features and sensitivities of ICS networks. Unlike conventional cyberattacks, skilled adversaries targeting ICS systems prioritize stealth and minimize disruptive actions during the initial stages. Active scanning and reconnaissance are less likely within the ICS environment, as attackers aim to avoid compromising their access or triggering alarms. Consequently, the ICS Kill Chain primarily focuses on describing targeted attacks and not unintended infections.

Sophisticated cyberattacks targeting ICS systems, aiming for substantial process or equipment disruption, necessitate attackers to acquire in-depth understanding of the automated processes, underlying engineering actions, and functional designs of the ICS and safety systems. This acquired knowledge empowers them to manipulate the systems and bypass or impair safety mechanisms, achieving a genuine cyber-physical attack with consequences beyond mere espionage, disruption, or intellectual property theft. To orchestrate such attacks, adversaries typically employ a two-stage approach, including several steps in each one of them.

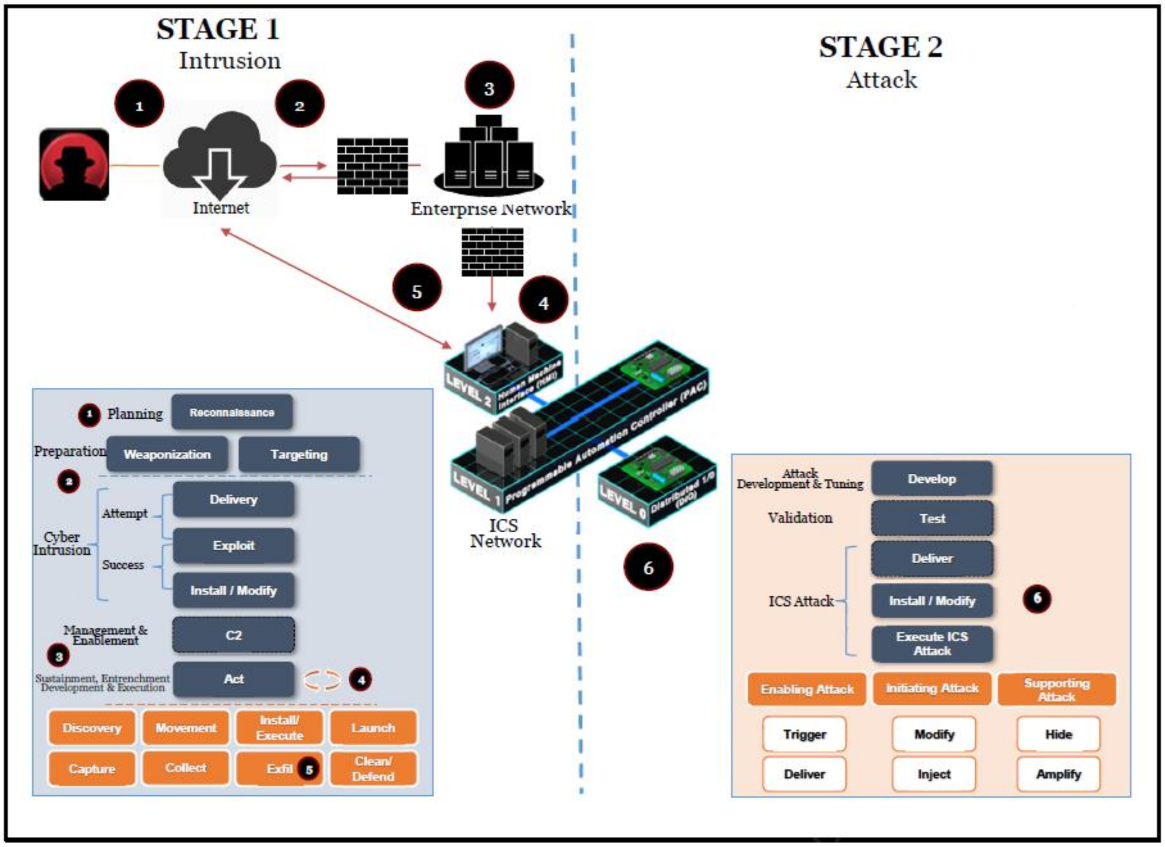


Figure 17 SANS Framework - ICS Cyber Kill Chain across the Purdue Model

The SANS ICS Cyber Kill Chain stands out from other frameworks by offering a high-level, two-stage perspective on attacker progression. Compared to MITRE ATT&CK for ICS, which provides a vast library of specific attacker tactics and techniques, the SANS model focuses on broader phases like reconnaissance and deployment. This simplicity aids in understanding the overall attack flow. Additionally, unlike the Diamond Model that emphasizes attacker capabilities like resources and infrastructure, the SANS framework concentrates on the attacker's actions within the ICS environment. By utilizing these different perspectives, security professionals can gain a well-rounded understanding of cyber threats and develop a more comprehensive defense strategy for their ICS systems.

The thesis focuses on breaking down and analyze the SANS ICS Cyber Kill Chain, a two-stage model outlining an attacker's progression, in the two following sections 4.1.1 and 4.1.2. It deconstructs each stage, revealing the adversary's tactics from initial reconnaissance to deployment and objective achievement. By comprehending these phases, defenders gain a strategic advantage for disrupting attacks and fortifying their ICS cybersecurity posture.

4.1.1 Stage 1

Research

Sophisticated adversaries prioritize extensive open-source intelligence gathering (OSINT) before initiating attacks. Social media, contract announcements, procurement orders, user forums, and other publicly available information that provide them with valuable insights of the target environments. Additionally, adversaries may establish dedicated test labs replicating expected equipment and configurations. This allows for pre-deployment malware testing against anticipated security solutions, such as specific antivirus and firewalls, maximizing attack efficacy. Furthermore, in-depth understanding of targeted ICS protocols and assets within a given environment becomes crucial for achieving desired effects. Targeted attacks require proportionally more extensive research and development efforts. It is essential to acknowledge that any internet-facing ICS asset is inherently vulnerable to reconnaissance and requires increased security measures.

1st Stage Delivery

Experienced adversaries in this stage favor established delivery tactics like phishing (or watering holes) campaigns or supply chain vulnerabilities to deploy their crafted attack modules. Whether the payload is malware or a remote access backdoor, effectiveness takes precedence over complexity. Skilled attackers meticulously tailor their approach, minimizing effort while maximizing impact.

Exploitation

Successful exploitation of vulnerabilities leads to proper infiltration that provides the establishment of a communication channel with the adversary, enabling further network accessibility. As previously noted, exploit sophistication is secondary to effectiveness within the target environment, although it is crucial for adversaries. Advanced adversaries use old exploits, obfuscated malware as well as zero-day exploits. While the 1st Stage Delivery focuses on reaching the target, the Exploitation phase prioritizes the attack module's successful execution. Supply chain backdoors are particularly dangerous as they combine the 1st Stage Delivery and Exploitation phase, shortening the Kill Chain and reducing detection opportunities for defenders.

C2

Sophisticated actors frequently implement redundant C2 channels to guarantee uninterrupted connectivity despite detection or removal. C2 communication does not always necessitate high-bandwidth, bidirectional connections. Secure networks, for instance, may utilize unidirectional path with extended transmission and execution times. Attackers frequently camouflage C2 within legitimate traffic or hijack existing channels (i.e., trusted VPN). In some cases, they may even physically implant communication bridges. Once established, attackers leverage this access to pursue their objectives. Understanding the outbound connections in the environment (such as odd DNS requests) is important when identifying a large set of adversaries who use the tactic of hosting random and obviously malicious C2 servers. However, advanced adversaries often use "neutral-space" C2 servers – distinct from their own infrastructure or IP address, to mask their activity and hinder attribution. Neutral-space C2 servers might be compromised vendor websites, universities, or ordinary looking websites. In this case it is also critical to identify the type of requests and data being sent out of the network. Examples of abnormal communications that could be rendered as suspicious are:

- traffic to a vendor's website might be normal for an industrial network originating from a specific vendor's component
- the type of data sent, such as small payloads and encoded data
- the HMI talking directly to this the website

Exfiltration

Successful infiltration grants adversaries' access to valuable data for attack customization. Encryption keys, network maps, project files, and historical datasets are all potential targets. Adversaries leverage established C2 servers to exfiltrate this information either directly or through temporary drop sites. Exfiltration methods range from obvious transfers like email, telnet, VNC or RDP to more subtle techniques like encrypted data streams, encoded DNS requests or HTTP GET commands. Understanding normal network behavior within their ICS environment empowers defenders to detect anomalies, as adversaries unfamiliar with the system are more susceptible to be discovered during this stage. While attackers often utilize compromised vendor websites or seemingly benign web pages as neutral-space C2 servers, analyzing the nature of outbound connections and transmitting data remains crucial. While traffic to specific vendors might be commonplace, unusual data payloads or communication directly from HMIs to unfamiliar destinations can signal malicious activity.

4.1.2 Stage 2

Tailored Capability

For adversaries aiming to induce physical disruptions or future infrastructure manipulation, exfiltrated data and network access alone are insufficient. Tailored capabilities are necessary for a predictable impact. While DoS attacks offer an uncertain approach in order to create a physical impact, highly specialized tactics, which targets a physical impact, limit its applicability to broader attack campaigns. The more tailored a capability, the more certain it is to have the desired impact, but the less likely it is to be useful against other targets. Consequently, adversaries conduct research and testing in isolated environments, minimizing detection risks.

2nd Stage Delivery

Delivery of the tailored attack module occurs via established C2 servers or methods mirroring the initial infiltration (1st Stage Delivery). However, a completely different attack vector might be employed to obfuscate the connection and avoid raising suspicion about the initial access point, thereby facilitating prolonged attacker persistence.

Impact

At this point, it is too late for the defender to counter the adversary. This stage is when the tailored capability has its desired impact. Likely, the tailored capability will not work perfectly regardless of the research because there are always unknown variables, even to the adversaries. While proactive defense is no longer an option, initiating an incident response procedure becomes paramount to ensure the safety of personnel and civilians. This response extends beyond the traditional domain of information security, encompassing all measures necessary to mitigate potential harm.

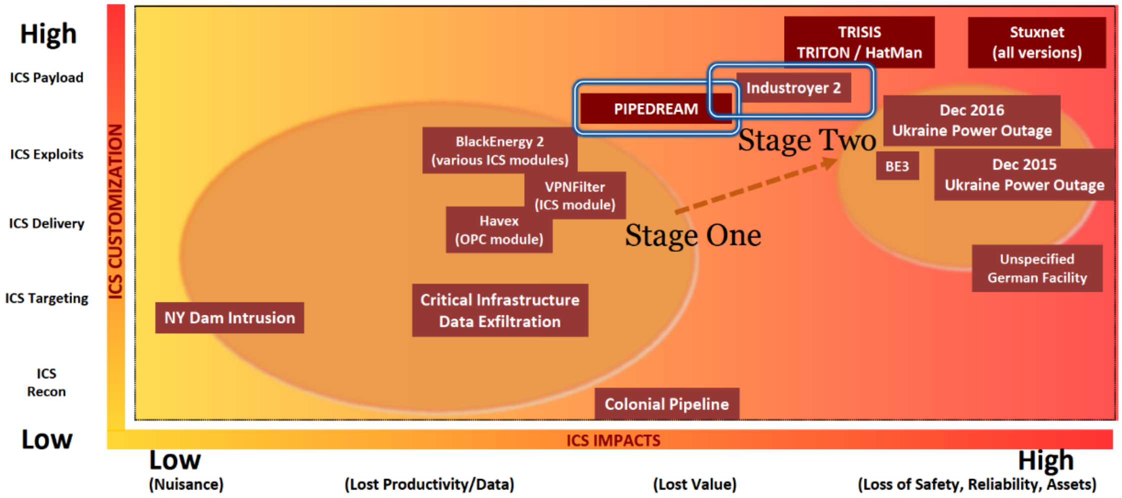


Figure 18 ICS Incidents and Access Campaigns - SANS ICS Summit 2023

4.2 “Living-of-the-Land” attack technique

ICS face a growing threat from Living-Off-the-Land (LotL) attacks. Living off the Land attacks are a post-infection technique, for network reconnaissance, lateral movement, and persistence. The ICS LotL attacks weaponize legitimate control system components, including engineering software, industrial protocols, authorized network access, and control system libraries, against themselves. This approach offers adversaries several advantages: lower deployment costs bypassing the need for additional malware, increased success rates by potentially causing significant operational disruptions or safety hazards, enhanced evasion capabilities, demands for swift response, and potential for immediate safety and engineering consequences.

ICS attackers increasingly leverage IT malware, often compromising IT business networks first, in order to access and exploit ICS networks. This stolen information, such as engineering project files (ladder logic), control network architecture diagrams, control system configuration files, facilitates targeted attacks within the control environment (ICS Cyber Kill Chain Stage 2).

Living-off-the-land (LotL) attacks leverage legitimate binaries (LoLBins) often signed by trusted vendors that are part of some built-in legitimate network administration tools such as: *wmic, certutil, ntdusil*, *psexec* and *PowerShell*, to bypass traditional detection, perform lateral movement and identification of high-value targets (“crown jewels”) within the victim's network. This enables attackers to exploit legitimate software and protocols within OT/ICS networks (Modbus, OPC-UA, Profinet, IEC 61850, and more) without deploying custom malware. Once remote access is established, attackers continue to leverage LotL tools to escalate privileges through native tools like Task Manager and manipulate system services (BitsAdmin, WMIC) for persistence. They then establish command and control channels (C2) using SSH or Rundll32 to maintain control and exfiltrate data in order to achieve malicious goals.

Living-off-the-land attacks in ICS can manifest through various means, including unauthorized access to Human-Machine Interfaces (HMIs) for manipulating control systems or exploiting Engineering Workstations (EWS) to reprogram Programmable Logic Controllers (PLCs) with malicious logic. LotL techniques have a documented history in ICS attacks, dating back to 2014.

The following real incidents, detailed in the next chapter Vb, exemplify this fileless cyberattack technique.

- ICS-tailored espionage malware, *Havex* (2013,2014) employed by a Russian APT (advanced persistent threat) group “Energetic Bear” or “Dragonfly” to conduct intelligence collection campaigns aimed at various organizations worldwide with a primary focus on the energy sector. It was designed explicitly to infiltrate industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems.

- Ukraine power distribution system attack (2015), where the Sandworm APT (advanced persistent threat) gained access by using *BlackEnergy3* malware, to an HMI of a power plant and then could remotely trip circuit breakers, causing a power outage.
- A disruptive malware, *Industroyer/Crashoverride* (2016) used by Sandworm APT, to target electric power grids in Ukraine.
- *Triton/Trisis* malware (2017), where the threat actor abused the engineering workstation (EWS) functionality, to reprogram PLCs by injecting malicious code through authorized communication channels. This malware targets SIS (Safety Instrumented Systems).
- Water treatment facility in Oldsmar Florida (2021) where an adversary gained access to the HMI and manipulated the chemical composition of the water, potentially reaching toxic levels.
- Russia's infamous Sandworm APT used living-off-the-land (LotL) techniques on deploying *Industroyer2* malware, to precipitate a power outage in a Ukrainian city (2022), coinciding with a barrage of missile strikes.
- *Incontroller/Pipedream* (2022) ,the seventh and most sophisticated ICS-specific malware was built to target machine automation devices.

A blend of traditional exploits and LotL techniques are highly anticipated, varying based on attacker objectives, environment, and security maturity. While addressing vulnerabilities remains crucial, prioritizing data integrity and developing comprehensive security programs are essential to combat the evolving threat of increasingly frequent and sophisticated LotL attacks in industrial environments.

4.2 Case Studies

A fundamental prerequisite for comprehending cyber risk management entails elucidating the mechanics of some notorious OT cyberattacks of history and their potential underlying malware. Leveraging the "ICS Cyber Kill Chain" framework outlined in the preceding chapter, cyberattacks targeting critical industrial environments typically progress through a defined sequence of stages.

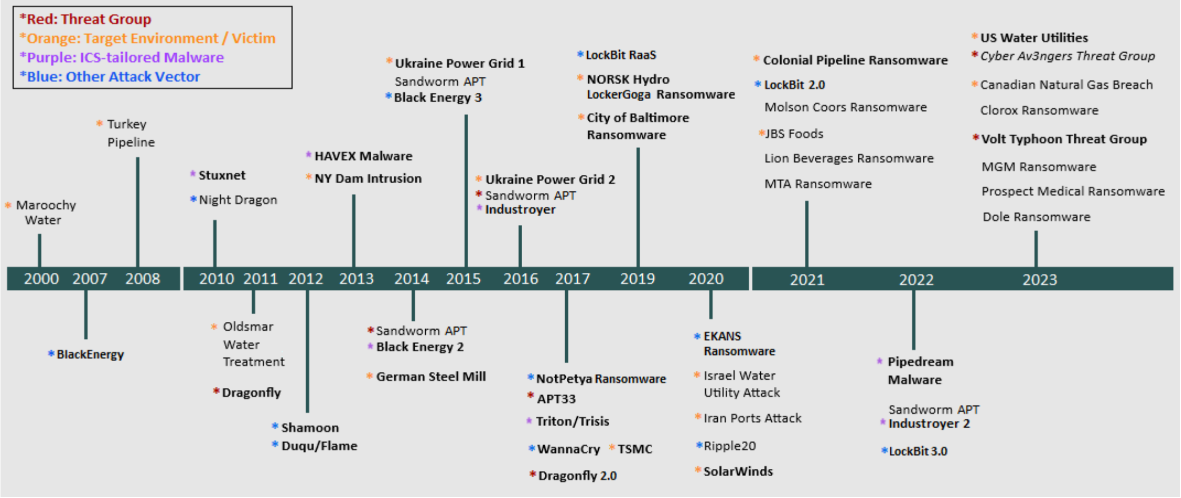


Figure 19 Timeline and History of ICS Cybersecurity Attacks (the most notorious in bold)

Advanced cyberattacks, including ransomware, often employ remote control mechanisms. Attackers issue commands to compromised devices from afar, observe the results, and repeat. This technique of leveraging compromised devices to attack other accessible machines is known as "pivoting." Ransomware groups, nation-state actors, and other sophisticated threats heavily rely on this approach for deeper infiltration and wider impact.

4.2.1 Ransomware Impacts Operations

Among the most prevalent and sophisticated threats of the present day are targeted ransomware attacks. Ransomware attacks can impact operations in one of the three below ways:

1. The attacks may reach all the way into OT networks and encrypt critical servers, thus shutting down industrial sites. For example, the *EKANS* ransomware, (also called "Snake" − spelled backwards) includes code that specifically targets OT networks and routinely shut down discrete manufacturing sites. EKANS ransomware is written in Golang and firstly appeared in mid-December 2019. It incorporates a static "kill list" to disable various antivirus and ICS processes, hindering potential defenses. Following this disruption, it deletes shadow copies, eliminating data restoration opportunities. Similar to several ransomware families, EKANS seeks to encrypt additional resources connected to the victim's machine across the network.
2. The attacks may impair only IT assets, but a victim organization may not be confident of the strength of their OT protections, and so decides to shut down physical operations out of "an abundance of caution".
3. The attacks may impair only IT systems, but physical operations rely on services provided by crippled IT systems and so they must shut down.

The Colonial Pipeline incident serves as a stark example of ransomware impacting physical operations of a critical infrastructure. This attack crippled America's largest gasoline pipeline, delivering 40% of the Northeast's supply, for six days. Public concerns over shortages led to panic, buying gas. Subsequent investigations, including CEO’s testimony, shed light on the attack’s sequence of events:

- Ransomware infected the IT network,
- The IT team notified the pipeline operations team,
- Within 50 minutes of being notified, the Operations Supervisor issued a stop work order to halt operations throughout the pipeline, out of concern that the malware might spread to operations.

The CEO testified that at the time of the shutdown, there was no evidence that the ransomware had penetrated the OT network, but the supervisor has the authority to stop the pipeline if he feels that safety is at risk. The pipeline was shut down according to standard operations procedure because the IT network was impaired, and the operator could not be confident of the pipeline’s safe operation in this state. However, established protocols granted the supervisor’s autonomy to halt operations if safety concerns arose.

Public reports on the attack highlight two potential disruption mechanisms: standard procedures mandated pipeline shutdown due to IT network compromise, and uncertainty regarding safe operations in this state. Unconfirmed reports claimed that physical operations depended on the IT-based custody transfer system (which tracks the movement of product through the pipeline). If those reports were accurate, then it would mean that, even if safety was not an issue, the pipeline could not have restarted until at least some of the IT-based systems were restored to normal functionality.

4.2.1.1 Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service (RaaS) lowers the barrier to entry for cybercriminals by providing pre-built ransomware infrastructure for rent. Developers profit through both rental fees and a share of the successful attacks, while affiliates avoid the cost and complexity of building their own tools.

The rapid growth of Initial Access Brokers (IABs) has facilitated ransomware attacks by providing easy network access for malicious actors. These individuals specialize in breaching victim networks and then selling access for as low as a few hundred dollars. This readily available network access, coupled with the availability of "Ransomware as a Service" (RaaS), significantly reduces the technical expertise required to launch ransomware attacks. This is evidenced by the correlation between increased inflows to IAB wallets and subsequent surges in ransomware payments. By monitoring IAB activity, potential attacks could be identified early, enabling timely intervention and mitigation efforts.

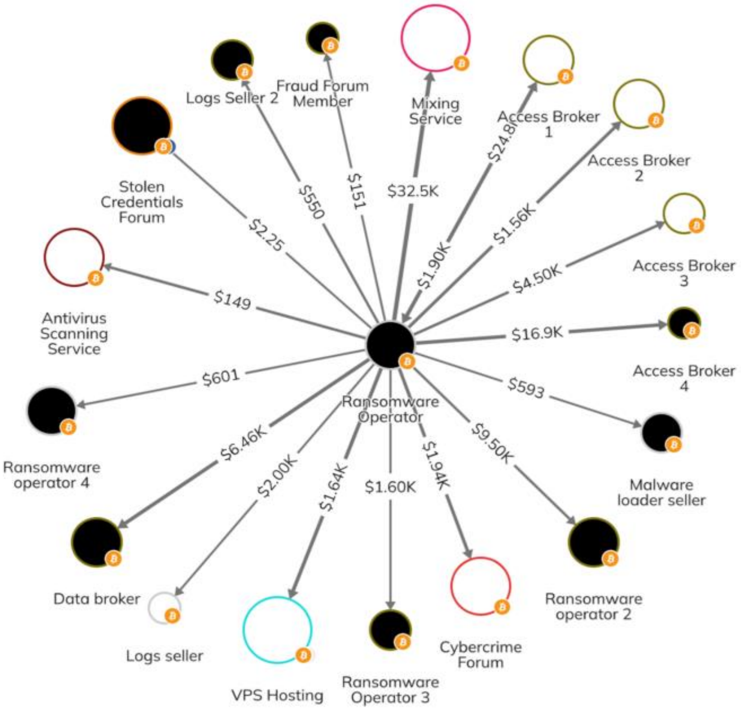


Figure 20 Ransomware actors have executed attacks that have brought in millions of dollars [34]

While post-compromise TTPs may differ slightly between ransomware groups and their affiliates, Living-off-the-Land (LotL) techniques remain prevalent.

The threat landscape of ransomware adversaries exhibits significant heterogeneity in technique and sophistication, impacting on a diverse array of industrial targets in 2023. Hundreds of active ransomware variants exist, including *LockBit, Alphv/BlackCat, Blackbasta, Royal, Cl0p, Hunters International, Rhysida, Akira,* and *NoEscape*. Rebranding and creating offshoot ransomware variants within the criminal ecosystem remain a widespread practice.

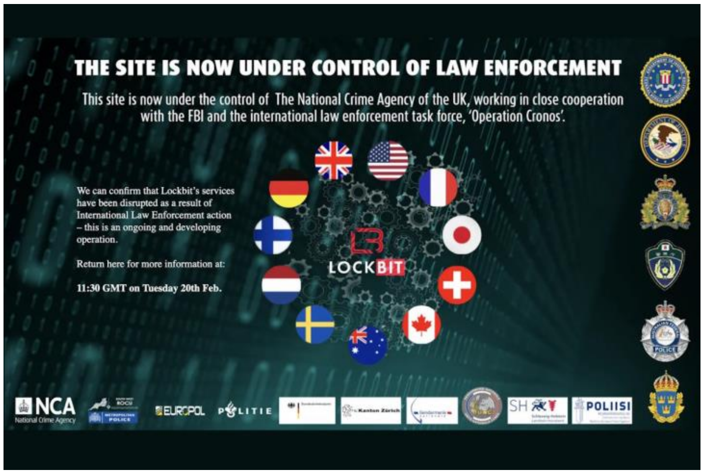
LockBit

LockBit ransomware was the most used and most prolific ransomware variant against industrial organizations. Specifically, LockBit operations accounted for 25% of the total ransomware incidents against industrial organizations in 2023, with *ALPHV* and *BlackBasta* accounting for 9% each. LockBit operates as a Ransomware-as-a-Service (RaaS) provider, with very few core members, creating its malware and running its website and infrastructure. This core group licenses its code to affiliates, who launch attacks against companies, steal their data, and try to extort money from them.

The operators of LockBit are predators who utilize extortion methods for the victim to be more likely to pay the ransom. StealBit, an information stealing tool in one of the tactics used to steal sensitive data, including ICS knowledge, from compromised systems. This stolen data serves as additional leverage, pressuring victim organization to pay ransom before data be encrypted by LockBit. In case the victim fails to pay, the exfiltrated data is uploaded to the LockBit’s dark web resources, which can be used by other threat actors.

LockBit operators capitalize on extortion tactics to increase the probability of the victim paying the ransom. One such tactic is stealing sensitive data, including industrial data from a victim organization, with *StealBit*, which is an information stealing tool created by the LockBit developers and typically deployed before LockBit encrypts compromised systems. If the victim doesn’t pay the ransom, the stolen data is posted to the LockBit dark web resources, which other adversaries can leverage.

For the last four years, the LockBit ransomware group has been on an unrelenting rampage. But LockBit’s hacking campaign has come to a juddering halt. A sweeping law enforcement operation, named "Operation Cronos" successfully infiltrated the notorious LockBit ransomware group. This operation, was led by the UK’s National Crime Agency (NCA) and was assisted by several law enforcement agencies around the globe, including Europol and the U.S. Federal Bureau of Investigation (FBI). Operation Cronos took control of LockBit's infrastructure and administration system, placing it offline. The operation seized and dismantled its dark web leak site, accessed its source code, seized around 11,000 domains and servers, and obtained details of the group's members. More than 200 cryptocurrency wallets linked to the group were seized. Also, within the gathered information there was company data from ransomware attacks where victims have paid a ransom to LockBit. “Even when a ransom is paid, it does not guarantee that data will be deleted, despite what the criminals have promised,” the NCA stated. Also, Operation Cronos obtained decryption keys for companies and organizations that have had their data locked but not paid to regain access. The dark web site, which LockBit used to publicly reveal the identities of victims refusing to pay a ransom for the release of their encrypted systems, was replaced with a law enforcement notice on Monday 19th February 2024, as shown in Figure 21.



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, ‘Operation Cronos’.

We can confirm that Lockbit’s services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

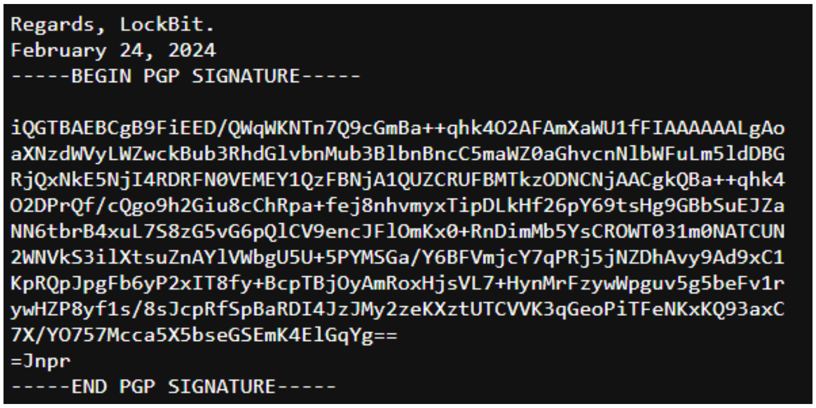
Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

Figure 21 A screenshot taken on February 19, 2024, shows a takedown notice that a group of global intelligence agencies issued to a dark web site called LockBit, Source: Reuters website [35]

A website associated with the LockBit ransomware operation appeared online on Saturday 24 February 2024, less than a week after the law enforcement operation. LockBit operators reportedly to be back up on the new infrastructure and with a new .onion address on the TOR network.

In the message (Figure 22) LockBit administrator listed more than two dozen servers they claim to contain victim's data, as well as, more than a dozen mirrors and half a dozen associated with the new leak site. Mocking the results of the Cronos operation, LockBit administrator claimed that the site was likely taken down exploiting a vulnerability [36] in the server software PHP that wasn't patched, due to "personal negligence and irresponsibility". The U.S State Department has offered up to 15$ million in rewards for information leading to the identification and/or arrest of LockBit leadership or people engaging in LockBit related activities.



```
Regards, LockBit.
February 24, 2024
-----BEGIN PGP SIGNATURE-----

iQGTBAEBCgB9FiEED/QWqWKNTn7Q9cGmBa++qhk4O2AFAmXaWU1fFIAAAAAALgAo
aXNzdWVyLWZwckBub3RhdGlvbnMub3BlbnBncC5maWZ0aGhvcnNlbWFuLm5ldDBG
RjQxNkE5NjI4RDRFN0VEMEY1QzFBNjA1QUZCRUFBMTkzODNCNjAACgkQBa++qhk4
O2DPrQf/cQgo9h2Giu8cChRpa+fej8nhvmyxTipDLkHf26pY69tsHg9GBbSuEJZa
NN6tbrB4xuL7S8zG5vG6pQlCV9encJFlOmKx0+RnDimMb5YsCROWT031m0NATCUN
2WNVkS3ilXtsuZnAYlVWbgU5U+5PYMSGa/Y6BFVmjcY7qPRj5jNZDhAvy9Ad9xC1
KpRQpJpgFb6yP2xIT8fy+BcpTBjOyAmRoxHjsVL7+HynMrFzywWpguv5g5beFv1r
ywHZP8yf1s/8sJcpRfSpBaRDI4JzJMy2zeKXztUTCVVK3qGeoPiTFeNKxKQ93axC
7X/YO757Mcca5X5bseGSEmK4ElGqYg==
=Jnpr
-----END PGP SIGNATURE-----
```

Figure 22 Message by LockBit administrators

According to Prodaft cybersecurity firm, within the course of three years, the number of LOCKBIT affiliates had increased to 194, some of which were tied to other notorious cybercrime groups, including EvilCorp, FIN7, and Wizard Spider.

The ransomware landscape in 2023 witnessed a marked shift towards greater efficiency and aggression. This was evidenced by the changing tactics and affiliations of threat actors, the rapid proliferation of RaaS strains, and the faster execution of attacks. The movement of affiliates underscored the dynamic nature of the ransomware underground and the ongoing pursuit of more lucrative extortion opportunities. Despite continued adaptation by threat actors to evolving regulations and law enforcement efforts, 2023 saw significant advancements in the fight against ransomware through collaborative efforts involving international law enforcement, affected organizations, cybersecurity experts, and blockchain intelligence. Great examples are the *Hive, Alphv/BlackCat*, and recently the *LockBit* disruption and takedown.

4.2.2 Supply Chain Attacks

In the case of OT environments, supply chain attacks present a higher risk due to the deep integration of third-party software and network interfaces within operational equipment. This reliance/dependency on using external components creates vulnerabilities that adversaries can exploit, infiltrate to the secure networks, and potentially build backdoors into the equipment.

Following a solidified OT security strategy, organizations must implement robust supply chain security measures within their OT environments. This requires a comprehensive mapping of external vendors with access to internal OT infrastructure. Critical to this process is defining access protocols and responsibilities for each vendor. Ongoing communication among all stakeholders in the supply chain fosters improved visibility and control over OT assets, minimizing potential vulnerabilities. Additionally, effective OT security necessitates a comprehensive asset inventory. This allows industrial organizations to visualize and understand the critical information and security posture of all devices within their network.

In 2017, the NotPetya malware, deployed by a Russian-backed group, infiltrated a Ukrainian tax software update, leading to widespread data loss and system disruptions. Notable victims included, the world's largest container shipping company**,** Maersk, experiencing a 6-day outage, and the pharmaceutical company Merck, securing a $1.4 billion settlement from its insurer. Four years later, in 2021, the *REvil* ransomware exploited a compromised cloud-based security update server at Kaseya (provider of IT and security management solutions for managed service providers -MSPs**)**, impacting 800 victims within 45 minutes. These incidents are examples of supply chain attacks. The "supply chain" term is deceiving, as it covers all the following different scenarios:

- Back doors may be deliberately inserted into software by vendors under the influence of hostile governments. For example: many western governments have banned Huawei and ZTE as suppliers of products or components for 5G wireless service because of concerns over back doors.
- Software vulnerabilities may exist in components which are then assembled into solutions and re-sold. Vulnerabilities are announced in a system's components. How can the high-level system vendors know about these vulnerabilities and act to evaluate and/or remediated them? How can end users be aware of how vulnerable their software is? Software Bill of Materials (SBOM) technologies are emerging to fill the gap.
- Malware may be stealthily inserted into otherwise-legitimate software products and services. Examples here include NotPetya, Kaseya and the SolarWinds Orion attacks. SolarWinds was a particularly advanced attack. A Russian-backed group was accused of inserting a RAT into the build process of the SolarWinds Orion product's security updates. Those compromised updates were later installed at up to 18K customer sites. It took over 6 months before the malware was discovered.

Supply chain attacks pose significant risks to OT and ICS, potentially leading to equipment damage, safety hazards for personnel and public, physical harm to manufacturing plants, operational downtime, and disruptions within the supply chain itself. Increased instances of such attacks within the industrial sector emphasize the criticality of prioritizing robust OT security and enhanced security practices.

4.2.3 ICS Espionage Malware

4.2.3.1 Havex *aka* Dragonfly (2013)

The Havex malware, a pre-existing Remote Access Trojan (RAT) primarily used for espionage, surprised the cybersecurity community when a variant specifically targeting Industrial ICS emerged. It was marked as the second known malware with ICS-specific capabilities and ignited concerns due to its suspected development by a well-funded, potentially nation-state actor aiming to gather intelligence from ICS networks. This capability could serve as a precursor to craft destructive malware similar to Stuxnet. Attributed to the Dragonfly threat group, Havex leveraged an industrial protocol scanner to identify vulnerable devices on TCP ports 44818 (Omron, Rockwell Automation), 102 (Siemens) and 502 (Schneider Electric).

The malware was further adapted for ICS environments by incorporating specialized code and modules. Publicly available information suggests the campaign spanned at least three years. Attackers employed various methods for initial infection, including, but not limited to, the following three prevalent techniques:

- Spear-phishing emails: Sending emails, disguised as legitimate communication, trick recipient into opening malicious attachments

- Watering hole attack: Attackers compromise vendors websites frequented by ICS personnel, infecting their systems with malware upon visiting the compromised site.
- Trojanized software installers: Attackers distribute ICS software installers that are trojanized with malware, which infects the system when executed by unsuspecting staff.

The varied methods used in this attack demonstrate the adaptability of adversaries, who employed diverse techniques of delivery for gaining access to systems. Notably, the observed tactics revealed the attackers' success in the planning phase, where they likely identified and exploited weaknesses, such as the trusting nature of engineers and the inherent reliance on the ICS supply chain.

Havex employs various methods to breach systems, aligning with different stages of the ICS Cyber Kill Chain, on **Stage 1**. The initial method involves spear phishing emails:

1. **Reconnaissance:** Attackers identify valuable targets and personalize emails.
2. **Weaponization:** A malicious file with an exploit is attached to the email.
3. **Delivery:** The targeted email containing the malicious attachment is sent.
4. **Exploitation:** Opening the attachment infects the system with Havex malware.
5. **Installation:** Havex communicates with a command and control (C2) server.
6. **Discovery & Exfiltration:** Havex scans the network, gathers information about ICS components, and sends it back to the C2 server.

This method primarily impacts the external network and might not reveal sensitive ICS details, unless engineering files are stored there. The second method, involving infected websites, employs different tactics in the initial stage (Stage 1) and likely follows a distinct ICS Cyber Kill Chain. The Havex intrusions reached Stage 2 with access to the ICS networks by the time the ICS port scanning and OPC scanning were taking place. That would qualify for the Develop phase of Stage2.

Lessons Learned

- ✓ Solid website architecture could have shut down the campaign's most impactful phase (watering hole attacks).
- ✓ No zero-day exploits were used, just repurposed Metasploit modules with known patches. However, if the victims that were infected from the initial websites understood their network traffic enough to tune and maintain passive defenses (whitelists, identify suspicious DNS lookups) , they would have identified the infections early and we'd have a lot more information about a not-as-successful campaign.
- ✓ Alert network monitoring by victims would have revealed unusual activity like OPC scans, systems calls, suspicious DNS lookups, and C2 server connections that were connected from OT network to the active Internet.
- ✓ Active defense could have neutralized Havex's capability to steal data, by sinkholing C2 servers. Network Security Monitoring (NSM) would have identified the malware. Incident Response would have identified and cleaned up the initial infection points.
- ✓ Moreover, sharing threat intelligence throughout the community with IoCs could have minimized the scope of the attack. The key takeaway is not to criticize targeted industries, but to learn and implement these practical defensive measures.

4.2.3.2 BlackEnergy 2&3 (2014-2015)

BlackEnergy2 (BE2) was originally served as a common malware framework used for DoS attacks by various threat actors . It was later modified by an APT group to target ICS. The BE2 exploited internet connected HMI from various vendors, enabling remote access to a core system in ICS environment. This allowed attackers to understand the industrial process and gain a visual representation of the ICS environment. Beyond HAVEX's capabilities, BE2 further advanced by exploiting vulnerabilities in specific ICS equipment to gain direct access.

It was initially designed for broader purposes and was adapted to target a diverse range of industries across Europe, the US, and the Middle East. Subsequently, an enhanced version, BlackEnergy3 (BE3), played a pivotal role in the first cyberattack-induced power outages. In 2015, attackers used BE3 to breach the enterprise networks of Ukrainian power companies. Pivoting and gaining access to control center ICS networks, they manipulated distribution management systems to manually trigger a disruptive power outage and delay restoration.

It was used to target a wide range of industries in Europe, US, and the Middle East. A further upgraded version called BlackEnergy 3 (BE3) was used to gain access to the enterprise networks of multiple power companies in Ukraine in 2015. From there, the adversaries pivoted into the ICS network of the control centers and after learning how to leverage the distribution management systems to manually manipulate electric utility operations and produce an outage, caused a disruptive attack followed by a delay of recovery. This is an example of an existing malware being repurposed and extended to target ICS that resulted in the first cyber-attack-caused power outages.

Crucially, neither BlackEnergy2 nor BlackEnergy3 possessed direct attack capabilities. They functioned as espionage tools, enabling adversaries to gain access and understanding, but not directly causing the outage. BE2 and BE3 could technically be used to get access directly into the ICS, especially BE2, and thus represent the start of the Develop phase of an ICS attack. Nonetheless, their ability to facilitate ICS infiltration demonstrates the crucial need for robust security measures in this domain.

BlackEnergy 2 (B2)

1. **Reconnaissance:** BlackEnergy 2 attacks often begin with broad reconnaissance techniques. Attackers might scan target networks for vulnerabilities, exploit publicly known weaknesses in ICS software, or even launch phishing campaigns to gain initial access credentials.
2. **Weaponization:** Unlike Stuxnet, BlackEnergy 2 itself isn't specifically designed for ICS attacks. However, attackers can leverage its modular architecture. They might develop or acquire custom plugins for BlackEnergy 2 that specifically target vulnerabilities in ICS components or exploit protocols used for communication within the control network.
3. **Delivery:** BlackEnergy 2 can be delivered through various methods, including phishing emails with malicious attachments, watering hole attacks compromising legitimate websites, or exploiting vulnerabilities in remote access software.
4. **Installation:** Once a system is compromised, BlackEnergy 2 can establish persistence and spread laterally within the network. It might exploit vulnerabilities in operating systems or leverage legitimate administrative tools to move undetected.
5. **Command and Control (C2):** BlackEnergy 2 communicates with attacker-controlled servers to receive instructions and upload stolen data. This C2 infrastructure allows attackers to remotely control infected systems and potentially launch further attacks.

BlackEnergy 3 (BE3)

1. **Reconnaissance:** Similar to BlackEnergy 2, BlackEnergy 3 attacks often rely on broad reconnaissance techniques. Attackers might leverage automated scanners to identify vulnerable systems, exploit known weaknesses in ICS software, or launch phishing campaigns with malicious attachments or links to steal initial access credentials.
2. **Weaponization:** BlackEnergy 3 builds upon its predecessor's modularity. Attackers can develop or acquire even more sophisticated custom plugins specifically designed to target vulnerabilities

in ICS components or communication protocols within the control network. These plugins might allow attackers to gain deeper access to critical systems and gather more detailed information about the ICS environment.

3. **Delivery:** BlackEnergy 3 likely utilizes similar delivery methods as BlackEnergy 2, including phishing emails, watering hole attacks, and exploitation of remote access software vulnerabilities.
4. **Installation:** Once a system is compromised, BlackEnergy 3 can establish persistence and spread laterally within the network. It might exploit operating system vulnerabilities or leverage legitimate administrative tools to remain undetected.
5. **Command and Control (C2):** BlackEnergy 3 likely maintains communication with attacker-controlled servers using similar C2 infrastructure as BlackEnergy 2. This allows attackers to receive instructions, upload stolen data, and potentially launch further attacks.

4.2.4 ICS Disruptive & Destructive Malware

4.2.4.1 Stuxnet (2010)

It was the first ICS malware found in the wild, when it was targeting the centrifuges in Iranian nuclear facilities, with the goal of inflicting physical damage by altering their rotation speed. The Stuxnet malware appears to have destroyed roughly 100 gas centrifuges at the Natanz facility, in Iran's uranium enrichment program.

The origins of the notorious Stuxnet malware remain unconfirmed. However, a theory stands that an Israeli agent used USB drives to plant the virus into the facilities. The Stuxnet malware leveraged four "zero-day" vulnerabilities to propagate, infecting USB drives or other removable storage devices that were subsequently connected to the infected machine. USB keys facilitated inter-site transmission, within an infected network, aggressively spread across firewalls, demonstrating significant lateral movement capabilities once it had a foothold on the IT network. The malware includes a rootkit, which is software designed to hide the fact that a computer has been compromised. Once the machine is infected, a Trojan identifies if the computer is running with Siemens' Simatic WinCC software. The malware then automatically uses a default password that is hardcoded into the software to access the control system's Microsoft SQL database.

The malware was extremely sophisticated and appeared to have embodied a deep knowledge of the structure of the site it targeted. The malware included mechanisms to disable or avoid specific anti-virus and other security products, it also included mechanisms to identify specific industrial equipment and configurations that were unique to the uranium enrichment site. The worm included code to mask its effects - the only thing that Iranian operators saw while their centrifuges where disintegrating was green lights on their HMIs.

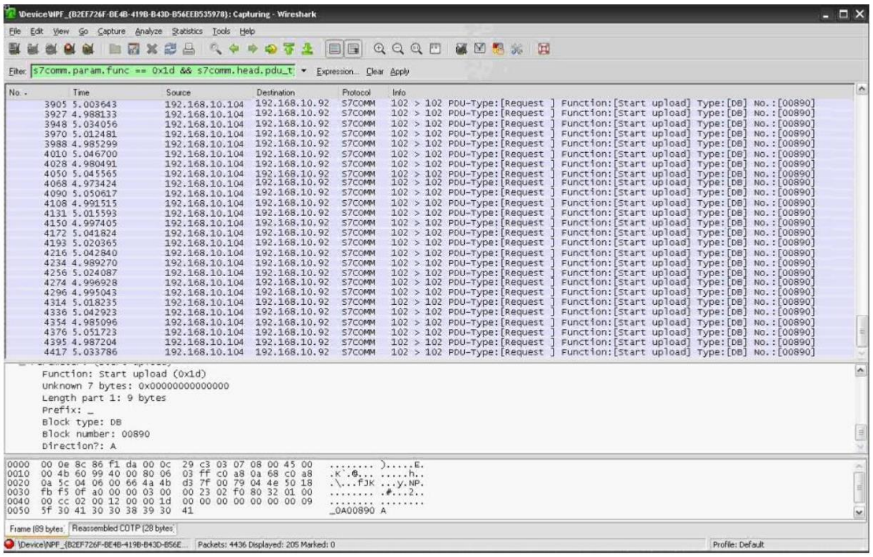
Stuxnet was discovered in 2010, however, it was a campaign likely unfolded over several year, with estimates placing its origins between 2006 and 2007. This extended period suggests significant pre-attack efforts by the attackers, aiming to create a highly targeted attack capable of physical destruction of specific centrifuges. This intelligence-gathering phase aligns with Stage 1 of the ICS Cyber Kill Chain, likely involving reconnaissance to identify potential entry points into the Natanz facility. Experts suspect that physical reconnaissance might have also played a role in acquiring such detailed knowledge about the facility layout and operations. It is crucial to consider the influence of both physical and digital aspects, along with the broader geopolitical context. For example, the Iranian uranium enrichment program at Natanz was a global concern, and its purpose and location were publicly disclosed by a dissident group in 2006. This, along with other non-cyber information, likely provided valuable insights for the attacker's planning and reconnaissance activities. In the weaponization phase, the malware code, combined with exploits, was likely placed on an infected engineering laptop or removable media device. This infected device then served as the delivery mechanism, introducing the exploit and malware into the Natanz network. Stuxnet, once installed on various Windows systems, replicated this exploit-and-install process, compromising additional systems until it could establish internet access and communicate with the attackers’ command and control (C2) servers.

The attack was designed to self-replicate and spread throughout the network until reaching specific targets. These targets were WinCC SIMATIC servers connected to particular Siemens controllers under specific conditions. Once these targets were compromised, Stuxnet entered the "Execute ICS Attack" phase (refer to Figure 17, Stage 2) and manipulated the centrifuges' rotational speed function, causing their physical destruction.

1. **Reconnaissance:** Attackers likely gained initial access through a combination of techniques, potentially including spear phishing emails, exploiting vulnerabilities in software used at the facility, or compromising a USB drive used by personnel.
2. **Weaponization:** Attackers developed the Stuxnet worm specifically tailored to exploit vulnerabilities in Siemens S7 PLCs (Programmable Logic Controllers) used to control Iranian centrifuges.
3. **Delivery:** The Stuxnet worm likely spread through removable media (USB drives) or compromised network connections.
4. **Installation:** Once on a system, Stuxnet exploited vulnerabilities in Windows operating systems to install itself and propagate further within the network.
5. **Command and Control (C2):** Stuxnet communicated with remote servers (C2 infrastructure) to receive instructions and potentially upload stolen data.
6. **Exploitation:** Having reached the control network, Stuxnet targeted specific Siemens PLCs. It manipulated control logic and sensor data to disrupt centrifuge operation, causing them to spin at excessive speeds and self-destruct.
7. **Impact:** The attack caused significant damage to Iranian centrifuges, hindering their nuclear program.

Lessons Learned

✓ *Visibility and Monitoring: Wireshark Capture of Stuxnet Infected WinCC Server*


\Device\NPF_{B2EF726F-BE4B-419B-B43D-B56EEB535978}: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Tools Help
Expression... Clear Apply
Frame (89 bytes)
Reassembled COTP (28 bytes)
\Device\NPF_{B2EF726F-BE4B-419B-B43D-B56E...
Profile: Default

Filter: s7comm.param.func == 0x1d && s7comm.head.pdu_t

```
No. -   Time      Source          Destination    Protocol Info
   3905 5.003643  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   3927 4.988133  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   3948 5.034056  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   3970 5.012481  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   3988 4.985299  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4010 5.046700  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4028 4.980491  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4050 5.045565  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4068 4.973424  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4090 5.050617  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4108 4.991515  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4131 5.015593  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4150 4.997405  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4172 5.041824  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4193 5.020365  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4216 5.042840  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4234 4.989270  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4256 5.024087  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4274 4.996928  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4296 4.995043  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4314 5.018235  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4336 5.042923  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4354 4.985096  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4376 5.051723  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4395 4.987204  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
   4417 5.033786  192.168.10.104  192.168.10.92  S7COMM   102 > 102 PDU-Type:[Request ] Function:[Start upload] Type:[DB] No.:[00890]
```

```
      Function: Start upload (0x1d)
      Unknown 7 bytes: 0x00000000000000
      Length part 1: 9 bytes
      Prefix: _
      Block type: DB
      Block number: 00890
      Direction?: A
```

```
0000   00 0e 8c 86 f1 da 00 0c  29 c3 03 07 08 00 45 00   ........ ).....E.
0010   00 4b 60 99 40 00 80 06  03 ff c0 a8 0a 68 c0 a8   .K`.@... .....h..
0020   0a 5c 04 06 00 66 4a 4b  d3 7f 00 79 04 4e 50 18   .\...fJK ...y.NP.
0030   fb f5 0f a0 00 00 03 00  00 23 02 f0 80 32 01 00   ........ .#...2..
0040   00 cc 02 00 12 00 00 1d  00 00 00 00 00 00 00 09   ........ ........
0050   5f 30 41 30 30 38 39 30  41                        _0A00890 A
```

Packets: 4436 Displayed: 205 Marked: 0

Figure 23 Source: Langner's Report To Kill a Centrifuge [37]

The Langner's group report leveraged Wireshark to analyze WinCC/PLC network traffic during the Stuxnet attack, revealing suspicious activity such as constant polling to the PLC indicating an abuse or an infection's presence**.** The report stated: "A Stuxnet-infected WinCC system probes controllers every five seconds for data outside the legitimate control blocks; data that was injected by Stuxnet". This highlights the importance of NSM personnel routinely performing deeper traffic analysis, beyond relying solely on IDS alerts. Such analysis can flag potential intrusions for further investigation by the incident response teams.

Understanding normal network traffic patterns is crucial for detecting anomalies. This underlines the importance of comprehensive asset identification and network traffic analysis, as well as investing in well-trained analysts alongside powerful tools.

Furthermore, analyzing normal interactions can inform the creation of detection rules that trigger alerts when specific thresholds are breached, reducing the reliance on constant manual traffic monitoring by analysts, while still advocating for regular inspections.

✓ *Threat and Environment Manipulation*: Captured network traffic, project files, and other forensic data could have been shared with threat analysis and environment manipulation teams to facilitate identification, extraction, and comprehension of the Stuxnet malware. This collaborative effort could have yielded Indicators of Compromise (IoCs) integrated into internal threat intelligence systems for enhanced network security monitoring and incident response. Additionally, insights gained from analyzing the threat could have modified the environment that potentially would have mitigated the effectiveness of Stuxnet.

✓ *Threat Intelligence*: While comprehensive threat intelligence might not have prevented an exceptionally targeted and well-funded unique attack like Stuxnet, its value emerged post-incident. Identifying vulnerabilities in Windows systems and Siemens controller functionalities, exposed by Stuxnet, enabled other organizations to develop IDS signatures and enhance NSM capabilities for Stuxnet detection and mitigation. Moreover, the attack revealed valuable TTPs utilized by the attackers. This knowledge, beyond mere indicators, empowered incident response teams worldwide, particularly those facing attacks leveraging Siemens' VPN and other compromised sites.

4.2.4.2 Industroyer/Crashoverride (2016)

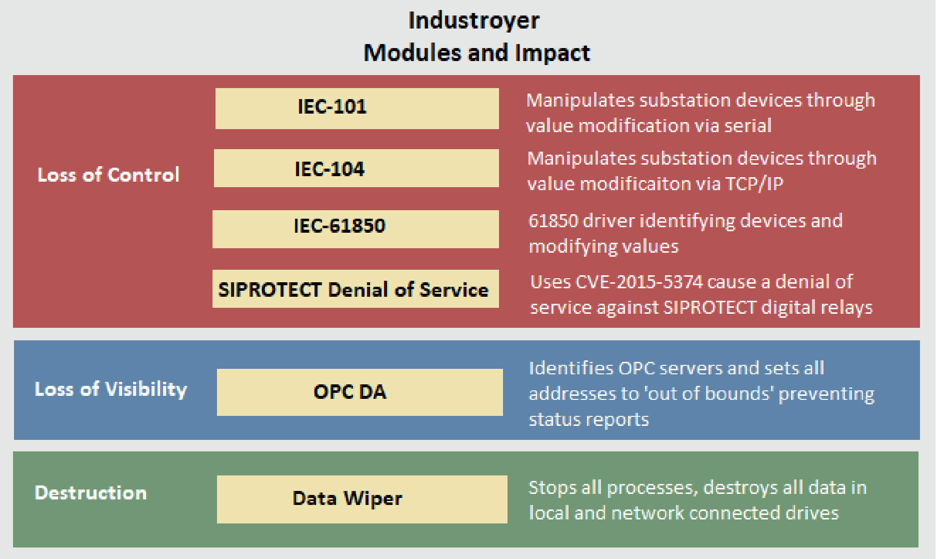
It was used in December 2016 by the Sandworm APT group to cut power in Ukraine. Industroyer was the fourth piece of ICS-tailored malware and the first known malware to cause disruptive effects to a power grid by interacting directly with a transmission substation. A power grid is a complex web of highways carrying electricity. Substations act as control centers (generation-transmission-distribution), and within them, protection relays play a vital role. These guardians of the grid constantly monitor the electrical current and trigger circuit breakers in case of anomalies. These crucial components safeguard against power outages, equipment damage, and even safety hazards.

Unlike BlackEnergy2, which was primarily focused on establishing a foothold within ICS environments and exploring its processes, the Industroyer malware differed significantly. Its objective was to cause physical damage by automatically disrupting electric grid operations, eliminating the need for direct attacker intervention. This malicious intent was manifested through its ability to communicate with targeted equipment using specialized ICS protocols and directly interact with grid components. This malware isn't picky about its target vendor and doesn't need weaknesses to work. It's like a clever thief who uses the built-in features of a house to break in, showing how attackers can weaponize normal, native functions for malicious purposes.

Industroyer can communicate seamlessly using standard ICS protocols like IEC104, IEC61850, and OPC. This allows it to issue targeted commands to manipulate critical processes state while bypassing operator's control. For example, it could force a circuit breaker open and prevent it from closing, even if the operator attempts to do so. The combination of modules (IEC104, IEC61850, OPC) though, allow the malware to be scalable across any electric grid using these protocols in Europe, Middle East, Asia, and if needed its would require only slight tailoring to include DNP3 to allow the malware to work in the US and the rest of the world. The SIPROTECT vulnerability was not required for the attack to work but could have had physical impacts if the protection equipment, a digital relay in this case, was no longer functioning when electric operators reconnected the equipment. However, no physical damage took place during this attack, only power disruption.

Industroyer had a modular framework consisting of an initial backdoor, a loader module, and various payload modules. A module within the payload, designated "104," leveraged the IEC 104 protocol to establish communication and control over industrial equipment. The 104 module was a dynamic link library (DLL) executed via a function named "CRASH". Its primary purpose was to send commands to remote terminal units (RTUs) and alter the state of critical data values (IOA). *IOA (Information Object Address) is a unique address assigned to an input or output at a substation. An IOA could point to a physical breaker device.* Industroyer effectively sent IEC104 commands by assuming a master position after being installed on an HMI. Then repeatedly sent open commands through the digital relay to the RTU to force open, and keep open, circuit breakers, thus de-energizing the equipment. The threat group responsible for the Industroyer capability was able to pivot from data historians, SQL servers of the IT to the OT network, and plant the malware.

Certain Industroyer payloads aimed to disrupt operations by triggering DoS attacks on targeted power grids' protection relays and remote terminal units (RTUs), effectively acting as a kill switch. In particular, one such payload targeted Siemens SIPROTEC 4 protection relays (*CVE-2015-5374)* by exploiting a vulnerability in the Digsi 4 communication protocol on UDP port 50000. It is worth noting that Siemens issued an advisory detailing workarounds and mitigations for this vulnerability. Additionally, newer SIPROTEC 5 relays feature improved security measures, including encrypted communication protocols.



Industroyer
Modules and Impact

Loss of Control	IEC-101	Manipulates substation devices through value modification via serial
	IEC-104	Manipulates substation devices through value modificaiton via TCP/IP
	IEC-61850	61850 driver identifying devices and modifying values
	SIPROTECT Denial of Service	Uses CVE-2015-5374 cause a denial of service against SIPROTECT digital relays
Loss of Visibility	OPC DA	Identifies OPC servers and sets all addresses to 'out of bounds' preventing status reports
Destruction	Data Wiper	Stops all processes, destroys all data in local and network connected drives

Figure 24 Industroyer modules and impact

1. **Reconnaissance:** Attackers likely conducted extensive reconnaissance to gain a deep understanding of the Ukrainian power grid's architecture and communication protocols. This might have involved techniques like scanning for vulnerabilities in network devices, analyzing publicly available information, or potentially even compromising internal systems for more granular intelligence.
2. **Weaponization:** Unlike BlackEnergy 2, Industroyer/CrashOverride wasn't a general-purpose malware platform. It was a custom-built malware specifically designed to target Industrial Ethernet protocols used by Ukrainian power grid equipment. This targeted approach demonstrates a high level of sophistication and preparation by the attackers.
3. **Delivery:** The exact delivery method for Industroyer/CrashOverride remains unclear. However, some theories suggest it might have been delivered through compromised workstations, removable media (USB drives), or targeted watering hole attacks aimed at personnel with access to critical systems.
4. **Installation:** Once delivered, Industroyer/CrashOverride exploited vulnerabilities in specific software or communication protocols to gain a foothold on targeted systems within the control network.
5. **Command and Control (C2):** There's limited information about the C2 infrastructure used by Industroyer/CrashOverride. However, it's likely the malware communicated with attacker-controlled servers to receive instructions and potentially confirm successful execution of the attack.

Lessons Learned

Securing critical ICS hardware like protection relays, often reliant on proprietary programming protocols, necessitates in-depth protocol comprehension, fundamental OT security knowledge, and continuous vulnerability research across design, implementation, and potential abuse vectors.

In order for the power grid sites to be defended effectively against the Industroyer, the below recommendation actions could be followed:

- ✓ For electric utilities, understanding the deployment and usage of protocols like IEC 104, IEC 61850, and, for North American utilities, DNP3, is crucial. This awareness allows security teams to effectively assess and mitigate potential risks associated with this malware.
- ✓ A security understanding of how the OPC communication protocol is implemented and utilized across various industries. Industroyer, is one of the four ICS-tailored malwares that can exploit OPC capabilities.
- ✓ Robust backups of engineering files such as project logic, IED configuration files, and ICS application installers should be offline and tested.
- ✓ Develop and test comprehensive incident response plan. This plan should involve tabletop exercises simulating substation outages and require manual operations alongside SCADA system recovery and forensic data collection. In these exercises relevant stakeholders and personnel from engineering, operations, IT, and security should be included.
- ✓ Leveraging YARA rules alongside other IoCs can enhance detection capabilities. While YARA rules offer greater confidence in identifying an infection, all available IoCs should be considered for a comprehensive search. The behavioral analytics to identify the communications on the network would provide the highest capability to detect this type of threat and similar ones.
- ✓ While some defenses and architecture changes might yield value in other scenarios, the following responses have demonstrated to be ineffective against this particular attack:
    - Transmission and distribution companies should not only rely on the usage of other protocols such as DNP3 as a protection mechanism. The completeness of the CRASHOVERRIDE framework suggests there may be other undisclosed modules such as a DNP3 module.
    - Passive defenses (isolated/air-gapped networks, antivirus, firewalls) and proper security architecture are inadequate against such attack and determined threat actors. This underscores the critical role of human defenders in actively identifying and responding to evolving security threats.

4.2.4.3 Triton/Trisis (2017)

Historically, high-profile ICS attacks focused on process control systems (e.g., SCADA), making them relatively ubiquitous**.** The *Triton* malware, however, breaks new ground by targeting safety controllers, specifically Safety Instrumented Systems (SIS). *Triton* is the fifth ICS tailored malware and was used to attack the SIS Triconex in the Middle East, in 2017. It is the first piece of malware that was specifically designed to target human life although the attack failed and caused an operational outage instead. It is also known as “*Trisis*” or "*Hatman*".

Facility staff promptly identified the attack after unintended processes shutdowns occurred upon perpetrators’ attempt to reprogram the safety instrumented systems (SIS) controllers, using the Triton attack framework. The attackers' malware is believed to have malfunctioned (bug in the script), triggering accidentally the emergency system and causing the shutdown.

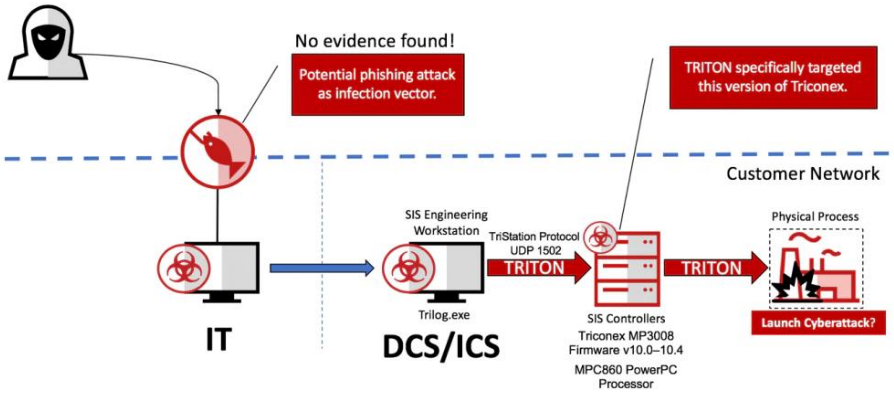


Figure 25 Triton framework, Source: Trellix website [38]

Security-conscious asset owners may implement a "read-only" application-layer firewall on their SIS controllers, as shown in Figure 26. Designed for Modbus/TCP, OPC, and similar protocols, these firewalls prevent unauthorized modification of safety outputs and access to proprietary configuration services. By including both the SIS Engineering Workstation (EWS) and SIS Controllers within the secure zone, this architecture minimizes exposure of programming protocols. An attacker on the L2 LAN cannot manipulate the safety system unless they exploit a firewall vulnerability. However, this approach requires physical access to the SIS EWS for configuration changes, which, unlike DCS (Distributed Control System) updates, should be infrequent.

1. **Reconnaissance:** Attackers likely conducted in-depth reconnaissance to understand the targeted facility's specific control system architecture and safety protocols. This might have involved techniques like analyzing engineering documentation, compromising internal systems for network maps, or even social engineering tactics to gain information from personnel.
2. **Weaponization:** Unlike Industroyer, Triton wasn't a one-size-fits-all malware. Triton, a specific component within Triton, was custom-built to target Triconex Tricon microprocessor-based safety instrumented systems (SIS) used in the facility. This targeted weaponization demonstrates a high level of attacker knowledge and preparation.
3. **Delivery:** The exact delivery method for Triton remains unclear. Potential theories include compromised workstations of personnel with access to control system networks, targeted spear phishing emails with malicious attachments, or even physical access to introduce infected devices.
4. **Installation:** Once delivered, Triron exploited vulnerabilities within the Triconex systems or the surrounding network to gain a foothold. Here, the focus wasn't necessarily on widespread infection, but rather on reaching specific safety control components.
5. **Command and Control (C2):** There's limited public information regarding the C2 infrastructure used by Triton. However, it's likely the malware communicated with attacker-controlled servers to receive instructions and potentially confirm successful manipulation of safety systems.

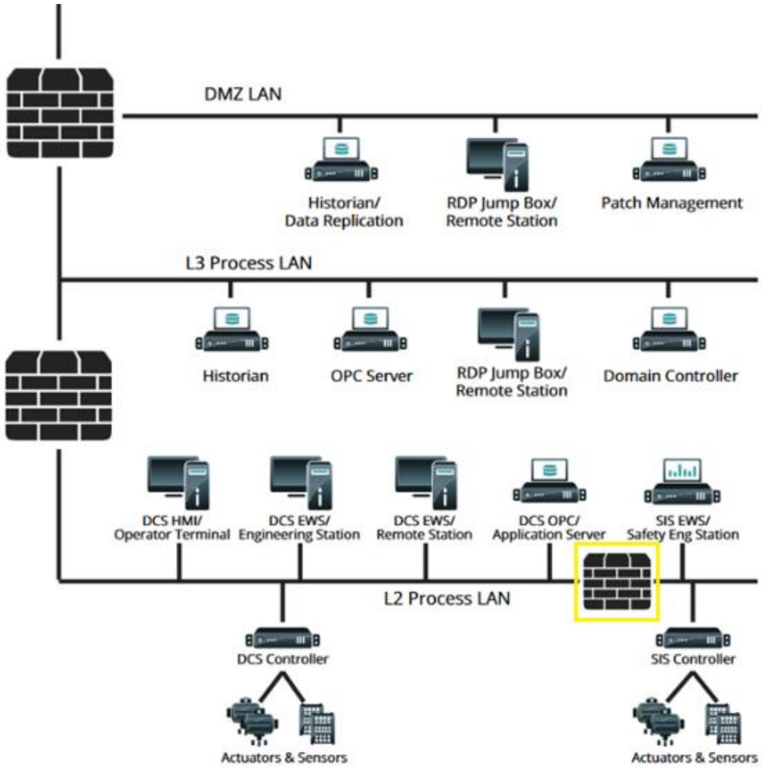

DMZ LAN
Historian/ Data Replication
RDP Jump Box/ Remote Station
Patch Management
L3 Process LAN
Historian
OPC Server
RDP Jump Box/ Remote Station
Domain Controller
DCS HMI/ Operator Terminal
DCS EWS/ Engineering Station
DCS EWS/ Remote Station
DCS OPC/ Application Server
SIS EWS/ Safety Eng Station
L2 Process LAN
DCS Controller
SIS Controller
Actuators & Sensors
Actuators & Sensors

Figure 26 Secure architecture with application-layer 'Read-Only' firewall between L2 and SIS LAN [39]

Lessons Learned

While anti-virus products have been updated to include TRISIS in their signatures, these products cater to Windows-based malware and corruption of the Windows OS. Anti-virus already struggles to detect new Windows malware, so defenders should not rely on it to detect new SIS-specific malware.

Unique characteristics of targeted ICS attacks like TRISIS render traditional IOCs ineffective. Instead, asset owners must adopt a proactive defense strategy focusing on adversarial behaviors and actions. By identifying the key stages of a SIS-targeted attack—initial ICS intrusion, lateral movement, and SIS attack execution—defenders can construct a layered defense to mitigate each stage of the intrusion scenario. As a guide to security teams, the subsequent items present a sample approach to defense implementation.

- ✓ Prevent initial intrusion by working with IT security teams to identify attacks of ICS interest including ICS-themed phishing and by targeting the personnel.
- ✓ Limit remote access from IT to ICS and use two-factor authentication (2FA) where it is allowed.
- ✓ Build detections for malicious ICS behavior incorporating YARA and other detection methodologies on inbound executables.
- ✓ Identify suspicious content moving from IT to ICS.
- ✓ Identify and investigate file movement and transfer, as well as any unfamiliar files.
- ✓ Isolate SIS, if possible, otherwise limit allowed communication to the minimum necessary. Remote access should only be allowed during emergencies, and physical disconnects should be used to control remote access.

- ✓ SIS-connected devices should include higher monitoring and security hardening. If the EWS is only used for configuration of the SIS as opposed to monitoring its state, consider leaving the system turned off until an engineer or operator manually configures it.
- ✓ If possible, implement application whitelisting on any SIS-connecting workstation like the EWS.
- ✓ Engineers and operators should not have local administrative privileges on the EWS.
- ✓ Consider using an application firewall on the EWS that only allows the Tristation (Triconex programming software) configuration software and other required software to make outbound network connections.
- ✓ In particular for the Triconex, the key switch should only be in PROGRAM mode when an operator is actively modifying the controller. Otherwise, it should always be in RUN mode. The REMOTE mode should be avoided as a safety system best practice, however operating the SIS in this position will prevent initial infection.
- ✓ Identify new file writes and new user logins – communication between HMIs and EWS should only occur at known times.

4.2.4.4 Incontroller (aka Pipedream) (2022)

Incontroller, the latest (up to the present time) and most sophisticated ICS-tailored malware discovered, demonstrates native interaction with a diverse range of ICS devices from multiple vendors. This exceptional capability represents a highly dangerous cyber threat, comparable to previous attacks (Triton, Industroyer and Stuxnet).

According to a CISA advisory [40], the malware is able to "scan for, compromise and control, certain ICS/SCADA devices." Those capabilities present a clear threat to the availability, control, and safety of ICS and processes, it can also be used to endanger operations and lives.

Emerging as the fifth industrial process disruption malware, Incontroller surpasses its predecessors in sophistication, evidencing extensive attacker's research and development. Beyond disrupting operations, Incontroller possesses the concerning capability to degrade and potentially even destroy industrial environments and processes. It wields the power to execute end-to-end cyberattacks, seamlessly transitioning between Stages 1 and 2 of the ICS Cyber Kill Chain [32].

The development of this malware demonstrates the risks of increasingly homogenous operational technology systems and modern component-based software. Incontroller covers a wide range of potential targets, encompassing various industrial control systems (ICS) including Programmable Logic Controllers (PLCs) from vendors like Omron and Schneider Electric, and Open Platform Communications Unified Architecture (OPC UA) servers. It can execute attacks that take advantage of universal industrial protocols including CODESYS, Modbus, Factory Interface Network Service (FINS), and OPC-UA. A PLC from Schneider Electric that is attacked by Incontroller uses CODESYS as the base system architecture. This is a third-party software component utilized by hundreds of industrial equipment manufacturers. Although Incontroller is currently able to detect and target PLCs of Omron and Schneider Electric, it can be used to attack controllers of various vendors due to its versatility.

Given that Incontroller abuses a variety of protocols and implements many ICS ATT&CK techniques, it is clear that the threat activity group possesses an extensive ICS knowledge beyond any known ICS activity groups. This malware can operate in both IT and OT networks, with three specific capabilities that adversaries can leverage against OT environments:

1. A tool that scans for OPC servers, enumerates OPC structure/tags, brute forces credentials, and reads/writes OPC tag values.

2. A capability meant to identify, access, modify, and disarm Schneider Electric PLCs. A framework that communicates using Modbus—one of the most common industrial protocols—and CODESYS, a library that is potentially possible to attack various vendors' devices.
3. A capability designed to scan, identify, and interact with Omron software and PLCs via HTTP, Telnet, and Omron FINS protocol. The tool can also interact with Omron's servo drives, which use feedback control to deliver energy to motors for precision motion control.

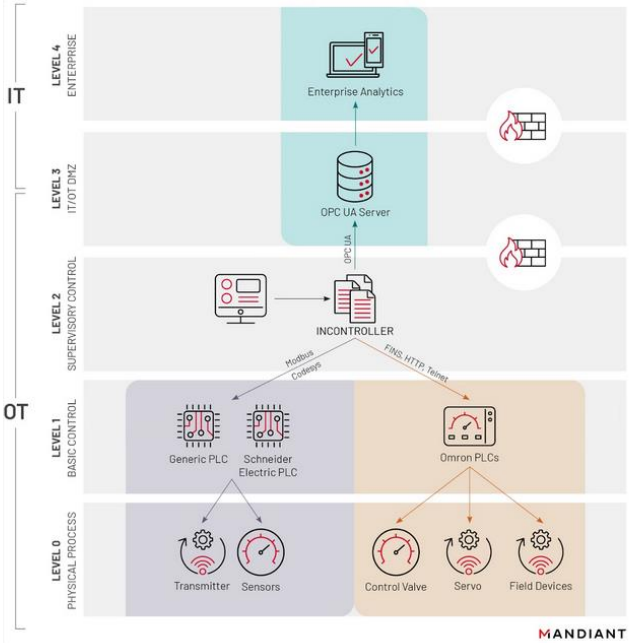


Figure 27 Incontroller analysis report, Source: Mandiant [41]

1. **Reconnaissance:** Attackers likely conducted reconnaissance to understand the target ICS environment. This might involve techniques like scanning for vulnerabilities in industrial control systems (ICS) devices, compromising internet-facing operational technology (OT) assets, or potentially using social engineering tactics to gather information from personnel.
2. **Weaponization:** Incontroller appears to be a modular malware platform specifically designed for ICS environments. Unlike some custom-built threats, Incontroller leverages its modularity to target different functionalities within an ICS. Attackers might develop or acquire plugins that exploit vulnerabilities in specific control systems, manipulate process data, or disrupt communication protocols.
3. **Delivery:** The exact delivery method for Incontroller remains under investigation. Potential theories include compromised workstations with access to control system networks, supply chain attacks targeting ICS software updates, or even exploiting vulnerabilities in remote access tools used for system management.
4. **Installation:** Once delivered, Incontroller could exploit vulnerabilities within ICS devices or the surrounding network to gain a foothold. The specific target might vary depending on the attacker's objectives, potentially focusing on human-machine interface (HMI) systems, programmable logic controllers (PLCs), or communication protocols.
5. **Command and Control (C2):** Incontroller likely communicates with attacker-controlled servers to receive instructions and potentially upload stolen data or provide attackers with a persistent foothold within the ICS environment.

Lessons Learned

One of the worst-case scenarios of an attack, using the Industroyer malware, could cause physical destruction by disabling safety controllers. The attacker disables PLCs responsible for safety controllers, such as the Omron NX-SL3300, and subsequently reprograms or disrupts other ICS assets to cause physical destruction to the industrial machinery. Compromising safety protections can lead the process into an unsafe state, either through natural progression or attacker manipulation. This, depending on physical limitations and facility design, could result in harm to personnel, the environment, or equipment damage. To counter the malware's capabilities, network defenders should implement the following mitigations:

- To ensure the security of Schneider Electric TM2xx series PLCs, especially those with firmware 5.0 or later, promptly change the default credentials 'Administrator'/'Administrator' to a complex password utilizing the EcoStruxure software.
- Fortify the security of Schneider Electric TM2xx series PLCs by restricting access to specific ports: UDP 1740-1743, TCP 1105, and TCP 11740. Moreover, deny access to TCP 11740 and UDP 1740-1743 on non-Schneider PLCs since these devices are associated with these ports for EWS operations.
- To bolster the security of Omron PLCs, restrict access to specific ports: TCP 80, TCP 9600, and UDP 9600. Permit only authorized Engineering Workstations (EWS) to communicate on these ports.
- Validate the EWS software (EcoStruxure Machine Expert and Omron Sysmac/CX-One/NX IO-Configurator). Remove unnecessary software. If possible, use application that allow listing software on the workstation. Restrict the workstation from making outbound network connections, especially to internet services.
- Enhance the security of EWS used for PLC programming, such as EcoStruxure Machine Expert, Omron Sysmac/CX-One, and NX IO-Configurator, by following these measures: validate the software's authenticity, remove any unnecessary software, and, if feasible, utilize applications that allow listing authorized software. Furthermore, restrict outbound network connections from these workstations, particularly to internet services, to minimize potential vulnerabilities.
- Conduct network telemetry analysis to identify unusual communications with PLCs from unauthorized EWS, or user accounts.
- Closely monitor affected PLCs for any new unauthorized outbound connections to other networked PLCs, on UDP 1740-1743, TCP 1105, and TCP 11740.
- Disable the Schneider NetManage discovery service for PLCs.
- Implement robust security measures for safety systems: maintain network isolation, closely monitor networks for unauthorized connections or devices, and strictly enforce change management procedures to verify the legitimacy of all configuration modifications.
- Develop and maintain a comprehensive Incident Response Plan (IRP) specifically tailored to ICS environments.
- Maintain a comprehensive spare parts inventory for critical control system components, encompassing hardware, software, firmware, configuration backups, and licensing information. Additionally, establish procedures for provisioning these critical components when needed. Consider implementing cold backups of level one ICS devices to facilitate rapid system restoration in the event of an incident.

4.2.4.5 Industroyer2 (2022)

Discovered in Ukraine in October 2022, Industroyer2 became the sixth known ICS-tailored malware. This malware targeted high-voltage electrical substations, manipulating physical breakers to switch their states between open and closed, potentially disrupting critical infrastructure. Industroyer2 is a trimmed-down variant of its predecessor Industroyer/Crashoverride and represent the first known ICS-tailored malware, being reconfigured, and redeployed against a power grid infrastructure.

Industroyer2 communicates directly with industrial equipment from an infected control center to substations on TCP port 2404, the default port for the IEC 104 protocol. Unlike Industroyer, Industroyer2 is a standalone executable that contains a more targeted functionality. It is built from the same source code as the Industroyer 104 module (payload 104.dll). The malware was set to execute via a scheduled task on a system in an attempt to shut down a power grid substation in Ukraine.

Unlike its predecessor, which relied on external modules, Industroyer2 is self-contained and focuses solely on the IEC 104 protocol, used for power system control. This malware disrupts operations by manipulating this protocol to communicate and control industrial equipment, primarily targeting Europe and the Middle East. Notably, its configurability allows attackers to tailor its behavior to specific intelligent electronic devices (IEDs) within the victim's environment, enabling focused attacks with reduced effort from the attacker.

The detailed information within Industroyer2 regarding specifically targeted substations and associated IOA (information object addresses), such as the IOA values and which Type IDs to be used, indicates a strong understanding of the victim’s environment. The IEC 104 network traffic (Application Protocol Data Unit packets-APDU packets) generated by Industroyer2 indicate some knowledge of the IEC 104 protocol. The lack of protocol state and timeout awareness or implementation within the malware sample shows that the threat group does not completely understand this protocol. The malware may not run correctly or completely against IEC 104 hardware.

1. **Reconnaissance:** Attackers likely conducted extensive reconnaissance activities to understand the target ICS environment and identify potential vulnerabilities. This could involve techniques like:
    - Scanning for vulnerabilities in network devices used in the power grid.
    - Analyzing publicly available information about Ukrainian power grid infrastructure.
    - Potentially compromising internal systems to gather detailed network maps and configurations (if this wasn't achieved in the 2016 attack).

2. **Weaponization:** Similar to the 2016 variant, Industroyer2 is believed to be custom-built malware specifically designed to target Industrial Ethernet protocols used by Ukrainian power grid equipment. This targeted approach suggests attackers may have refined the original Industroyer based on knowledge gained from the previous attack.
3. **Delivery:** The exact delivery method for Industroyer2 remains unclear. However, potential theories based on the 2016 attack and common ICS attack vectors include:
    - Compromised workstations of personnel with access to control system networks.
    - Removable media (USB drives) containing the malware, potentially introduced through social engineering tactics.
    - Watering hole attacks targeting websites frequented by power grid personnel.

4. **Installation:** Once delivered, Industroyer2 likely exploited vulnerabilities in specific software or communication protocols to gain a foothold on targeted systems within the control network.
5. **Command and Control (C2):** There's limited information about the C2 infrastructure used by Industroyer2. However, it's likely the malware communicated with attacker-controlled servers to receive instructions and potentially confirm successful execution of the attack.

Lessons Learned

To effectively defend power grid sites against Industroyer2 attacks, the following best practices are essential:

- ✓ **Limit TCP/2404 access:** Restrict communication on TCP port 2404 to necessary communications only.
- ✓ **Enhance ICS traffic monitoring:** Implement robust visibility and monitoring of North-South network traffic within ICS environments. This allows asset identification, connection details analysis, and detection of suspicious activities such as abruptly terminated control center-substation connections or anomalous traffic patterns like continuous breaker status polling on TCP/2404.
- ✓ **Enforce application allowlisting**: Implement host-based allowlisting to prevent unauthorized applications from execution or download.
- ✓ **Enforce multi-factor authentication:** Implement multi-factor authentication (MFA) for all users, especially those with privileged access, and for remote access scenarios.

Despite limited public awareness of cyberattacks with physical consequences, reports suggest thousands, potentially millions, of attacks target OT systems. However, inconsistency and opacity in reporting criteria hinder accurate assessments. Applying a conservative approach that only considers confirmed, deliberate attacks causing physical disruption in process and manufacturing industries reveals a concerning upward trend. Even under this restrictive definition, attacks yielding physical consequences are projected to reach critical levels by 2027-2028, demanding immediate attention and improved reporting practices.

5. Cyber Defense Development

5.1. Types of ICS Cybersecurity Programs

An important first step towards maturing an ICS/OT cybersecurity program is proactively assessing the divide between IT and OT cybersecurity strategies. Applying lessons from IT cybersecurity and tailoring them to OT environments can be a years-long process toward maturation.

Despite their differences, all Industrial Control Systems (ICS) share a common vulnerability: the need for robust security. A comprehensive ICS security strategy is essential to address the inherent challenges these systems face across various industries. Risk-based and Compliance-driven ICS cybersecurity programs represent two distinct approaches to safeguarding industrial control systems (ICS) from cyberattacks. While both strategies aim to protect critical infrastructure and operations, they differ in their underlying principles and methodologies.

5.1.1 Risk-based ICS Cybersecurity Strategy

This strategy is a proactive approach that allows for a more comprehensive understanding of an organization’s security posture by identifying, assessing, and mitigating cybersecurity risks of their critical assets. This strategy is based on the principle that organizations should focus their cybersecurity efforts on the assets that are most critical to their business and the risks that are most likely to occur.

It involves identifying and evaluating potential cybersecurity threats, prioritizing the risks based on their likelihood and impact, and implementing targeted security measures to address the most critical vulnerabilities. This approach is tailored to the specific needs and risks of each organization, ensuring that resources are focused on the most pressing concerns. Moreover, it is generally considered that this program is more effective in protecting against cyberattacks, as it can also be more adaptable to changing business needs and evolving threats.

The NIST Framework v2 describes a four-tier/three-section format that can be used for evaluating organizational risk management. The three sections that describe the organization’s position in terms of cybersecurity preparedness are as follows:

- *Risk management process:* The risk management process section deals with whether the organization has formalized risk management practices. It also identifies whether the organization has prioritized its cybersecurity activities with its risk objectives, their threat environment, or their business/mission goals.
- *Integrated risk management programs*: This section identifies organizations based on their awareness of risk associated with their operations, their handling of risk management as an organization, and their process to distribute cybersecurity information throughout the organization.
- *External participation (third-party risks):* The external participation section deals with the organization’s understating of and interaction with other entities in the larger cybersecurity supply chain they are part of.

These sections can then be used to categorize organizations into four implementation tiers in terms of their cybersecurity preparedness.

- ***Tier 1: Partial:*** Organizations do not have any organized risk management plan, resulting in ad hoc cybersecurity risk management steps and no process for coordinating with external organizations.

- ***Tier 2: Risk Informed:*** Organizations have management-generated cybersecurity practices, which create an internal level of organizational risk management steps and processes but have no formalized cybersecurity capabilities to interact with outside organizations.
- ***Tier 3: Risk Informed and Repeatable:*** Organizations have fully approved cybersecurity practices across the organization, which are capable of adjusting against emerging changing threats and technologies. The cybersecurity plan is fully developed and implemented to provide risk-based collaboration with external organizations.
- ***Tier 4: Adaptive:*** The adaptive organization has a cybersecurity risk management system that can adapt to lessons learned from previous occurrences. Cybersecurity risk management is a shared concern across the organization and evolved through feedback from previous occurrences, information obtained from trusted sources, and continued awareness of activities on their own network. This approach also enables the organization to share their cybersecurity approach with partner organizations to maximize their cyber risk management strategies across the enterprise.

5.1.2 Compliance-based ICS Cybersecurity Strategy

In contrast with the risk-based, this strategy focuses on adhering to industry regulations and standards. It prioritizes meeting specific compliance requirements, often driven by mandated regulations or contractual obligations. The requirements of this approach provide a baseline level of protection and can help organizations avoid potential fines or penalties associated with non-compliance. While compliance is essential, it may not always address the full spectrum of cybersecurity threats. Organizations that solely rely on compliance may be exposed to vulnerabilities not covered by the regulations they are trying to comply with.

Achieving OT security compliance requires a systematic approach. Organizations must first identify relevant regulations and standards governing their industry and operations. This initial assessment clarifies compliance expectations. Subsequently, a thorough evaluation of the OT security posture is crucial. This involves comparing current systems, networks, and security policies against the identified regulations, forming the foundation for a tailored compliance plan. The plan outlines actions to bridge compliance gaps, such as implementing new security controls, updating policies, and training employees. Finally, successful implementation necessitates ongoing monitoring and regular audits to ensure the effectiveness of the compliance program.

5.1.3 Hybrid ICS Cybersecurity Strategy: Unifying Risk and Compliance

Integrating both risk-based and compliance-driven approaches offers the most comprehensive approach to ICS cybersecurity. By combining proactive risk assessment with adherence to regulatory requirements, organizations can achieve a robust and adaptable cybersecurity posture that protects critical infrastructure and operations.

This hybrid approach that merges risk-based and compliance-driven strategies offers several advantages. It fosters a comprehensive security posture by addressing both mandated controls (compliance) and the organization's unique vulnerabilities (risk-based). This prioritizes security measures strategically, ensuring resources are directed towards the most critical threats while still meeting regulatory requirements. Additionally, a unified strategy allows for continuous adaptation as the threat landscape evolves or compliance regulations change (future-proofing).

However, implementing this approach requires careful consideration. Merging these strategies can introduce complexity, particularly for organizations with intricate compliance demands. Additionally, it might necessitate acquiring additional expertise to effectively assess risks, navigate compliance regulations, and select the most appropriate security controls.

Overall, unifying risk-based and compliance-driven strategies presents a powerful tool for achieving a robust cybersecurity posture. Organizations should weigh the potential benefits against the complexity involved and ensure they have the necessary expertise for successful implementation.

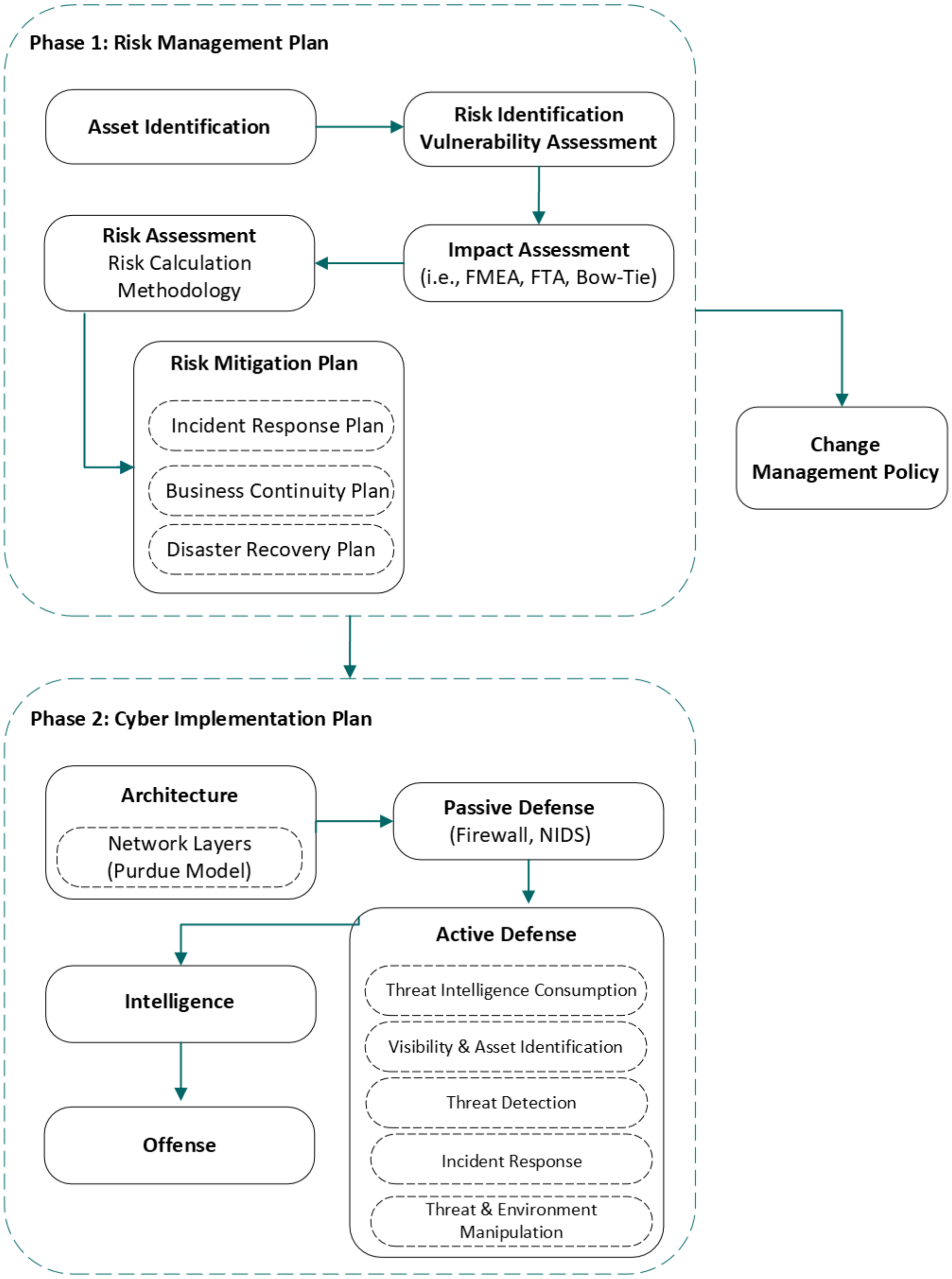

Phase 1: Risk Management Plan
Asset Identification
Risk Identification Vulnerability Assessment
Impact Assessment (i.e., FMEA, FTA, Bow-Tie)
Risk Assessment Risk Calculation Methodology
Risk Mitigation Plan
Incident Response Plan
Business Continuity Plan
Disaster Recovery Plan
Change Management Policy
Phase 2: Cyber Implementation Plan
Architecture
Network Layers (Purdue Model)
Passive Defense (Firewall, NIDS)
Active Defense
Threat Intelligence Consumption
Visibility & Asset Identification
Threat Detection
Incident Response
Threat & Environment Manipulation
Intelligence
Offense

Figure 28 Methodology of Cyber Defense Development Plan

5.2 Risk Management Plan

Facing significant potential disruptions, industrial organizations and critical infrastructure operators must effectively manage cyber risks. Before implementing strategies, leaders need a clear understanding of cyber threats. This definition should encompass operational, business, legal, financial, and security impacts. No single stakeholder group can handle cyber risk alone; collaboration and a comprehensive view are essential.

Risk is the potential loss of an object of value. According to the NIST glossary [42], cybersecurity risk is defined as risk related to the loss of CIA (confidentiality-integrity-availability) of data or information/control systems that reflect potentially adverse impacts to organizational operations. It can also be expressed as an intentional interaction with uncertainty. Risk is also a quantity that can be communicated to the organization’s internal and external stakeholders.

The traditional IT risk models tend to have a blind spot on the physical consequences of cyberattacks on industrial processes. An integrated approach will incorporate engineering and reliability data, such as process hazard analysis (PHA) and failure mode and effect analysis (FMEA), which are commonly used in industrial operations. These risk assessments can identify potential scenarios where cyberattacks could cause unreliable, unsafe, or even destructive outcomes in control systems – a critical aspect missing from traditional IT-focused risk models.

Effectively managing cyber risk in critical infrastructure and industrial environments demands collaboration across OT security, process engineering, and business continuity teams. To achieve this, each business unit should participate in the risk assessment process by:

- ✓ Identifying critical assets and systems
- ✓ Mapping internal and external dependencies
- ✓ Inventorying existing security controls and the associated cybersecurity architecture
- ✓ Assessing the potential business impact and outlining disaster recovery plans
- ✓ Leveraging existing Process Hazard Analysis (PHA) and/or any safety-related analysis
- ✓ Defining stakeholders with clear roles and responsibilities (both internal and external)
- ✓ Assigning risk ownership and outlining escalation procedures for unmitigated or accepted risks

Fortified industrial cybersecurity depicts on a well-defined Industrial Cyber Risk Management (ICRM) program. This below picture depicts the core components of ICRM: the designated roles of stakeholders, their activities in identifying, assessing, and mitigating threats, and the collaborative efforts that establish a strong cybersecurity posture. By comprehending these interrelated elements, organizations can implement a comprehensive ICRM program, safeguarding their critical industrial control systems.

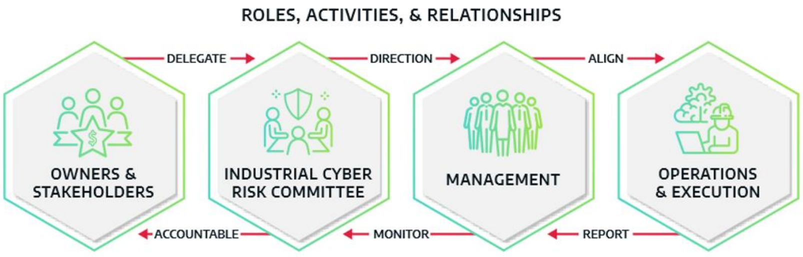


Figure 29 Industrial Cyber Risk Management: Roles, Activities and Relationships [43]

5.2.1 Asset Identification

The cornerstone of crafting effective cybersecurity policies lies in meticulously identifying the network and software assets that are essential to an organization's operations. This crucial step is indispensable for risk management and ensuring unyielding performance in industrial environments. Specifically, this process entails establishing and maintaining a comprehensive inventory of industrial control systems (ICS) devices to gain granular visibility into the organization's OT assets. By establishing a comprehensive asset inventory, organizations can prioritize cybersecurity measures, effectively allocate resources, and mitigate potential vulnerabilities. To establish OT asset visibility, organizations must assess and process organizational assets, specifications, software versions, network roles, and operational data. This comprehensive evaluation enables organizations to identify potential vulnerabilities and threats that could compromise their critical assets and operations.

Another effective way for organizations to identify and prioritize critical assets is to employ a scaled rating system like the Common Criteria for Informational Security Evaluation (Common Criteria or CC) [44]. CC establishes evaluation assurance levels (EALs) that assess the reliability and security of equipment. Organizations can assign higher EAL values to assets deemed more essential to their operations. For instance, a firewall would receive a higher EAL rating than a web server, signifying its greater importance and the need for correspondingly stronger security measures. By leveraging the CC valuation method, organizations can create a hierarchical overview of the network assets and services demand the most attention.

For most organizations, continuously identifying and evaluating critical assets is an essential yet ongoing process. To ensure that the most critical assets receive adequate protection, organizations must meticulously assess their actual values. This task typically falls within the purview of the organization's information security (InfoSec) team, in collaboration with legal, business, and IT personnel.

Crown Jewel Analysis

Every organization possesses its "crown jewels" – the most valuable assets that are indispensable to its operations and, as such, demand the highest level of protection. These crown jewels may encompass individuals (e.g., a head of state, who is meticulously guarded), specific activities (e.g., national elections, whose integrity is paramount), sensitive data (e.g., intellectual property or customer PII), or any core asset that forms the foundation of the organization. In industrial settings, OT assets and their associated business processes often represent the crown jewels. Compromising these assets could inflict severe harm on the organization, leading to operational disruptions, financial losses, and even threats to human safety. Therefore, these critical assets must be prioritized for comprehensive security, even if it means de-prioritizing the security of other, less critical assets and processes. Consequently, correctly identifying these crown jewel assets is of paramount importance.

Accurately identifying an organization's "crown jewels" necessitates a risk-based OT security approach, which involves prioritizing asset criticality by assessing the likelihood of each known threat materializing (e.g., successful attack) within each business unit and the potential impact of such an attack on the organization as a whole. These crown jewels typically consist of critical data, systems, communication links, and interfaces that are essential for managing and controlling components and functions (e.g., engineering and operator workstations, leak detection systems).

Assessing an asset's risk involves a comprehensive analysis and correlation of large datasets, associated with various factors, including attacker capabilities, malware behavior, device vulnerabilities, existing security measures, network layout, communication protocols, and more.

A practical approach to consequence analysis involves first identifying the critical elements of the physical process and their corresponding control mechanisms. Then, by tracing back through the digital interfaces that connect these elements, we can effectively map out potential attack vectors that can be exploited by malicious actors.

The Crown Jewels Analysis (CJA) method offers a systematic way to gather insights from experts (SMEs), identify and record critical dependencies, and prioritize vital assets for smooth operation. This repeatable process thoroughly analyzes physical and logical assets, data, and connections to ensure core functionalities. Understanding the essential components empowers organizations to effectively manage vulnerabilities, respond to incidents, and plan for disaster recovery, ultimately guiding where to prioritize security fundamentals.

By understanding the specific role of each device, organizations can strategically allocate security resources, prioritizing protection for critical assets. This enhances the overall safety and security of the OT environment and ICS. Leveraging OT asset visibility is a vital step in the organization's cybersecurity program, enabling comprehensive risk assessment, efficient threat detection, and informed cybersecurity investments. Ongoing collaboration between IT and OT ensures effective security measures and reduces risks to stakeholders. In essence, OT asset visibility is a foundational element in the protection and optimization of industrial operations.

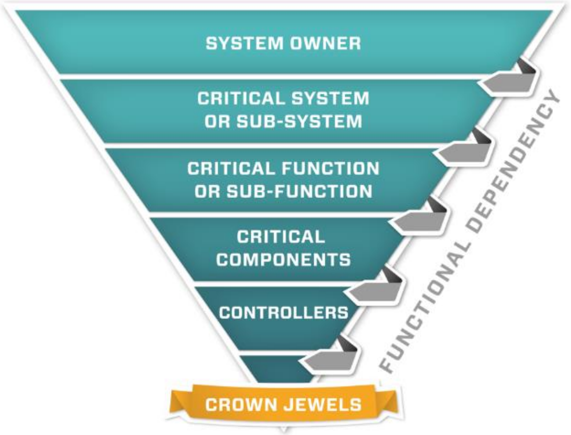


Figure 30 Source: Dragos, Cascading into Crown Jewels [45]

5.2.2 Risk Identification – Vulnerability Assessment

Following the comprehensive identification and valuation of network assets, along with detailed vulnerability and threat assessments, the cybersecurity plan development progresses to risk identification testing. These tests evaluate the network's susceptibility to the identified threats, providing crucial insights for prioritizing and mitigating potential security breaches. This task may be undertaken by the organization's InfoSec team or network administrators. Outsourcing the vulnerability (or risk) assessment to specialized third-party security contractors is also a common practice for enterprises seeking a comprehensive and objective evaluation of their network's vulnerabilities.

A diverse range of methodologies and software solutions are employed for conducting vulnerability and risk assessments, collectively known as penetration testing. The most prevalent approach involves engaging a highly skilled ethical hacker, often referred to as a white-hat hacker, to assume the role of a malicious attacker and attempt with various techniques, to breach the network's security. After obtaining necessary authorization from senior management, the white-hat hacker diligently executes a series of standard penetration testing techniques, which include:

- ❖ *Sniffing:* Using a packet analyzer, the white hat captures data packets as they move across the network, logs them, and decodes their raw data. They can then analyze the data, in effect spying on the network users.

- *Port Scanning:* Using a port scanner package to probe the network servers and devices for open ports that can be exploited. They can also identify services running on a host for potential exploitation.
- *Vulnerability Scanning:* Using a network vulnerability scanner tool to scan the enterprise for different types of common vulnerabilities such as system misconfigurations and default password usage, as well as to create DoS attacks by generating malformed packets.
- *Social Engineering (SE) Attacks:* Most cybersecurity attacks start with phishing or other similar types of SE attacks.

Another tool that plays a crucial role in a vulnerability assessment is *Threat Intelligence platforms,* that provides valuable insights into emerging threats, known vulnerabilities, and potential attack vectors. By leveraging threat intelligence, organizations can enhance the effectiveness of their vulnerability scans, prioritize remediation efforts, and proactively defend against evolving cyber threats. Threat intelligence platforms aggregate and analyze a vast amount of threat data, including vulnerability disclosures, exploit kits, and threat actor TTPs. This comprehensive data helps organizations identify potential vulnerabilities that may be exploited by attackers. By correlating vulnerability data with threat intelligence, organizations can prioritize their vulnerability remediation efforts, focusing on those vulnerabilities that are actively being exploited or are high-risk.

5.2.3 Impact Assessment

The primary goal when managing security risks is to minimize them to an acceptable level. To accomplish this, the organization must identify which threats pose a real concern to them. This is determined by assessing the impact of each security event occurring, through a process known as *impact assessment and analysis.* Impact assessment and analysis is a purely business function that determines which threats pose a danger to the organization so that appropriate proactive measures can be implemented. Using the values established in the asset identification process, a cost can be calculated for occurrences of the different possible incidents noted in the risk identification procedure.

In the realm of industrial and utility risk assessment, a distinct set of risk analysis tools is employed, differing from those typically utilized in enterprise networks. Specifically, risk assessments for OT environments necessitate the integration of process hazard analysis (PHA). PHAs are instrumental in identifying and assessing the potential hazards inherent in individual industrial processes.

A comprehensive PHA thoroughly evaluates the influence of production equipment, process control instrumentation, utilities, and human factors on the industrial process. Specifically, the PHA meticulously examines the potential consequences that could arise from various industrial accidents, encompassing fires, explosions, and hazardous materials incidents. While numerous methodologies exist for conducting PHAs, six fundamental tools are typically employed to facilitate this analysis:

- FMEA (failure mode and effects analysis)
- LOPA (layer of protection analysis)
- FTA (fault tree analysis)
- ETA (event tree analysis)
- CCA (cause-consequence analysis)
- Bow-Tie diagrams

5.2.4 Risk Assessment – Risk Register

The fundamental objective of a risk assessment is to identify and implement measures that enable an organization to comprehend the cybersecurity threats posed to its operations, assets, personnel, and reputation. This entails thoroughly evaluating the likelihood and potential consequences of security incidents within the organization's network infrastructure. Once these variables have been comprehensively assessed, organizational management can establish the acceptable level of risk, commonly expressed as risk tolerance or risk acceptance.

Eliminating all risk from any endeavor or network environment is an implausible endeavor. Accordingly, the overarching aim of risk assessment procedures is to generate guidelines that enable organizations to manage risks effectively, minimizing threats to an extent that aligns with their priorities, constraints, risk appetites, and assumptions. By comprehending their own risk tolerance levels, organizations can prioritize systems that demand immediate attention, optimizing their cybersecurity investments.

Risk assessments typically employ a matrix structure to effectively connect identified threats with their associated impact and likelihood levels. As an illustration, the table below presents an exemplary risk assessment matrix. This example identifies potential threat actors and incorporates existing safeguards. The subsequent steps outline the ICS risk assessment process.

- Identify and document asset vulnerabilities
- Collect threat and vulnerability information from available information sources
- Identify and document threats to the targeted organization's assets.
- Analyze potential impacts
- Identify risk responses

Although industrial environments are by nature susceptible to cyber threats, OT security professionals have the means to deal with these risks. Implementing manual recovery procedures, fortifying defenses, and eliminating vulnerabilities can minimize the outcome of an attack to a lower impact level. The unique blend of industrial engineering and network security expertise is why the industrial cyber risk incorporates both traditional IT risk as well as business continuity concerns. Building upon the analysis, an OT-centric risk equation is proposed:

Industrial Cyber Risk (ICR) = Likelihood * Impact * Exposure * Threat Actor * (1 - Safeguards)

This formula incorporates the following factors:

- **Likelihood (L):** This represents the probability of a cyberattack occurring on the ICS system. It can be a value between 0 (no chance) and 1 (certain to happen), considering factors like:
  - Historical data on cyberattacks targeting similar ICS systems.
  - Intelligence reports on known threats targeting your industry or region.
  - Vulnerabilities present in your ICS environment and their exploitability.

- **Impact (I):** This metric reflects the severity of potential consequences from a successful cyberattack on an OT/ICS system integrated into a critical infrastructure network. It ranges from 0 (low) to 1 (high) and considers IACS system categorization for the maritime domain as also applicable to any critical infrastructure network. Predetermined system impact elements are based on IACS – No. 166 2020, 7.7.2.3.

  Impact Analysis: The analysis focuses on the confidentiality, integrity, and availability (CIA) of OT/ICS system data due to cyber threats. This ultimately considers potential impacts on human safety, critical infrastructure integrity, and environmental threats. A separate table details the mapping between impact and the CIA triad for each system category.

Category	Impact	Confidentiality	Integrity	Availability
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	**LOW (L)**	**MEDIUM (M)**	**LOW (L)**
II	Those systems, failure of which could **eventually** lead to dangerous situations for human safety, safety of the of the vessel and / or threat to the environment.	**MEDIUM (M)**	**HIGH (H)**	**MEDIUM (M)**
III	Those systems, failure of which could **immediately** lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment	**MEDIUM (M)**	**HIGH (H)**	**HIGH (H)**

Figure 31 CIA triad per OT system category , based on IACS – No. 166 2020, 7.7.2.3.

- **Confidentiality:** Unexpected or unauthorized disclosure of information
- **Integrity:** Unexpected or unauthorized modification of information or functionality.
- **Availability:** Unexpected or unauthorized destruction of the information or disruption of access to, or use of, a system.

- **Exposure (E):** This metric reflects the likelihood of an attack reaching the vulnerable system. It can be a value between 0 (no chance) and 1 (certain exposure), considering factors like:
  - Internet connectivity and remote access points.
  - Supply chain vulnerabilities in ICS software or hardware.
  - Interconnections with IT systems that could be exploited.
  - Insecure remote access methods.
  - Physical access controls for personnel.

- **Threat Actor (TA):** This metric represents the capability and motivation of potential attackers targeting the ICS system. It can be a value between 0 (no threat) and 1 (high threat level), considering factors like:
  - Common cybercriminals.
  - Hacktivists.
  - State-sponsored actors.
  - Industrial espionage actors.
  - Disgruntled insiders.

- **Safeguards (S):** This metric represents the effectiveness of existing security measures in mitigating cyber risks. It can be a value between 0 (no safeguards) and 1 (highly effective safeguards), considering factors like:
  - Network segmentation to isolate critical systems.
  - Patching vulnerabilities in ICS components. OEM support.
  - Implementing security protocols for remote access.
  - User access controls and training for ICS personnel.
  - Monitoring System, Intrusion Detection and Prevention systems (IDS/IPS).

The below table provides a guideline for assigning values to the factors used in the ICR formula (Likelihood, Impact, Exposure, Threat, Safeguards) based on severity levels (Low, Moderate, High).

Factor	Low (0.1-0.33)	Medium/Moderate (0.34-0.66)	High (0.67-0.99)
Likelihood (L)	- Unlikely historical incidents or exploitability of vulnerabilities.	- Moderate historical incidents or potential for targeted attacks.	- Frequent historical incidents or highly exploitable vulnerabilities.
Impact (I)	Failure of which will not lead to dangerous situations for human safety, safety of the critical infrastructure and / or threat to the environment.	Failure of which could eventually lead to dangerous situations for human safety, safety of the of the critical infrastructure and / or threat to the environment.	Failure of which could immediately lead to dangerous situations for human safety, safety of the critical infrastructure and / or threat to the environment
Exposure (E)	- Limited internet connectivity - Strong supply chain security.	- Some internet connectivity - Potential for supply chain vulnerabilities.	- Extensive internet connectivity - Known supply chain vulnerabilities - Insecure remote access.
Threat Actor (TA)	- Low activity of cybercriminals, no state-sponsored actors targeting similar systems.	- Moderate activity of cybercriminals, potential for targeted attacks by some actors.	- High activity of cybercriminals, confirmed targeting by state-sponsored actors.
Safeguards (S)	Weak security measures: - Limited patching - Poor access controls.	Moderate security measures: - Some patching implemented - Basic access controls.	Highly effective security measures: - Consistent patching, - Strong access controls, advanced intrusion detection.
ICR Rate	Min: 0.00009 Max: 0.00794	Min: 0.00881 Max: 0.64514	Min: 0.06649 Max: 0.00960

Figure 32 ICS Risk Calculation, Factors per Criticality

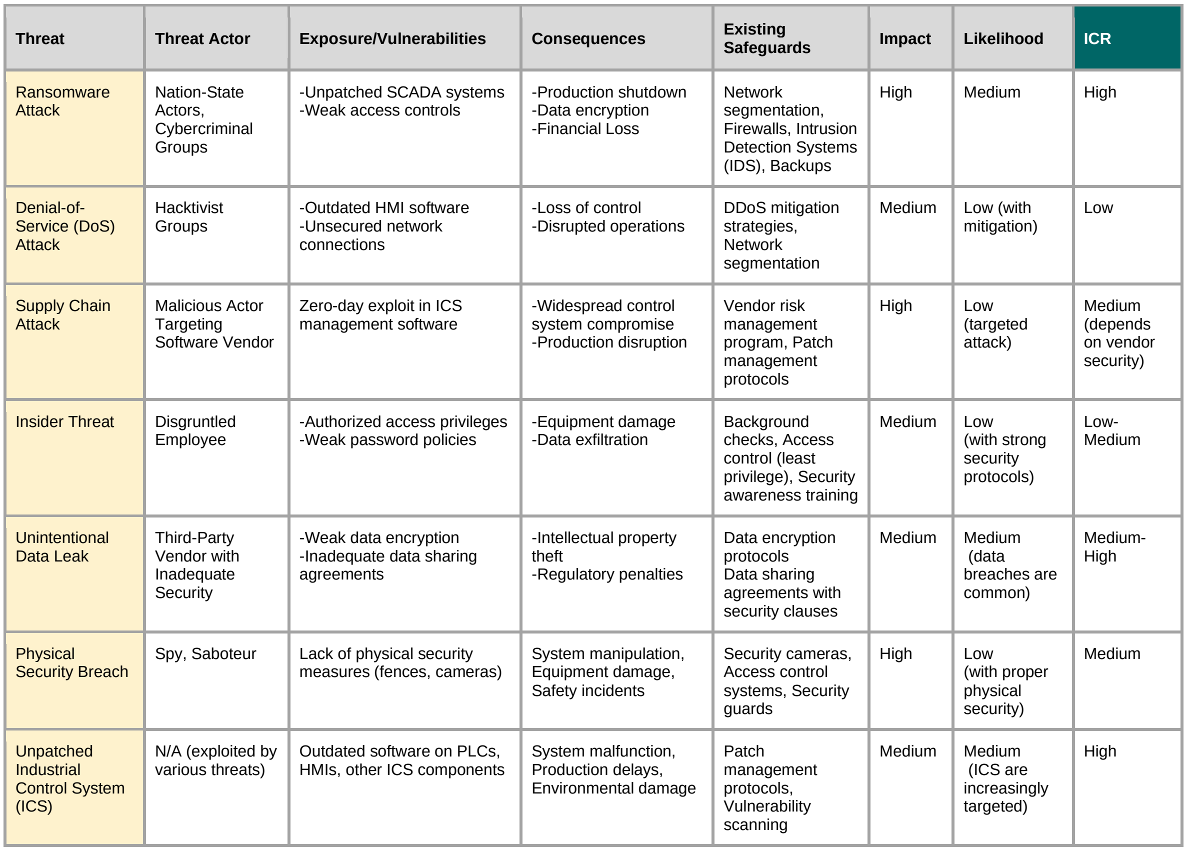
Example: Assigning values to each factor remains crucial. Here's a hypothetical example:

- **Likelihood (L):** 0.4 (Moderate likelihood based on historical data and industry trends)
- **Impact (I):** 0.8 (High potential impact considering failure of which could immediately lead to dangerous situations for human safety, safety of the site and/or threat to the site)
- **Exposure (E):** 0.6 (Moderate exposure due to some internet connectivity and potential supply chain vulnerabilities)
- **Threat Actor (TA):** 0.7 (High threat level considering the presence of both common cybercriminals and state-sponsored actors)
- **Safeguards (S):** 0.5 (Moderate effectiveness of existing security measures)

Plugging these values into the formula: **ICR = 0.4 * 0.8 * 0.6 * 0.7 * (1 - 0.5) = 0.0672 (High)**

This ICR score (0.0672) provides a quantitative estimate of the cyber risk associated with this specific ICS system. It can be used for comparison with other assets within the ICS environment to prioritize risk mitigation efforts.

The recommended ICR formula offers a quantitative score for cyber risk comparison and prioritization across ICS assets. Assigning factor values requires careful consideration of the specific environment and potential threats. Notably, the formula highlights the importance of safeguards (S) in mitigating cyber risk. However, it can be adapted to incorporate additional environment-specific factors like system recoverability. Risk management frameworks typically combine quantitative and qualitative assessments to determine optimal security measures for ICS systems. It's important to remember that these are general guidelines; specific values should be based on a thorough risk assessment considering historical data, intelligence reports, vulnerability assessments, and the specific threats targeting your industry or region.



Threat	Threat Actor	Exposure/Vulnerabilities	Consequences	Existing Safeguards	Impact	Likelihood	ICR
Ransomware Attack	Nation-State Actors, Cybercriminal Groups	-Unpatched SCADA systems -Weak access controls	-Production shutdown -Data encryption -Financial Loss	Network segmentation, Firewalls, Intrusion Detection Systems (IDS), Backups	High	Medium	High
Denial-of-Service (DoS) Attack	Hacktivist Groups	-Outdated HMI software -Unsecured network connections	-Loss of control -Disrupted operations	DDoS mitigation strategies, Network segmentation	Medium	Low (with mitigation)	Low
Supply Chain Attack	Malicious Actor Targeting Software Vendor	Zero-day exploit in ICS management software	-Widespread control system compromise -Production disruption	Vendor risk management program, Patch management protocols	High	Low (targeted attack)	Medium (depends on vendor security)
Insider Threat	Disgruntled Employee	-Authorized access privileges -Weak password policies	-Equipment damage -Data exfiltration	Background checks, Access control (least privilege), Security awareness training	Medium	Low (with strong security protocols)	Low-Medium
Unintentional Data Leak	Third-Party Vendor with Inadequate Security	-Weak data encryption -Inadequate data sharing agreements	-Intellectual property theft -Regulatory penalties	Data encryption protocols Data sharing agreements with security clauses	Medium	Medium (data breaches are common)	Medium-High
Physical Security Breach	Spy, Saboteur	Lack of physical security measures (fences, cameras)	System manipulation, Equipment damage, Safety incidents	Security cameras, Access control systems, Security guards	High	Low (with proper physical security)	Medium
Unpatched Industrial Control System (ICS)	N/A (exploited by various threats)	Outdated software on PLCs, HMIs, other ICS components	System malfunction, Production delays, Environmental damage	Patch management protocols, Vulnerability scanning	Medium	Medium (ICS are increasingly targeted)	High

Figure 33 Example of a Cyber Risk Assessment

Effective risk assessment in modern production environments demands the utilization of automated tools that continuously access and analyze up-to-date vulnerability and advanced persistent threat (APT) databases. Risk assessment consultancy has evolved beyond a mere annual manual process; it must now become an ongoing, automated endeavor.

A majority of industrial firms and utilities already have the capability to monitor cyber risks. The primary tool for this purpose is a well-structured Risk Register. A Risk Register serves as a central repository where business leaders and management can access and manage their entire portfolio of risks, including cyber risks. When effectively utilized, Risk Registers ensure that industrial firms and utilities maintain a unified understanding of their cyber risk profile. This, in turn, facilitates informed risk management decisions by prompting organizations to continually assess whether the right risks are being tracked, measured, and managed in a consistent and repeatable manner. Risk monitoring activities involve regularly updating the Risk Register and integrating its insights into routine risk communication initiatives.

Once a Risk Register has been established, organizations must assess each risk individually. Additionally, it is important for organizations to consider both inherent and residual risks. Understanding the distinction between these two terms is essential for effectively managing and mitigating cyber threats.

- ***Inherent Risk:*** refers to the level of risk that exists before any security controls are implemented. It's the baseline level of risk associated with a particular asset, process, or activity. Inherent risk is often considered the "true" risk, as it represents the potential for harm in the absence of any protective measures. Alternatively, this may be the current level or risk (including current mitigation factor) prior to any additional mitigation efforts.

- ***Residual Risk****:* on the other hand, is the remaining level of risk after security controls have been implemented. It's the risk that persists after implementing preventive, detective, and corrective controls to mitigate the inherent risk. Residual risk is the risk that organizations must accept or continue to manage.

5.2.5 Risk Mitigation – Resilience

Risk mitigation (risk reduction) is a systemic approach to reducing the extent of exposure to a risk and/or the likelihood of its occurrence. There are several management plans that come together to produce an effective risk mitigation plan. These plans include the following:

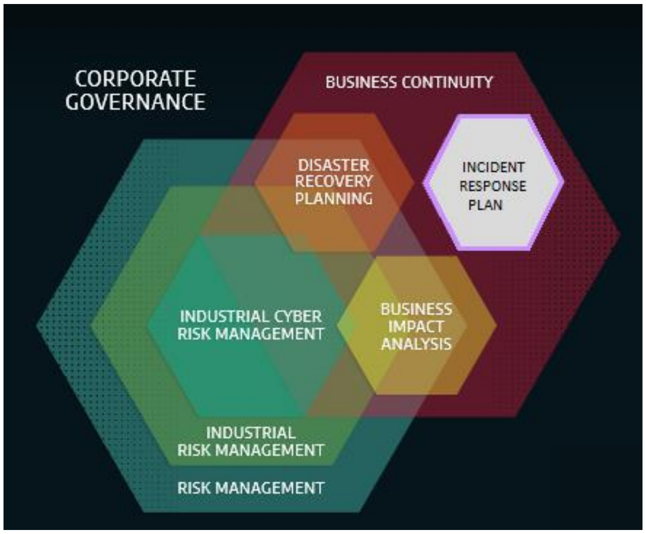


Figure 34 Risk Management Plans – Nested Relationship

- **Incident Response Plans (IRPs)**

A comprehensive incident response plan (IRP) serves as an organization's blueprint for effectively addressing and recovering from security incidents. It is designed to be proactive first – in monitoring activities to spot potential troubles. It is also activated in situations where the organization's edge protection and personnel training efforts have failed. The IRP encompasses information security, forensics, and cybersecurity functions to identify the source, vector, and target of attacks or exploits against the organization's systems. The plan's implementation should effectively guide the organization towards the appropriate course of action to minimize damage and restore normalcy. The details of this topic can be found in the following *Chapter 5.5.4*.

- **Business Continuity Plans (BCPs)**

A comprehensive business continuity plan (BCP) serves as the cornerstone for an organization’s preparedness, growth strategy, and future resilience in the event of disruptive events. It acts as an overarching framework that guides the design and implementation of incident response and disaster recovery plans. The BCP meticulously identifies critical business functions and outlines procedures for responding to and recovering from business interruptions caused by identified risks and business impact assessments. This ensures the most cost-effective continuation of operations. The BCP encompasses all internal business units, including external vendors, and aims to comprehensively address potential disaster scenarios that could hinder or halt organizational operations. These scenarios typically include natural disasters, utility disruptions (power, network), and man-made interruptions (hacker attacks, terrorist activities). A robust BCP goes beyond disaster recovery plans and incorporates risk analysis, business impact analysis, plan maintenance, training, and integration processes, along with plan validation. These components are typically developed by the organization’s enterprise resource planning (ERP) or information security (Infosec) teams. Executive support and endorsement are crucial for the successful execution and implementation of the BCP.

- **Disaster Recovery Plans (DRPs)**

Despite its criticality, a disaster recovery plan (DRP) can quickly become obsolete/outdated without regular updates. Similar to the incident response plan (IRP), modifications to the DRP must be documented to capture lessons learned from past incidents and improve security policies and procedures. The DRP should explicitly outline the organization’s security policies governing update frequency, storage, and preservation guidelines. Additionally, processes must be established to ensure that all stakeholders are familiar with the DRP and capable of implementing it effectively in the event of a disaster. The DRP should encompass recovery strategies for a wide range of data loss and system failures, encompassing natural disasters (flood, fire), electrical-related failures (power outages), and system data corruption (viruses, sabotage, hacking). Hard copies of the DRP documentation should be duplicated and made accessible not only at the primary site but also with the off-site backups. As the plan undergoes updates, all copies must be simultaneously revised to maintain consistency and effectiveness. The disaster recovery plan should at least include the following supporting documentation:

- Printed copies of the official DRP for proper distribution to all involved parties of the DRP
- Complete listing of what comprises the DRP documentation package
- Listing of the name and contact information for all individuals who are members of the DRP team
- Hardware and Software inventory associated with all endpoint and network connections devices, along with copies of any applicable information manuals
- Copies of critical software and hardware drivers stored on removable hard drives or other media that can be stored safely and securely away from the facility in encrypted and password-protected formats
- Baseline metrics, both the latest and necessary historical data

The plans must be in place and managed properly to provide a successful cybersecurity risk management plan. These separate plans work together to form the structure of the organization’s cybersecurity policies.

5.3 Change Management

Despite the initial design and implementation of a cybersecurity plan, it is often left unchanged over time, failing to adapt to evolving network architecture and cybersecurity threats. To effectively address these dynamic factors, a comprehensive change management policy should be implemented to govern modifications and ensure proper documentation. This policy should encompass procedures for handling changes in various areas, including:

- Information system ownership
- System architecture
- System status
- Additions or deletions of system interconnections
- System scope
- Certification and accreditation status

In the context of OT networks, where availability often supersedes confidentiality as the primary concern, the discovery of unauthorized configuration changes necessitates distinct actions. To effectively manage change, a reference point, known as a baseline, is essential for evaluating alterations. After assessing the potential impact of identified risks, organizations must establish a security baseline that defines their acceptable risk tolerance level.

5.3.1 Change Management Documentation

One of the major components of the change management policy is the documentation and tracking specifications for approved changes. Documentation is a record keeping of significant changes in equipment, software, plans or actual events (such as security violations). Having good documentation procedures is one of the keys of effective ongoing change management. The change management policy should address the following documentation by assigning responsibility for creating and maintaining these items to specific personnel or groups:

- *A current, functional software code library for all the ICS components*. This library should contain the latest stable software versions deployed for each ICS component (PLC, data historians, engineer’s stations, switches, routers, firewalls)
- *An archive library of ICS software*. This library should contain at least one previous software revision for each ICS component in the ICS.
- *A current hardware inventory of all ICS control and network devices.* This inventory should be cross-references to the software code library.
- *A current network architecture schematic*. This map should show the physical paths and locations of all wiring, junction boxes, and data communications connections. Documentation should be maintained to annotate where each piece of network equipment belongs and who should have access to that equipment. This is especially important for a topology showing physical and logical connections of the critical servers, routers, switches, IDS, and firewalls.
- *Equipment changes history*. A history of equipment upgrades can prove to be extremely important in production environments. When any new equipment arrives, it should be inventoried, physically tagged/labeled, tested, and fully documented.

The change management policy should specify what controls are used to prevent unauthorized access or changes to operational code. Access to all the configuration documentation listed should be controlled to prevent public or casual access. Update capabilities should be limited to the authorized staff only.

Archives of the software, hardware inventory, current configuration, and schematics should be maintained in a physical location separate from the production system copies. This is typically specified in the disaster recovery plan (covered in the Chapter 5.2.5).

5.3.2 Change Management Configuration

Deviations from the baseline configuration introduce vulnerabilities that can hinder organizational productivity and profitability. To mitigate these risks, organizations must implement a robust configuration change management process that adheres to their overarching change management policy.

Configuration change management entails meticulously tracking and managing all configurable elements within the network. This comprehensive approach is crucial for ensuring the reliable and secure operation of network infrastructure and processes.

Configuration changes to network devices can be addressed manually or through automated tools. While manual management offers flexibility, automated tools can streamline the process and facilitate scalability as networks evolve and expand.

5.4 Cybersecurity Implementation Plan

The vulnerability of critical infrastructures to cyberattacks by extremists and nation-states poses a multifaceted challenge to cybersecurity. While sophisticated security strategies are crucial, organizations must clearly define their objectives before implementation. A generic approach that merely seeks ‘security’ or ‘defense’ is inadequate to address the diverse threats and skill sets required.

Cybersecurity defenses can be categorized as passive or active. Passive defenses prioritize denial, essentially blocking access to assets upon detecting an attack. In contrast, active defense adopts a proactive approach, detecting, diverting, and engaging with adversaries to understand their TTPs. These TTPs represent adversary attack patterns or tradecraft, enabling organizations to anticipate and prevent attacks. Examples of tradecraft include attack execution methods, targeted devices, exploited vulnerabilities, and technical tools employed for persistence, lateral movement, data exfiltration, and remote access. Active defense further involves strategically altering the environment or adversary perception to proactively detect and mitigate attacks.

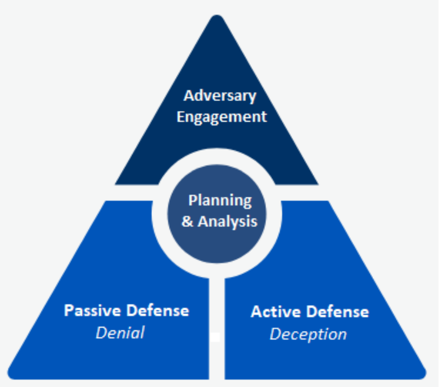


Figure 35 Active vs Passive Defense [46]

While traditional passive cybersecurity measures may suffice for low-risk facilities, organizations operating critical infrastructure must recognize the escalating sophistication of cyberattacks and adapt their defenses accordingly. Active monitoring, anomaly management, and the expertise of qualified personnel are crucial to effectively counter non-traditional, targeted attacks.

To assist industrial managers in comprehending their cybersecurity challenges without requiring them to become cybersecurity specialists, ARC Advisory Group developed the Industrial Cybersecurity Maturity Model (ICSMM). This model enables managers to strike a balance between cybersecurity investments, their risk appetite, and the cost-benefit analysis of additional security layers. The ICSMM also provides a clear framework for distinguishing between passive and active cyber defense strategies. The ICSMM breaks cybersecurity down into a series of incremental steps, each addressing a specific security issue in a straightforward manner. These steps encompass securing individual devices, defending facilities from external attacks, containing malware that may infiltrate control systems, monitoring systems for suspicious activity, and actively managing sophisticated threats and cyber incidents. For each step, the ICSMM outlines a corresponding set of actions, technologies, and human resources required to effectively implement and maintain the associated security measures.

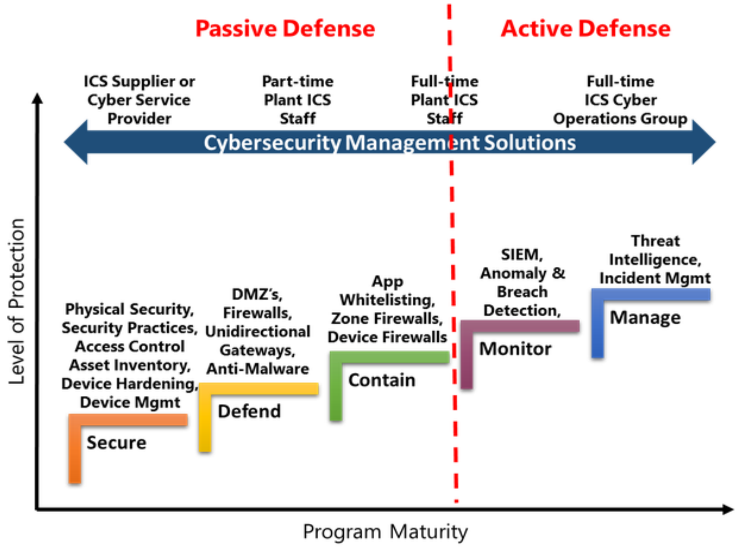

Passive Defense
Active Defense
ICS Supplier or Cyber Service Provider
Part-time Plant ICS Staff
Full-time Plant ICS Staff
Full-time ICS Cyber Operations Group
Cybersecurity Management Solutions
Level of Protection
Physical Security, Security Practices, Access Control Asset Inventory, Device Hardening, Device Mgmt
Secure
DMZ's, Firewalls, Unidirectional Gateways, Anti-Malware
Defend
App Whitelisting, Zone Firewalls, Device Firewalls
Contain
SIEM, Anomaly & Breach Detection,
Monitor
Threat Intelligence, Incident Mgmt
Manage
Program Maturity

Figure 36 Passive vs Active Defense [47]

The Sliding Scale of Cyber Security, presented by SANS, provides a structured roadmap for ICS facilities to enhance their cybersecurity posture. This model serves as a comprehensive framework for understanding and implementing various cybersecurity measures. Additionally, the scale offers several practical applications, including facilitating communication with non-technical personnel, prioritizing resource allocation, evaluating cybersecurity effectiveness, and validating incident root cause analysis. This chapter contributes to the thesis by translating theory into practice. It provides key steps and considerations to guide the practical implementation of the recommended layered defenses on critical infrastructure.

The model is organized into five interconnected categories: Architecture, Passive Defense, Active Defense, Intelligence, and Offense. This continuum emphasizes that cybersecurity measures are not always clearly defined or static. Grasping these interrelated categories enables individuals and organizations to comprehend the purpose and impact of their security investments, establish a maturity model for their cybersecurity program, and effectively analyze cyberattacks to identify root causes. While all five categories are essential, organizations should prioritize their implementation based on the expected return on investment. The ultimate goal of achieving cybersecurity is to establish a solid foundation and cultivate a security culture that adapts and enhances over time. This approach empowers defenders to continuously refine their skills and strengthen their defenses in response to evolving threats and challenges. Moreover, the scale serves as a valuable tool for measuring an organization's cybersecurity maturity journey. Organizations should prioritize achieving the fundamental elements on the left side of the scale before venturing into the more advanced aspects on the right.

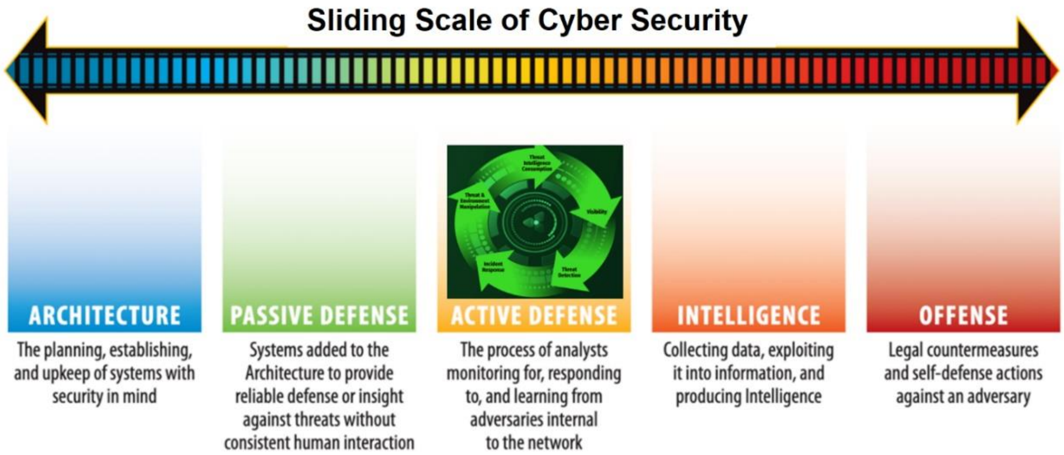

Sliding Scale of Cyber Security
Threat Intelligence Consumption
Threat & Environment Manipulation
Visibility
Incident Response
Threat Detection
ARCHITECTURE
The planning, establishing, and upkeep of systems with security in mind
PASSIVE DEFENSE
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction
ACTIVE DEFENSE
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network
INTELLIGENCE
Collecting data, exploiting it into information, and producing Intelligence
OFFENSE
Legal countermeasures and self-defense actions against an adversary

Figure 37 Source: Whitepaper of Rob Lee, founder, and CEO of security firm Dragos [48]

The foundational stages of the security scale, Architecture and Passive Defenses, prioritize fundamental security practices like network segmentation, system hardening, and deploying anti-malware, firewalls, and basic intrusion detection technologies. These measures effectively neutralize most cybercriminal and casual threats, minimizing the need for constant human interaction. However, as modern cyber adversaries become more sophisticated, traditional defenses are no longer sufficient. Today's threat landscape demands a proactive approach that encompasses active defense strategies.

Organizations that have successfully implemented robust Architecture and Passive Defenses can further upgrade their defense level by forming a dedicated team of cybersecurity experts to execute the Active Cyber Defense Cycle. This taskforce demands specialized knowledge of cybersecurity tactics and a comprehensive grasp of the physical processes they are protecting.

5.4.1 Architecture

The cornerstone of a secure architecture lies in the meticulous planning, engineering, and design of systems tailored to the organization's unique requirements. To achieve this alignment, organizations must first clearly define the core business objectives their IT systems serve, which may vary across industries and companies. Security should be seamlessly integrated into these systems, empowering, and enabling the fulfillment of these objectives. Unlike a solely defense-oriented approach, Architecture should encompass both normal operating conditions and emergency operating scenarios, ensuring the system's resilience and adaptability to any challenge.

In this context, "architecture" is defined as encompassing the processes and actions that contribute to and culminate in a system that is meticulously designed and maintained with security as a paramount consideration. This approach encompasses the following principles:

- Employing the most robust and secure implementations of protocols and systems whenever feasible.
- Identifying and implementing network data flows to enable comprehensive monitoring of network connections.
- Proactively maintaining patching for all systems to the best of the organization's ability

Establishing a robust security-minded architecture is a complex endeavor. However, investments in this area significantly enhance the effectiveness of both passive and active defenses. As the industry moves towards greater IT/connectivity, it becomes increasingly crucial to establish robust boundary protection between the OT and IT networks. This entails implementing safeguards that allow authorized data exchange while effectively shielding the OT network from potential threats emanating from the IT network, non-ICS personnel, and the Internet.

Boundary protection encompasses the deployment of dedicated devices that regulate the flow of information between security zones with varying security requirements or policies. These devices include gateways and routers, firewalls, intrusion detection systems (IDS), antivirus/antimalware software, encrypted tunnels, virtual private networks (VPNs), and data diodes. Traditional cybersecurity measures like firewalls are often insufficient to address the inherent vulnerabilities that pervade industrial networks. These flaws originate from design shortcomings in systems and protocols that have remained unresolved over time. A more effective approach entails constructing a secure architecture from the outset. This encompasses securing the supply chain, designing networks for resilience and security, maintaining, and patching systems, and adopting a comprehensive defense strategy.

The Purdue Model [49] is a widely established high-level architecture model for industrial control system networks that organizations could refer to. The purpose of this structure is to show the partition and segmentation that is needed amongst network segments by their function. A proper segmentation of a network can drastically reduce its vulnerability level, resulting in its robust security.

Network Layers

Organizations should implement a defense-in-depth strategy to safeguard critical infrastructure systems (ICS) from online threats. This strategy involves employing multiple layers of security measures, including firewalls and networks, to prevent unauthorized access and mitigate the impact of cyberattacks.

- An Internet firewall between the Internet and an IT DMZ network
- A DMZ firewall between the DMZ and the IT network
- An IT/OT firewall between the IT network and an ICS DMZ
- An ICS DMZ firewall between the ICS DMZ and the ICS plant-wide network
- Production unit firewalls between the plant-wide network and individual DCS, SCADA, or production cell controllers
- Device network firewalls between production units and their networks of connected PLCs
- A SCADA WAN firewall between a SCADA system and the WAN that connects the system to remote sites and equipment

IT security defense best practice recommends that no two layers of firewalls be sourced from the same vendor, in hopes that no single vendor's firewall vulnerability can be used to traverse multiple layers in this defensive structure. However, this approach has inherent limitations, leading Secure OT practitioners to favor physical isolation measures, such as air gaps and unidirectional gateways, over software-based defenses. A single layer of unidirectional protection between the Internet and control devices directly responsible for physical operations is sufficient to prevent online attacks from traversing multiple layers and disrupting operations. In addition to control-critical networks, secure OT sites typically employ unidirectional gateways to isolate non-critical networks, which typically include:

- The Internet
- IT networks, through which Internet-based attacks often pivot into ICS target

- Any wireless network, since wireless communications intrinsically broadcast, and it is impossible to identify which nearby wireless devices have access to the wireless communications

Air gaps and unidirectional gateways are the only physical protection that secure OT endorses to defeat online attacks from noncritical networks reliably.

- Air gaps permit no online information/attack flows at all
- Unidirectional gateways are a combination of hardware and software – the hardware is physically able to transmit information in only one direction, and the software replicates databases, and emulates protocol servers and devices.

Unidirectionally replicated databases and emulated devices operate within IT networks, enabling users to interact with them as if they were the original ICS systems. Unidirectional gateways facilitate data flow from control-critical networks to external networks, while strictly prohibiting any data or attack traffic from entering the control-critical domain. These gateways are commonly employed as a replacement for one firewall layer in a defense-in-depth network architecture. Secure OT sites deploy firewalls extensively within control-critical networks and between ICS networks within the same control-critical group, but they do not use firewalls between control-critical and non-critical networks.

5.4.2 Passive Defense

Passive defense systems are seamlessly integrated into the system architecture, to provide continuous protection against threats, or insights, without constant human intervention. These autonomous systems, such as firewalls, anti-malware programs, intrusion prevention systems, antivirus software, intrusion detection and prevention systems, and other conventional security solutions, aim to minimize the reliance on human personnel. While they offer consistent protection, their effectiveness can fluctuate depending on the specific threat and the system's configuration. While passive defense systems may not be able to block every advanced attack, they can effectively deter a significant portion of threats and force attackers to employ more intricate and costly methods. Several established models offer guidance on implementing passive defense systems. These include the following:

- **Defense in Depth**: This approach involves layering multiple security measures to create a robust defense against cyberattacks.

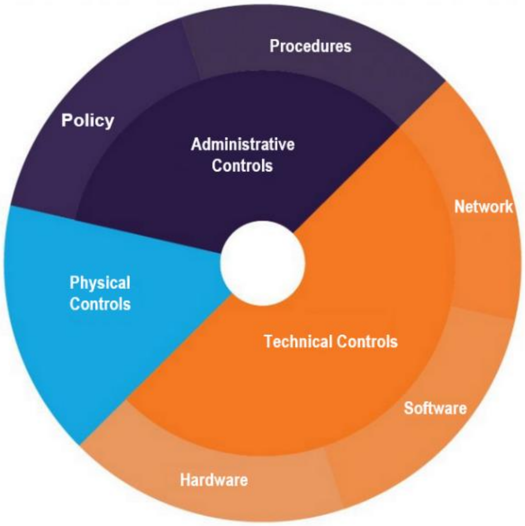


Figure 38 Defense in Depth [50]

- **NIST 800 Series**: This extensive collection of standards and guidelines covers a wide range of cybersecurity topics, including passive defenses.
- **NIST Cybersecurity Framework**: This framework provides a comprehensive approach to cybersecurity management, encompassing risk assessment, mitigation strategies, and continuous improvement.

Network Intrusion Detection Systems

Unidirectional protections are frequently employed to enable both signature-based and anomaly-based network intrusion detection systems (NIDS). These gateways replicate traffic captures from SPAN and mirror ports on ICS switches to intrusion detection sensors. Utilizing a unidirectional gateway for this function permits the IDS sensor to be safely deployed on an IT network. Connecting the IDS sensor to the IT network offers several advantages, including the ability to remotely manage the sensor from a central security operations center (SOC). This remote management capability is crucial because most IDS sensors require frequent adjustments. Deploying a unidirectionally-fed IDS on the IT network simplifies such remote adjustments for SOCs, while simultaneously safeguarding the control-critical network from potential attacks originating from the IT network.

Moreover, software assurances provided by network switch vendors regarding unidirectional communication can be compromised by unauthorized access to switch software. This could enable attackers to reconfigure SPAN or mirror ports to transmit attacks to monitored networks. Additionally, ICS networks are sensitive to changes in traffic volume, and bursts of alerts destined for a central SOC can disrupt operations. Deploying the NIDS sensor on the IT network ensures that alert traffic is isolated to the IT network, without affecting operations.

While the OT environment presents challenges for implementing passive defenses effectively, even simple measures like limiting inbound and outbound connections, requiring authentication from remote locations, and maintaining firewalls with ingress and egress filtering can prove to be highly valuable. Passive cybersecurity defenses are crucial for protecting ICS and OT systems, serving as the frontline against cyberattacks. By employing a combination of physical and logical security measures, organizations can substantially mitigate the risk of cyberattacks and safeguard their critical infrastructure from unauthorized access, data breaches, and disruptions. By adopting passive defense models, organizations can effectively enhance their cybersecurity posture and significantly minimize the threat posed by cyberattacks.

5.4.3 Active Defense

Active defense, as initially conceived in military strategy, aims to overwhelm adversaries through continuous engagement with well-coordinated teams operating from interconnected positions. In the context of cybersecurity, active defense signifies a proactive approach where security analysts proactively monitor, respond to, and learn from threats within the network.

Active defense, as defined here, is intentionally limited to internal threats to distinguish it from retaliatory cyberattacks, also known as “hack-back” strategies. Analysts engaged in active defense include incident responders, malware reverse engineers, threat analysts, network security monitoring analysts, and other security personnel who utilize their expertise and the network environment to proactively identify, investigate, and respond to threats. The emphasis on analysts rather than solely on technological tools underscores the proactive nature of active defense, mirroring the original strategy’s emphasis on adaptability and maneuverability.

The active defense phases will be meticulously detailed in the following Chapter 5.5.

5.4.4 Intelligence

One of the foundational pillars of successful active defense is the ability to effectively utilize adversary intelligence to inform security modifications, procedures, and actions within the environment. This process is often visualized as an ongoing cycle encompassing data collection, processing, and extracting insights from that data, and analyzing and synthesizing information from diverse sources to generate intelligence. The Intelligence Life Cycle serves as a structured and well-established methodology for planning and producing finished intelligence products. The Intelligence Cycle, as illustrated in the following picture, comprises five pivotal stages:

1. **Planning and Direction:** Determining the intelligence requirements and outlining the intelligence collection plan.
2. **Collection:** Gathering data from various sources, such as open-source intelligence (OSINT), network traffic analysis (NTA), and threat intelligence feeds.
3. **Processing and Exploitation:** Analyzing and transforming raw data into actionable intelligence.
4. **Analysis and Production:** Evaluating the collected intelligence against the intelligence requirements and producing tailored reports.
5. **Dissemination and Feedback:** Sharing intelligence with stakeholders and incorporating insights into decision-making processes.

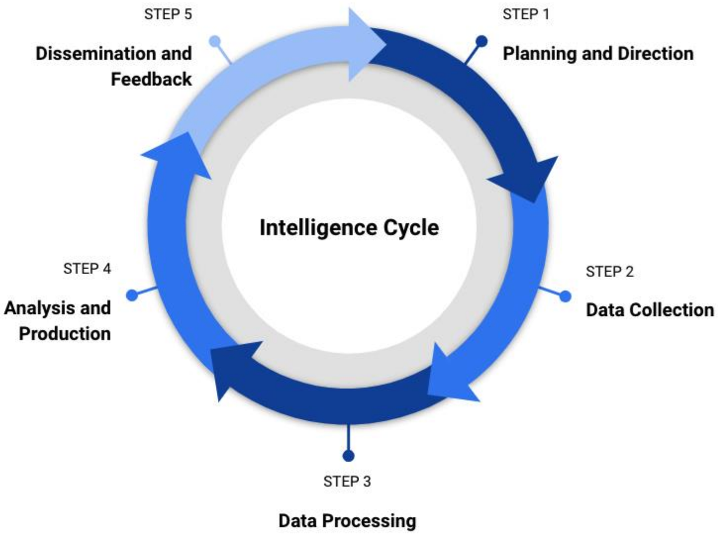


Figure 39 Intelligence Cycle [51]

While technological tools are invaluable for gathering and processing information, the human analyst plays a critical role in transforming raw data into actionable intelligence. Human analysts possess a deep understanding of the organization's operations and the adversary's modus operandi, enabling them to effectively analyze information from diverse sources, including network traffic, threat intelligence feeds, and open-source data. By integrating this data with their expertise, analysts can produce intelligence assessments that shape decision-making and guide security operations. Technology can automate tasks and provide visual representations, but it cannot replicate the human analyst's ability to critically evaluate, discern patterns, and draw meaningful conclusions.

Intelligence analysis, like solving a crime, demands a combination of critical thinking, judgment, and experience. Human analysts are the cornerstone of effective intelligence programs, and their contributions are indispensable in protecting organizations from cyberattacks.

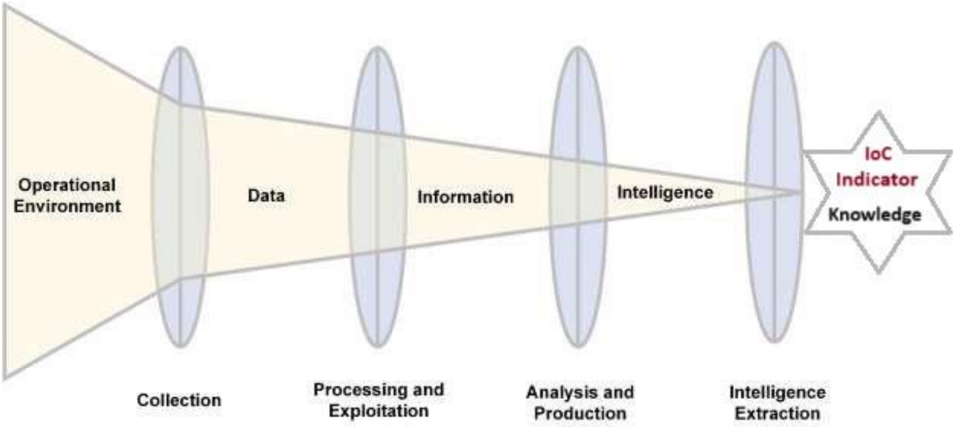


Figure 40 Relationship of Data-Information-Intelligence-Knowledge [52]

Effectively utilizing Threat Intelligence necessitates three crucial factors:

a. **Defenders must comprehend the nature and scope of their adversaries.** Security teams should clearly identify the adversaries that pose a genuine threat to their organization, considering their potential, capabilities, and intentions to harm.

b. **Defenders must be capable of translating Threat Intelligence insights into actionable measures.** Intelligence should serve as a catalyst for proactive security measures, driving changes to processes, procedures, and security controls within the organization.

c. **Defenders must distinguish between generating and consuming Threat Intelligence.** While some organizations may engage in threat intelligence collection and analysis, most rely on external sources for Threat Intelligence consumption. Understanding the distinction between these two roles is essential for effective collaboration and integration of Threat Intelligence within an organization's security posture.

Two widely recognized intelligence models offer valuable frameworks for understanding and responding to cybersecurity threats:

- ❖ **Cyber Kill Chain:** This model effectively describes the steps adversaries take to penetrate and attack defender systems. It breaks down these actions into distinct phases, providing a clear roadmap for detecting and mitigating cyberattacks. The model will be covered in the following C*hapter 4.1*.
- ❖ **Diamond Model of Intrusion Analysis:** This model focuses on analyzing the four fundamental aspects of any cyber incident: adversary, infrastructure, capability, and victim. By meticulously examining these factors, security professionals can gain a comprehensive understanding of the attack's nature, origin, and potential impact.

5.4.5 Offense

Offense, the pinnacle of the cybersecurity scale, encompasses proactive measures taken against the adversary beyond friendly networks. While offensive actions hold the potential to augment cybersecurity posture, their legal implications for civilian organizations remain a subject of ongoing debate. Offense can serve purposes beyond cybersecurity, including national policy or conflict. In the realm of cybersecurity, offensive actions are defined as lawful countermeasures and counterstrike measures directed against an adversary outside friendly systems in the context of self-defense.

The Offense phase is a powerful defense practice, but it should be implemented cautiously. It requires significant expertise and resources, and some methods, like hack back operations, raise significant legal and ethical concerns. However, when used strategically, Offense can disrupt attacker activities, gather valuable intelligence, and ultimately strengthen your overall cybersecurity posture.

Industrial organizations worldwide face a growing threat from cyberattacks. While many have adopted defensive technologies and practices, these passive measures may not be sufficient to deter advanced, targeted attacks. To effectively safeguard their operations, industrial organizations must implement an active defense program informed by actionable intelligence.

5.5 Active Defense In-Depth

Active cybersecurity measures can be effectively employed when organizations have established robust architecture, passive defenses, and a detailed asset inventory. Active defense becomes necessary when adversaries manage to penetrate these initial layers of protection. Effective active defense strategies build upon a foundation of strong cybersecurity architecture, followed by passive defenses and a meticulously maintained asset inventory. Given attackers only need to succeed once, while defenders must constantly protect against everything, adversaries are likely to breach an organization's defenses eventually. Tools that incorporate threat intelligence can aid analysts in detecting and locating cyber intrusions. Incident response (IR) teams utilize various tools to hinder and deter attackers' progress. Some common IR tools include white worms, honeypots, and address hopping.

At its core, Active Cyber Defense (ACD) involves a direct confrontation between the defender's expertise and the adversary's skills. Effective ACD implementation requires a foundation of well-defined, defendable system architecture, functioning passive perimeter defenses, and skilled defenders capable of engaging the adversary effectively. These prerequisites can introduce additional costs for organizations seeking to adopt ACD.

Active defense empowers security personnel to proactively monitor an organization's infrastructure, identify and neutralize threats internally before they disrupt operations. It is crucial to emphasize that active defense does not involve accessing or impacting adversary networks.

The pinnacle of ICS security best practices lies in implementing and sustaining the ICS Active Cyber Defense Cycle (ACDC), a repeatable process driven by skilled cyber defenders with expertise in both cybersecurity and process engineering. This cycle effectively safeguards control systems by securing, maintaining, monitoring, and responding to threats.

The ACDC has proven to be a successful strategy for active defense ICS environments, both within and outside of government sectors. Its four interconnected phases work in tandem to maintain security, contributing to the safety and reliability of operations. Effective protection of industrial networks from cyber threats can be achieved through the adoption and implementation of the ICS ACDC.

- ✓ **Understand:** Gain a comprehensive understanding of the OT network's topology to effectively monitor for irregularities and potential intrusions.
- ✓ **Detect:** Proactively identify genuine threats and initiate an incident response process to assess the extent of the infection, contain its spread, and eradicate the threat while maintaining business continuity.
- ✓ **Contain:** Interact with the threat in a secure environment, utilizing specialized skills such as malware analysis to gather insights and recommend necessary modifications to logical or physical infrastructure for enhanced security.
- ✓ **Collect:** Throughout the entire cycle, gather information about the threat and combine it with external threat intelligence to continuously improve the security posture.

The ICS ACDC is an iterative process that fosters continuous improvement in cybersecurity posture. It encourages security professionals to view security as an ongoing process and to constantly learn, adapt, and collaborate to protect industrial networks effectively. ACDC consists of *five* phases that work together to maintain security, contributing to the safety and reliability of operations.

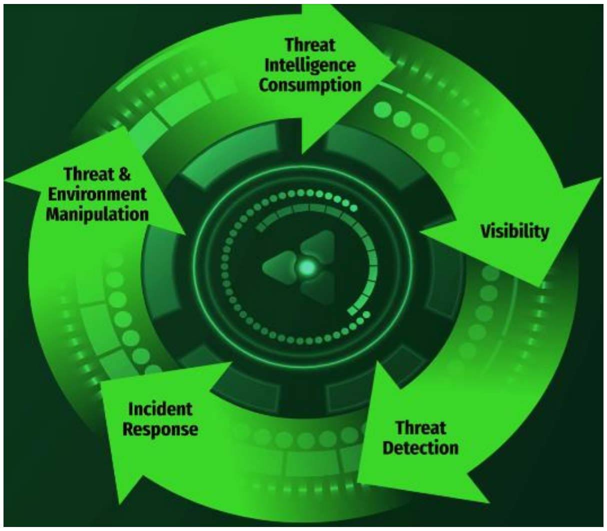

Threat Intelligence Consumption
Visibility
Threat Detection
Incident Response
Threat & Environment Manipulation

Figure 41 Active Cyber Defense Cycle (ACDC) [53]

5.5.1 Threat Intelligence Consumption

Cyber threat intelligence is a powerful tool that arms security professionals with comprehensive and actionable information about threats and attackers. This empowers them to detect, assess, and even prevent similar attacks.

The threat profile of an OT environment varies depending on factors such as organization size, critical infrastructure sector, geographic location, geopolitical landscape, adversary motivations, and evolving attack techniques.

In the context of proportionate prevention and response, threat intelligence serves as a crucial element for prioritizing proactive measures and informed decision-making, enabling cost-effective mitigation of cybersecurity risks.

Organizations frequently encounter difficulties with threat intelligence when they obtain external information that fails to address their specific organization or systems. Often, the “intelligence” provided is merely a data feed, lacking the context and actionable insights that true threat intelligence should offer. Intelligence is a formalized process and product, not just information. A threat, by definition, possesses the capability, intent, and opportunity to cause harm to an organization.

For example, despite the widespread attention and exploitation of the Heartbleed vulnerability, it was not considered a threat to every organization. For organizations that did not have the affected versions of OpenSSL installed, the vulnerability could not be exploited, thereby eliminating the opportunity for harm. Hence, the vulnerability itself did not pose a threat to those organizations unless they possessed the specific vulnerability.

During the Threat Intelligence Consumption phase, analysts meticulously evaluate the organization’s environment, mission, and threat landscape. This comprehensive understanding enables them to identify and prioritize relevant threat intelligence sources, both internal and external. This crucial information is then disseminated to other ACDC team members, particularly those engaged in network security monitoring, to enhance their threat detection capabilities.

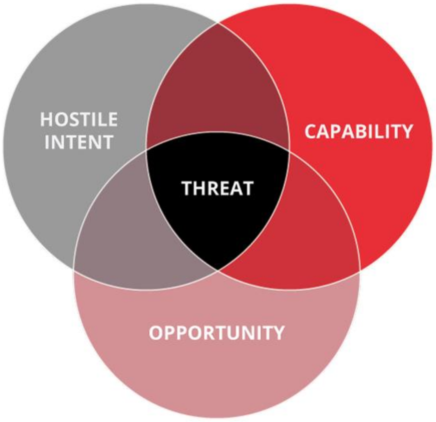


Figure 42 Threat Triangle [54]

Organizations increasingly employ cyber threat intelligence (CTI) to proactively enhance their security posture and make informed strategic decisions. Actionable CTI provides detailed insights into adversary TTPs, enabling defenders to identify and mitigate potential threats effectively. Sector-specific CTI offers particularly valuable context for tailoring security measures to the unique threat landscape of critical infrastructure organizations.

Technical threat intelligence encompasses indicators of compromise (IoCs), such as malicious IP addresses, file hashes, and other technical signatures associated with ongoing attack campaigns. Security analysts utilize IoCs to assess the scope of a compromise, identify affected devices and systems, and deploy security controls to detect and alert for these indicators. However, IoCs have inherent limitations, as adversaries can rapidly modify their TTPs, rendering specific IoCs obsolete.

To achieve enduring security, ICS security teams should prioritize identifying and leveraging TTPs rather than relying solely on IoCs. Understanding adversary methodologies enables defenders to anticipate and prepare for potential attack vectors, extending the effectiveness of their security posture.

CTI gathers information from various sources, including hardware and software vulnerability advisories, STIX/TAXII feeds, in-depth cyber threat reports, malware analysis reports, and publicly documented TTPs used in real-world attacks. Additionally, security advisories issued by leading ICS vendors, provide valuable insights into adversary methodologies and potential vulnerabilities.

Threat intelligence by nature relies on sharing information insights into current, evolving, and emerging threats.

5.5.2 Visibility and Asset Identification

Enhance OT cybersecurity by achieving comprehensive visibility. Obtain a comprehensive asset inventory, establish a passive network monitoring capability, and leverage tools capable of dissecting and interpreting industrial protocols within network traffic streams.

Asset Identification and Network Security Monitoring (NSM) personnel are tasked with identifying network changes that provide insights into the organization’s environment. While network architects maintain baseline network topology maps, these baselines are subject to constant change, making NSM personnel to be the best equipped to detect these alterations promptly. Identifying changes in the environment facilitates timely feedback to Threat Intelligence Consumption personnel, enabling them to assess potential shifts in the threat landscape.

NSM personnel utilize threat intelligence processed by Threat Intelligence Consumption personnel, including Indicators of Compromise (IoCs) and TTPs, to identify and assess potential threats. Upon identification, they determine whether the threat poses a genuine risk to the organization and meets the established threshold for initiating incident response.

There are four principal methodologies to perform Asset Identification: Physical Inspection, Passive Scanning, Active Scanning, and Configuration Analysis, as shown in the Figure 44.

i. Physical Inspection

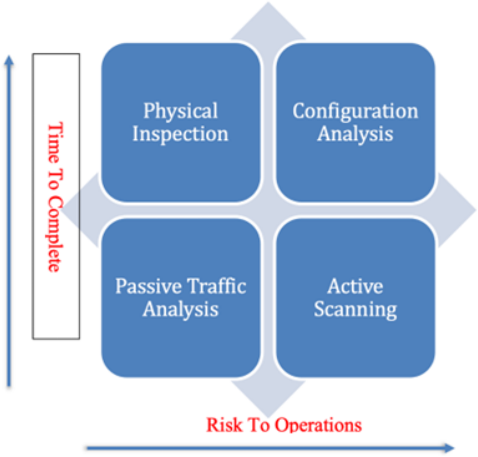


Figure 43 Methods of ICS Asset Identification, Risk vs Time [55]

Physical inspection of assets can be a time-consuming and challenging process in large, geographically separated networks. It can also be hazardous in certain areas. Despite these limitations, it is crucial to understand how to perform physical inspections, identify assets, and trace fiber optic cables throughout a facility to determine network connectivity. Physical inspection may not be the most efficient method for asset identification, but it can be valuable in specific scenarios. For instance, in mesh or star topology networks, devices often overlap. By identifying central points, such as core routers, and tracing fiber optic cables in a hierarchical manner, that can effectively identify devices and their connections.

ii. Traffic Analysis (Passive Scanning)

Passive scanning, also known as traffic analysis, provides a rapid and secure method for examining network communications. Unlike traditional asset inventory methods, passive scanning delves deeper into system interactions, enabling the analysis of protocols and communication patterns. This granular insight not only enhances asset identification but also expands threat detection capabilities. Traffic analysis plays a pivotal role in root cause analysis, allowing for the differentiation of technical faults from security breaches. The revision streamlines the language and enhances the formality of the writing style. It also clarifies the benefits of traffic analysis for both asset identification and threat detection.

iii. Active Scanning

While passive scanning can uncover similar insights to those obtained through active scanning, it relies on network traffic to gather information, which can be time-consuming and may not always yield complete data. Active scanning, in contrast, directly interacts with devices to retrieve specific details, making it the preferred method when detailed information is urgently needed. This approach effectively generates an inventory but lacks the capability to analyze communication patterns between devices.

Active scanning methodologies exhibit a wide range of risk profiles, varying from highly hazardous to relatively safe depending on the operational environment. While active scanning offers the fastest asset identification capabilities and often provides more comprehensive asset inventory information, it may not generate an updated network topology or communications schema due to security restrictions. This method effectively identifies assets but lacks the capability to analyze device communication patterns.

Active scanning tools are best utilized for periodic assessment purposes rather than continuous operation or permanent deployment. It is advisable to test active scanning tools in a controlled lab environment before employing them in production, ensuring operational oversight during non-critical periods such as maintenance windows.

iv. **Configuration File Analysis**

Configuration files serve as valuable verification tools for confirming the presence of assets connected to the network. They can be cross-referenced with engineering documents and network designs to establish a baseline representation of the intended network topology. This information complements other asset identification methods, providing a comprehensive picture of the network's configuration.

Gathering configuration files (e.g., ARP tables, firewall configurations) from network devices, particularly central points, such as routers or managed switches, efficiently identifies registered devices on the network, including unauthorized devices and passive sniffers.

5.5.3 Threat Detection

Effective threat detection relies on advanced technology capable of analyzing large data sets and identifying malicious patterns that may indicate attempted attacks or unauthorized access. Network security defenders can effectively detect threats by analyzing deviations from a baseline of normal network activity. Traditional security systems, such as intrusion detection systems (IDS) and log aggregation tools, generate valuable alert data that can be correlated to identify anomalous behavior indicative of potential intrusions. For instance, a series of failed login attempts on a human-machine interface (HMI) followed by IDS alerts on another network segment might suggest an adversary's presence.

However, it is crucial to mitigate false positives, which are instances where potential threats are detected but prove to be non-malicious. False positives can overwhelm defenders with unnecessary alerts, diverting attention away from genuine threats. Therefore, thorough analysis of detected threats is essential to ensure that resources are not wasted on inconsequential events. This analysis involves validating the legitimacy of threat indicators, discarding false positives, and prioritizing true positives that represent genuine security incidents. Upon identifying a true positive, network security monitoring personnel initiate the incident response process.

In the realm of IT security, the primary objective of threat detection is often to block suspicious activity. While false positives can cause inconvenience, the worst-case scenario typically involves unauthorized access or data compromise. Therefore, IT security systems aim for high accuracy while balancing the need for real-time protection with the risk of false positives. This dual-pronged approach serves two distinct purposes: incident investigation and immediate blocking.

In contrast, threat detection in ICS security prioritizes thorough investigation and subsequent actions rather than immediate blocking. The inherent safety and reliability constraints of ICS systems demand a more cautious approach. While detecting and blocking malicious activity is essential, the potential consequences of doing so, such as disrupting critical processes or compromising reliability, must be carefully weighed. Antivirus solutions, for instance, may inadvertently cause safety or reliability issues if they detect and block malware that is essential for the system's operation.

Therefore, the primary goal of threat detection in ICS security lies not only in immediate blocking but in facilitating comprehensive investigation and informed response actions. This approach ensures that security measures are aligned with the specific needs and constraints of ICS environments, prioritizing safety, and reliability while effectively mitigating cybersecurity risks. The are four types of threat detection: *configuration analysis, modeling, indicators, and behavior analytics.*

- *Configuration Analysis:* is an environmental-based approach that identifies changes to a system or network. Examining changes to configuration parameters, such as a PLC's mode switch from RUN to PRGRM, can provide valuable forensic insights. However, configuration analysis alone lacks the contextual information necessary to determine whether a change is malicious or benign. Integrating threat context into configuration analysis elevates it to a threat behavior detection approach.
- *Modeling:* is an evolutionary approach to configuration analysis that utilizes mathematical models, such as machine learning techniques, to develop a baseline profile of the environment. This approach involves analyzing historical data to identify patterns and acceptable deviations in configuration changes. For instance, a machine learning model might determine that Function Code 121 is typically used less frequently but is acceptable within a specified threshold, such as five times within a 24-hour period. Threat modeling focuses on identifying and assessing potential attack scenarios that are specific to the organization's OT environment. By understanding the unique characteristics and vulnerabilities of their OT network, organizations can prioritize their mitigation efforts and implement targeted security measures. While modeling excels at detecting anomalies in the environment, it requires continuous data feeds and updates to maintain its effectiveness. Additionally, modeling alone does not provide contextual information about potential threats, leaving analysts with contextless alerts that may be difficult to interpret and prioritize.
- *Indicators:* Indicator-based detection methods focus on identifying specific elements of adversary activity, such as the digital hash of a piece of malware. While indicators provide the most contextual information when utilized correctly, they often become ineffective when applied too broadly. Adversaries regularly modify the atomic elements of their intrusions and malware, rendering indicator-based approaches reliant on a continuous influx of updated indicators. The key to effective indicator-based detection lies in identifying patterns that directly correlate to adversary capabilities or infrastructure. This extends beyond IP addresses and malware, encompassing unique file paths created by adversaries during their malicious actions. For instance, if an adversary establishes a file path that deviates from the system's native directory structure, it serves as a valuable indicator. The distinguishing characteristic is the deviation from the norm. Indicator-based detection, like other approaches, can generate both true and false positives.
- *Threat Behavior:* are the evolution of indicators, by moving beyond identifying specific attributes to capturing adversary TTPs. Instead of focusing on individual elements like VPN IP addresses, file hashes, or specific commands, threat behavior analytics detect patterns that represent adversary tradecraft. This approach provides valuable context for defenders without being tied to specific details. For instance, instead of relying on a multitude of indicators to detect DNS exfiltration from an HMI, a threat behavior analytic would alert whenever a user leverages a VPN to access an HMI, drops a new file, and then sends commands to an RTU (Remote Terminal Unit). This tradecraft-focused approach enables threat behavior analytics to scale across different attack types and even adversary groups. For example, rather than creating an endless list of indicators for "DNS exfiltration from an HMI", a single threat behavior analytic can effectively detect this activity regardless of the adversary's tactics or tools. For instance, if an adversary introduces a new file onto a system, establishes a connection to an unfamiliar IP

address, and then initiates scans for OPC (Open Platform Communications) communications, this sequence of actions could constitute a threat behavior.

This approach does not hinge on identifying the specific file or IP address involved; rather, it aims to detect a combination of events, namely "new file" + "new external IP address" + "OPC Scanning," occurring within a specific timeframe. This pattern would effectively represent the HAVEX behavior. Threat behavior analytics do not produce true or false positives because they do not target specific malware or adversaries – "this detection alerts on HAVEX". Instead, they identify behaviors that are associated with malicious activities – *"this detection alerts on behaviors leverages by HAVEX".* This approach raises alerts for behaviors that may not always be indicative of a threat, but they warrant further investigation due to their potential malicious implications. Threat behavior analytics do not claim to provide definitive conclusions about the legitimacy of detected behavior; rather, they act as a trigger for deeper analysis.

HAVEX (Remote Access Trojan-RAT, discovered 2013), was specifically designed to target ICS. It possesses various capabilities, including scanning networks for specific industrial protocols and leveraging OPC (OLE for Process Control) to directly gather and exfiltrate information to internet-connected servers accessible by attackers. It was primarily used for espionage, by targeting thousands of companies across critical sectors like defense, energy, aviation, and petrochemicals in North America and Europe. The information gathered could be utilized for future attacks or ongoing espionage efforts.

5.5.3.1 Network Security Monitoring (NSM)

Threat detection is the primary function of security monitoring, safeguarding critical OT environments by preventing security breaches and maintaining a secure posture. Organizations are mandated to implement documented processes that adhere to security event monitoring specifications. Compliance mandates logging security events and generating alerts for events deemed critical. These include malicious code detection and failed events (e.g., failed login attempts).

Proactive security defenders employ network monitoring to identify malicious activity, utilizing deviations from normal network behavior as indicators. NSM draws upon a comprehensive understanding of the network and its assets to detect anomalies over time. Spikes in bandwidth utilization, new devices on the network, communications with anomalous IP addresses, and elevated firewall/IDS alerts require investigation. NSM, as a continuous process, gathers, identifies, and analyzes threat indicators to facilitate timely responses. By integrating threat intelligence, NSM proactively detects threats before they gain network access.

Proactive data collection from ICS networks is crucial for effective security. The process may initially be challenging, but it becomes sustainable once established. Logging from field devices, though often disabled, provides valuable insights when enabled and centralized. The small and stable nature of ICS networks compared to IT networks facilitates data collection and analysis, enhancing the defender's ability to detect and mitigate threats.

At the implementation level, security monitoring involves using devices and tools to monitor and report on network or device security issues. NIST defines three crucial aspects of continuous security monitoring: vulnerability monitoring, application monitoring, and threat monitoring. By integrating these monitoring activities, OT security administrators achieve comprehensive situational awareness, enabling them to proactively identify and mitigate security threats. There are generally two categories of tools associated with these activities:

- *Proactive tools:* such as IDSs and SIEMs, provide continuous vigilance over network devices and their security states. By identifying and alerting on misconfigurations, software defects, hardware failures, anomalous network traffic, and unexpected protocols, these tools empower ICS security administrators to proactively address vulnerabilities, collaborate with vendors, and strengthen network security.

- *Detective tools:* enable proactive threat detection and response. These tools collect and analyze network data to identify and alert on malicious activity in real-time, including zero-day malware, command and control traffic, and data exfiltration. OT security administrators can leverage these tools to combat advanced threats effectively.

NSM is not merely about intrusion detection; it encompasses comprehensive monitoring of the ICS network, detecting a wide range of issues from misconfigurations to policy violations. By identifying and addressing these issues preemptively, NSM provides two major advantages:

NSM promotes operational efficiency by:

- Expediting system validation and restoration to a stable operational state
- Minimizing troubleshooting time and effort
- Preventing configuration errors and deviations from established procedures, ensuring seamless operations and process integrity

NSM enhances system optimization by:

- Refining segregation and enforcement zones for control networks
- Quickly generating and validating firewall rules
- Eliminating (thereby hardening) non-required ports and services and characterizing changes in system communications.

5.5.3.2 North/South vs East/West Traffic Analysis

North-South traffic describes network traffic that originates from or terminates within the organization’s internal network, while East-West traffic refers to data flow between servers within a data center or across different cloud environments. Unlike North-South traffic, which involves ingress and egress data movement, East-West traffic represents the lateral transfer of data within the network infrastructure.

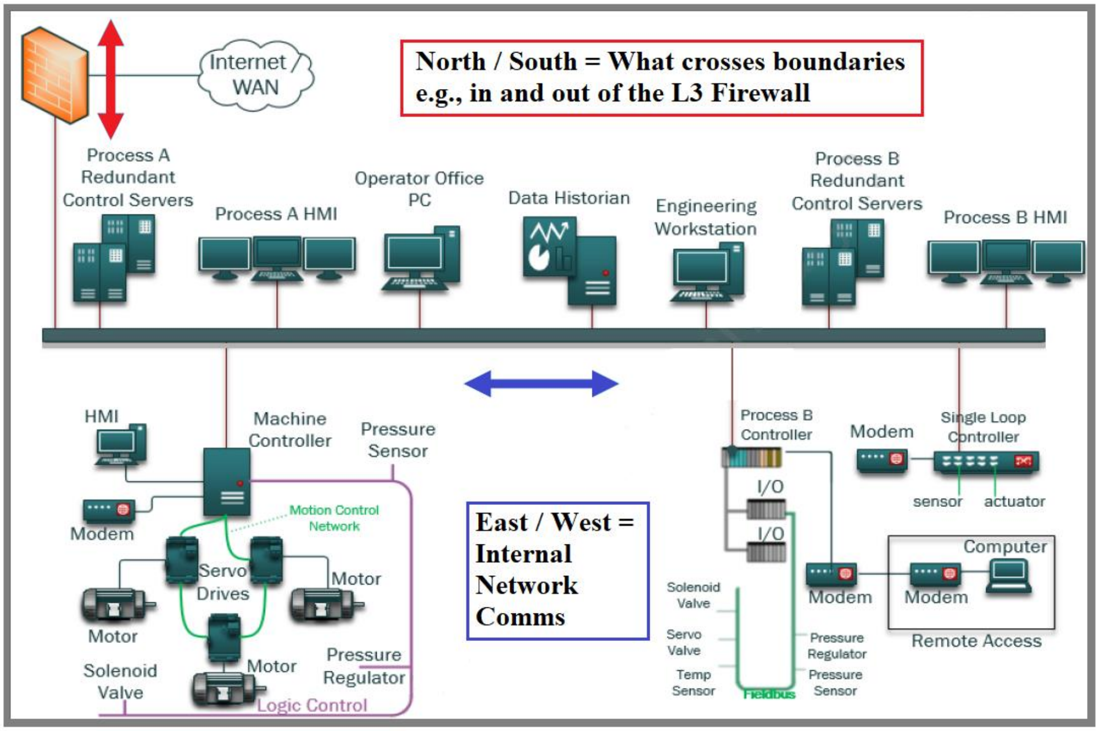


Figure 44 Traffic Analysis, SANS ICS

Placing detection tools outside the ICS network’s perimeter, while advantageous for certain aspects (such as indicator checking cross-site traffic, identifying the type of connections going in and out of operations site), it overlooks a substantial portion of ICS-related traffic, particularly those obscured by OEM/integrator VPN encryption. A more comprehensive approach entails deploying detection tools within the ICS network, enabling visibility into both north-south and east-west traffic communication patterns. Effective east-west traffic analysis necessitates establishing trust with operational personnel. Deployment in a purely passive mode, without interfering with communications or introducing preventive measures, is highly recommended. This configuration enables comprehensive visibility into ICS communications, facilitating asset identification and vulnerability assessment. More significantly, it provides the ability to detect critical adversary actions such as lateral movement, logic manipulation, and control exploitation.

5.5.4 Incident Response

During the Incident Response (IR) phase, security personnel focus on identifying the full extent of the intrusion and implementing procedures to contain and eliminate the threat. Threat intelligence gathered during the previous phases plays a crucial role in this process. IOCs, such as registry key modifications, file presence, or identified abnormalities, can be quickly identified, and analyzed with the aid of threat intelligence. This significantly reduces the time required to fully assess the threat and accelerate containment efforts. IR personnel also assume the responsibility of collecting information or samples of the threat, especially if it involves malware. This data is essential for further analysis and understanding of the attack, enabling defenders to develop more effective countermeasures.

Incident Response (IR) is a structured approach to effectively handling and managing the aftermath of a security incident. Incidents, as defined by each organization, typically encompass security breaches, intrusions, or loss of visibility/control in an ICS environment. Incident declaration is solely authorized by a designated individual with the appropriate level of authority.

While the primary goal of IR is to restore the network to its pre-incident state, it is not always an immediate objective. Instead, IR focuses on implementing a structured and organized response plan to address the incident and ensure the continued safe operation of ICS systems. Effective incident response necessitates the ability to swiftly triage situations and adapt incident response procedures to the specific context of control systems, while prioritizing safety and system integrity.

There are various techniques and guides for helping to establish incident response practices, teams, and methodologies, but they mostly focus on IT. The ICS incident response landscape is relatively young, and the limited available information tends to be high-level guidance or closely guarded tradecraft. Nevertheless, it is crucial to examine the IT incident response lifecycle and steps to identify applicable practices and adapt them to the unique demands of ICS systems.

The National Institute of Standards and Technology (NIST) developed a Computer Security Incident Handling Guide (SP 800-61 Rev2) [56], which provides guidance to security personnel in developing an incident response procedure. In the electrical generating and distribution market, NERC CIP 008-06 [57], “Incident Reporting and Response Planning” provides guidance for BES (Bulk Electric System) operations to generate incident handling procedures for cybersecurity incidents. The guidelines include establishing roles and responsibilities for cybersecurity incident response teams and individuals. It also specifies requirements for incident handling procedures.

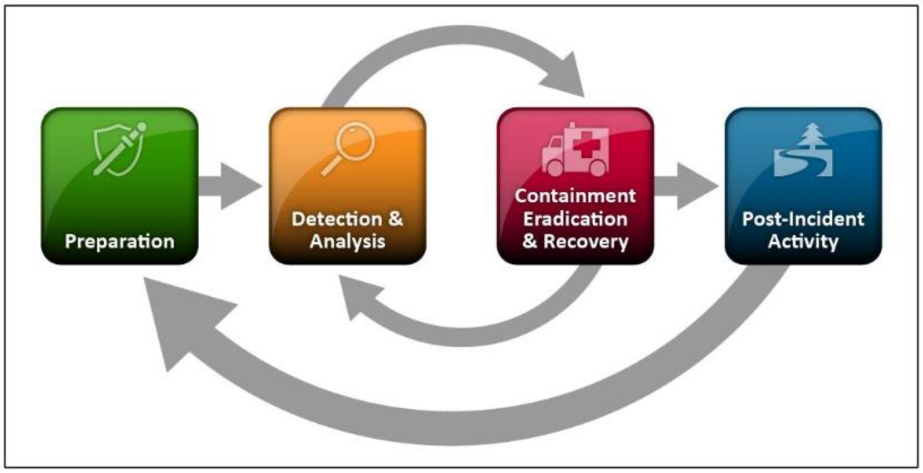


Figure 45 The Incident Response Lifecycle [50]

In general, the major priorities of Incident Response in ICS environment are:

- Maintain safe and reliable operations
- Acquire meaningful forensic data
- Perform timely analysis
- Contain and eradicate threats

Efforts to effectively address ICS incident response face significant challenges. Limited publicly available practices and a lack of case studies hinder progress. Legacy devices with rudimentary logging capabilities and incompatible tools further complicate incident response. Additionally, preparedness often falls by the wayside due to budgetary constraints and operational priorities. Finally, the use of undocumented and proprietary operating systems and protocols adds another layer of complexity. Obscurity, rather than transparency, is not a reliable security strategy.

5.5.5 Threat and Environment Manipulation

To make industrial control systems (ICS) less attractive to attackers, defenders must have the ability to adapt and modify either the threat itself or the ICS environment. This includes countering malware capabilities, disrupting malicious human actions, and modifying legitimate software or protocols to mitigate potential vulnerabilities.

Efforts to manipulate threats and environments generate valuable information that can be used to identify and categorize indicators of compromise (IOCs) and attack TTPs. This information can then be fed back into the threat intelligence consumption phase, allowing defenders to refine their strategies and continuously improve their security posture.

The ACDC cycle encourages organizations to learn from their past experiences and document their knowledge to enhance organizational resilience. This approach ensures that even when personnel turnover occurs, the organization’s collective cybersecurity expertise remains intact. As a result, organizations can effectively identify and respond to emerging threats in a timely manner.

Manipulating threats can yield valuable insights for network security monitoring (NSM) and incident response (IR). This information can be shared with other organizations to enhance cybersecurity collaboration and threat intelligence sharing. Additionally, identifying weaknesses in the threat, such as hardcoded IP addresses/passwords or automated scanning mechanisms, can be leveraged to neutralize the threat effectively.

Attribution of attacks is often challenging due to the use of automated features in destructive malware. While attribution is not a primary goal of ACDC, the gathered information can be employed for attribution attempts outside of the ACDC, particularly in cases involving national-level malware. Attribution is less relevant for network defense but can be crucial for political impact, national-level responses, and board-level decision-making.

Effective analysis of threats within the ACDC framework necessitates that defenders work with malware in a controlled environment. A safe working environment is paramount to ensure the protection of sensitive data and systems. Manipulation of threats in a production network is strongly discouraged due to the potential of triggering hidden routines within the malware, such as self-destruction or data-destruction. Incorrectly handling malware can also alert adversaries of defenders’ presence, potentially prompting them to modify their tactics. To prevent unauthorized communication, malware should not be allowed to establish connections to active internet resources.

The automated nature of malware makes it a particularly attractive target for manipulation within ICS environments. By analyzing and understanding the malware’s routines, deactivation commands, or weaknesses, defenders can gain insights into its capabilities and potentially neutralize its threat.

Identifying vulnerabilities in the malware relies on pre-gathered intelligence that can provide an opportunity to modify the environment, effectively disrupting the malware’s operations and preventing it from causing harm. Environmental manipulation can involve both logical and physical changes, such as deploying honeypots or altering hardcoded system passwords.

Careful planning is essential when implementing environmental changes. Erroneous alterations can confuse operators, disrupt system processes, and even trigger warranty or support issues. During an incident response scenario, incident responders should actively participate in planning environmental changes to ensure they do not hinder their operations or investigations.

Environmental manipulation should not be considered a primary defense strategy but rather a tool to complement other cybersecurity measures. It is crucial to prioritize the protection of critical assets and maintain system integrity while implementing environmental modifications.

6 Beyond Traditional Security: Leveraging Cutting-edge technologies

State of the Art in cybersecurity applied to critical infrastructures, is still evolving but traditional security technologies and practices are not enough to protect these environments from advanced threats. Critical infrastructure operators need to adopt a more holistic approach to security that includes the use of Cloud Computing, AI, Blockchain, Digital Twins, and ICS Honeypots. As the cyber threat landscape continues to evolve, new and innovative technologies will be needed to protect ICS/OT systems. Organizations that are proactive in adopting new security measures will be better able to protect themselves from cyberattacks.

6.1 Cloud Computing and IIoT

Cloud computing has become so deeply embedded in modern digital and internet infrastructure that its pervasiveness often goes unnoticed. Its substantial benefits – cost savings, scalability, and the outsourcing of infrastructure security and availability – have led to a rapid adoption. However, the overwhelming focus on these benefits has resulted in a policy gap, where the criticality of cloud computing to the functioning of essential systems and the need for commensurate oversight structures have not been adequately addressed.

6.1.1 Benefits

Cloud computing offers a plethora of benefits for the cybersecurity of critical infrastructure systems, making it a compelling choice for organizations seeking enhanced protection and resilience.

1. **Shared security resources:** cloud providers invest heavily in advanced security measures, including multi-layered security, intrusion detection and prevention systems, and vulnerability scanning, often exceeding the resources available to individual organizations. This security expertise provides critical infrastructure systems with a robust defense against evolving cyber threats.
2. **Scalability and elasticity:** cloud infrastructure's scalability and elasticity ensure that critical infrastructure can adapt seamlessly to fluctuating demands without compromising security. Organizations can easily scale up or down computing resources based on real-time needs, ensuring that critical systems have the necessary bandwidth and performance to handle peak usage periods without compromising security posture.
3. **Remote access and management:** cloud-based systems enable remote access and management, enabling organizations to monitor and maintain critical infrastructure from anywhere in the world, even when physically distant from the systems. This remote accessibility simplifies troubleshooting, facilitates proactive maintenance, and expedites incident response in case of security breaches.
4. **Backup and disaster recovery:** cloud providers offer robust backup and disaster recovery services, safeguarded from potential system outages or disasters. Critical data is continuously backed up and stored in secure locations, ensuring that organizations can swiftly restore operations in the event of disruptions. This backup capability protects against data loss, minimizes downtime, and safeguard continuity of critical services.
5. **Compliance and regulatory support:** cloud providers often adhere to strict compliance and regulatory standards, such as ISO 27001, PCI DSS, and HIPAA. By adopting cloud solutions, organizations gain access to a robust compliance framework, demonstrating their commitment to data security and protecting themselves from potential legal liabilities. This adherence to industry standards instills confidence in data confidentiality, integrity, and availability, particularly for organizations handling sensitive information.

6. **Managed security services:** cloud providers offer managed security services, offloading the responsibility for security tasks such as monitoring (SOC) services, vulnerability management, incident response, and penetration testing to experienced security professionals. This outsourcing of security responsibilities frees up internal resources to focus on core business operations, while ensuring that critical infrastructure is under the experts watchful eye.
7. **Security as a Service (SaaS) offerings:** cloud providers provide a variety of Security as a Service (SaaS) offerings, integrated directly into cloud-based critical infrastructure systems. These SaaS-based solutions enhance protection against emerging threats, reducing the need for organizations to maintain and update their own security infrastructure. This combination of cloud-based security expertise and SaaS offerings provides a comprehensive defense against a wide range of cybersecurity threats.

In conclusion, cloud computing offers a compelling solution for enhancing the cybersecurity of critical infrastructure systems. By leveraging the shared security resources, scalability and elasticity, remote access and management, backup and disaster recovery, compliance and regulatory support, managed security services, and SaaS-based security offerings, organizations can safeguard critical infrastructure from evolving cyber threats, ensuring the resilience and operability of essential services.

While cloud computing can offer significant security benefits, it is crucial to carefully evaluate cloud providers and select one that has a strong track record of security, compliance, and customer support. Organizations should also implement additional security measures, such as multi-factor authentication, strong password policies, and regular vulnerability scans, to further protect their critical infrastructure in the cloud.

6.1.2 Risks-Challenges

The cloud, just like its on-premises predecessors, faces risks. The Cyber Statecraft Initiative at the Atlantic Council's report [58] explores emerging risks associated with critical infrastructure organizations leveraging new cloud services and offerings. This report highlights the potential risks posed to critical infrastructure (CI) by cloud compromises or outages. It acknowledges the benefits of cloud computing but argues that existing policy tools are not sufficient to address these new risks. The report recommends that sector risk management agencies (SRMAs) (like the Department of Homeland Security, the Environmental Protection Agency, the Department of Energy and more) establish cloud management offices to oversee cloud adoption and security. It also emphasizes the need for organizations to systematically assess their cloud computing adoption and implement best practices when working with Cloud Service Providers (CSPs). It also encourages the Cybersecurity and Infrastructure Agency (CISA) to support the use of established frameworks for secure cloud integrations.

Moreover, this report highlights two key cloud security risks: increased dependence, limited control, and visibility. Dependency risk arises when the use of multiple cloud services, create an increasingly complex infrastructure that potentially amplifies the threat of security breaches. The second risk factor, delegated control, and visibility, describes how organizations lose control and visibility over their cloud infrastructure, making it difficult to manage security risks. The Atlantic Council's report concludes that existing policy tools are not equipped to manage these new risk factors. It recommends that policy structures should be developed to provide greater visibility into cloud usage and risk, and that Sector Risk Management Agencies (SRMAs) also should be equipped with appropriate tools to manage cloud risks within their sectors. The report also calls for a cross-sector cloud risk management structure to facilitate greater transparency and oversight. These recommendations are a starting point for developing a comprehensive cloud risk management policy.

Visibility into cloud usage and risk is essential for effective risk management, but additional tools will be needed to fully address the challenges posed by cloud computing.

In addition to the report's research and the categorized risk factors, some extra potential risks associated with cloud computing for critical infrastructure cybersecurity could involve the following:

1. **Vendor lock-in:** Organizations that rely on cloud providers may become locked into a particular vendor, making it difficult and expensive to switch to another provider if the need arises. This lock-in can make it difficult for organizations to control their own data and systems.
2. **Shared responsibility model:** With cloud computing, there is a shared responsibility model for security. The cloud provider is responsible for the security of the cloud infrastructure, while the organization is responsible for the security of its data and applications. This shared responsibility model can be complex and confusing, and it can be difficult to ensure that all parties are meeting their obligations.
3. **Data location and sovereignty:** Organizations that store data in the cloud need to be aware of where their data is stored and how it is protected. In some cases, data may be stored in jurisdictions with different data privacy laws and regulations. This can raise concerns about data sovereignty and the ability to comply with local laws.
4. **Advanced persistent threats (APTs):** APTs are highly sophisticated cyberattacks that often target critical infrastructure. Cloud computing can provide an additional attack surface for APTs, as it provides a new way for attackers to gain access into critical systems.

Recurring incidents like the SolarWinds hack [59], where Russian government-affiliated hackers exploited Microsoft Azure's IAM services, demonstrate a growing trend of cloud attacks. This trend is exemplified by the recent breach of Microsoft's Azure e-mail cloud system by Chinese hackers [60], impacting approximately 25 organizations, including government agencies and their associated consumer accounts.

Despite these risks, cloud computing can still be a valuable tool for improving the cybersecurity of critical infrastructure systems. Organizations that adopt cloud computing should carefully consider the risks and take steps to mitigate them. This may include using a multi-cloud approach, implementing strong access controls, and encrypting data.

Secure IIoT and Cloud Communications

The dynamic evolution of cloud-related technologies is giving rise to the concept of edge computing, where computation and data analysis are decentralized to devices closer to the data origin. This trend introduces intricate interdependencies between the cloud, edge devices, telecommunications infrastructure, and distributed storage technologies, hindering the clear delineation of this sector for critical infrastructure designation.

The Industrial Internet of Things (IIoT) facilitates enhanced connectivity of control-critical cyber assets, often termed "edge devices," enabling:

- Real-time data transfer from edge devices at industrial sites to cloud-based platforms for "big data analysis"
- Automatic firmware updates for edge devices to enhance security and functionality
- Information/attack flows returning to edge devices to control the devices and/or physical infrastructure

The OT sites, in their endeavor to safeguard communications, have two primary strategies to respond to the emerging demands and requirements:

- Non-controllable edge devices, primarily used for monitoring purposes, can be isolated on their own dedicated networks. These networks may be directly or wirelessly connected to the IT network at the plant or indirectly linked to cellular or internet networks. For sites with such hybrid networks, meticulous and prominent labeling of IT and ICS cabling and communication components is crucial to prevent inadvertent cross-connections at the site.
- Control-critical edge devices, which directly influence physical processes, must be deployed and managed adhering to the established best practices for securing OT sites. These devices may be situated on a primary ICS network, forming part of a group of interconnected control-critical ICS networks, or reside independently on a dedicated control network.

To securely exchange data between edge devices and cloud-based services, a unidirectional gateway is commonly employed. This gateway extracts information from edge devices, converts it into formats compatible with cloud infrastructure, and transmits it securely over the internet.

In control-critical networks, software updates for edge devices are not directly deployed from the cloud. Instead, an IIoT update server within the control-critical network is responsible for distributing updates. Secure OT practices strictly prohibit the automatic deployment of firmware updates without prior testing and validation in a dedicated ICS testing environment.

For control-critical networks, the flow of information or potentially harmful data from the cloud to physical systems is meticulously monitored and controlled. Continuous, detailed control of physical processes from an internet-based cloud is not permissible. For instance, cloud-based HMI services, which allow remote operators to send detailed instructions to industrial sites worldwide, are prohibited in secure OT environments.

6.2 AI/ML

Artificial intelligence (AI) is rapidly transforming cybersecurity, offering significant advantages to defense teams. Its capabilities can revolutionize defensive operations, providing a decisive edge against cyber threats. By leveraging AI effectively, organizations can strengthen their security platforms, proactively detect sophisticated attacks, automate tasks, and expedite incident response. However, alongside these substantial benefits arise valid concerns regarding the reliability and ethical use of AI in cybersecurity defense.

OT and ICS stand to particularly benefit from advancements in AI and machine learning (ML) for cybersecurity. Traditional rule-based systems are susceptible to vulnerabilities arising from novel malware and software exploits, often bypassing signature-based defenses. The convergence of OT/IT systems, driven by AI/ML-enhanced and internet-connected control systems, intelligent manufacturing, and the proliferation of connected medical devices, necessitates robust cybersecurity solutions.

6.2.1 Benefits

The cybersecurity industry witnesses a surge in AI adoption for security platforms, driven by its potential to enhance situational awareness, improve threat detection, and enable predictive analysis. Traditionally, these platforms relied on aggregating and analyzing vast quantities of security event data for threat detection and response. However, AI integration revolutionizes their capabilities, fostering intelligence and efficiency. AI algorithms process diverse, complex data sources, identifying patterns and anomalies in real-time. This empowers security teams with the ability to detect sophisticated attacks to respond swiftly and effectively. Furthermore, AI automates repetitive tasks, delivers actionable insights, and streamlines threat detection with minimized false positives. The continuous learning and adaptation of AI to evolving threats strengthens overall defense efficacy, allowing organizations to better safeguard critical assets and swiftly respond to security incidents.

Predictive analytics, fueled by AI, empowers defense organizations to anticipate and mitigate cyber threats. Leveraging historical data to identify attack patterns, AI algorithms forecast future threat vectors, enabling proactive defense strategies. This foresight bolsters situational awareness and strengthens overall defensive posture. However, maintaining accurate and reliable predictive models hinges on continuous refinement and validation, which ensures informed decision-making and effective preventive measures.

AI accelerates baseline traffic learning, empowering AI/ML systems to discern anomalous behavior and patterns within assets and networks. Such deviations might indicate environmental compromise or misconfigured systems. Signature-based solutions are inadequate, failing to safeguard critical environments from evolving threats. AI, however, adapts dynamically to network growth and changes. It identifies patterns and behaviors in real-time, excelling at detecting anomalies within network traffic. By leveraging and learning from vast enterprise data generated by connected devices, AI significantly enhances the accuracy and efficiency of network traffic monitoring, thanks to its rapid data processing capabilities.

AI technology can identify indications of hackers employing AI in their attacks, while machine learning tools are aiding security agencies to catch operations relying on “living-off-the-land” techniques. CISA's Roadmap for AI (November 2023) [61] outlines a strategic approach to harnessing AI for cybersecurity while mitigating associated risks.

Using machine learning, the initiative aims to:

- Promote beneficial AI applications in security
- Secure AI systems from cyber threats
- Deter malicious AI use against critical infrastructure

Immediate priorities of the AI Roadmap include:

- Emphasizing AI cybersecurity principles in development
- Developing tools to safeguard critical infrastructure

"AI cybersecurity" encompasses both safeguarding AI systems and defending against AI-driven attacks. Threat identification alone is insufficient; effective response is paramount. Enterprises achieve optimal security outcomes by integrating continuous AI monitoring with automated response solutions like SIEM and SOAR. This empowers security teams to gain deeper insights into their environments, particularly at OT/IT convergence points.

6.2.2 Risks-Challenges

While AI-powered security platforms offer significant advantages, concerns persist about the maturity of their underlying algorithms. Specifically, the potential for generating both false positives and negatives remains a challenge. Striking a balance between accurate threat detection and minimizing false alarms necessitates meticulous fine-tuning of detection mechanisms. This is crucial to mitigate the risks associated with erroneous alerts and ensure reliable threat identification.

Acquiring appropriate data for training AI/ML systems poses a significant challenge to effective fine-tuning. These systems rely on relevant problem-specific data for learning, but businesses often lack access to, or possess insufficient quantities of, the "correct" data, leading to potential biases in outcomes. Utilizing representative and high-quality data mitigates this issue, preventing inconsistent or discriminatory results.

Organizations attempting to maximize AI/ML potential face significant challenges, particularly concerning data availability and quality. Effective machine learning requires a large, relevant dataset, without which even sophisticated algorithms struggle to generate accurate insights and predictions.

Aligning AI outputs with business objectives presents another hurdle. Ensuring AI solutions meaningfully contribute to organizational goals necessitates careful calibration and a deep understanding of the problem domain. Finally, training and maintaining AI/ML systems incur substantial costs. High computational power, skilled personnel, and consistent access to clean, high-quality data are essential for their optimal performance. Guaranteeing accurate data is paramount for achieving reliable results.

The expanding integration of AI in defense cybersecurity necessitates prioritizing ethical considerations. Guaranteeing individual privacy, upholding transparency, and mitigating biases are critical aspects demanding attention. AI algorithms must be designed and implemented with respect for data privacy and adherence to relevant regulations.

Furthermore, ensuring transparency in AI model operations and decision-making processes is essential for building trust and enabling effective oversight. Proactive identification and mitigation of biases within training data and algorithms are crucial to prevent discriminatory outcomes and ensure equitable defense practices. Striking a balance between harnessing AI's potential and adhering to ethical principles underpins the maintenance of public trust and the integrity of defense cybersecurity.

Despite substantial challenges, significant OT/ICS security benefits can be achieved through AI/ML adoption. However, enterprises must pre-define security and business objectives, invest in high-quality, properly trained data, and implement rigorous testing to mitigate potential errors and ensure reliable performance.

Hackers are increasingly targeting critical infrastructure using "living-off-the-land" techniques, exploiting existing tools and privileges instead of malware for stealthier attacks. They leverage flaws, misconfigurations, and default passwords to establish seemingly legitimate accounts and move undetected within networks. Machine learning, AI, and big data analytics are crucial for identifying these anomalous activities.

Defense organizations must actively monitor AI advancements and conduct regular technology assessments to exploit emerging opportunities and maintain a leading edge in cybersecurity. Embracing flexibility, adaptability, and proactive innovation are crucial for effectively navigating the dynamic cyber threat landscape. By seamlessly integrating AI into defensive strategies, security teams can leverage enhanced security platforms, improved threat detection, predictive analytics, and heightened situational awareness to outmaneuver adversaries and maintain a competitive advantage.

6.3 Blockchain

6.3.1 Benefits

Emerging as a disruptive force across diverse sectors, blockchain technology, championed by leading industry players, promises to revolutionize banking, real estate, supply chains, voting systems, and energy management. Its burgeoning applications extend to ICS network security, offering enhanced data integrity, robust authentication, and secure communication. Leveraging distributed ledgers, asymmetric cryptography, consensus algorithms, and smart contracts, blockchain holds significant potential to bolster the security posture of critical infrastructure.

Blockchain, a novel distributed ledger technology, offers secure data storage where information cannot be forged or tampered with. Smart contracts, and automated scripts residing on the blockchain, facilitate multi-step process automation. The core principles of blockchain involve distributed data storage, transmission, and asymmetric encryption, eliminating reliance on central servers. Complex verification mechanisms ensure data integrity, consistency, and efficient data exchange. By simplifying industrial device transactions and data exchange, blockchain technology has the potential to reduce costs and enhance ICS efficiency. In the future, blockchain-based credit mechanisms for distributed IoT could allow for the monitoring and management of intelligent devices through records and smart contracts for regulating their behavior, ultimately addressing industrial control system network security concerns.

Beyond secure data storage, blockchain offers several additional applications for ICS. One crucial example involves protecting and verifying device firmware and application software updates. As network security measures improve, attackers increasingly resort to methods like inserting Trojans in downloadable software. Notably, the 2014 Havex malware variant targeted OPC-aware devices through Trojanized software, highlighting the vulnerability. Registering firmware and software updates on a blockchain would create an immutable record, effectively preventing such attacks. Other potential applications include:

- Authentication, authorization, and non-repudiation for device configuration and program changes
- Protection, verification, and non-repudiation of critical data like historian streams or regulatory reports

Below are listed some concrete applications of blockchain technology within ICS/OT systems, directly addressing critical cybersecurity challenges faced by the industrial domain.

1. Secure Communication and Data Sharing:

- **Smart grids:** Establishing a secure peer-to-peer network for energy trading between prosumers and consumers, ensuring data integrity and privacy.
- **Manufacturing:** Sharing production data between different machines and facilities securely, protecting against unauthorized access or manipulation.
- **Water management:** Securely sharing sensor data about water levels and quality across different departments within a water treatment plant.

2. Enhanced Access Control and Identity Management:

- **Power plants:** Implementing smart contracts to automate access control for critical infrastructure, granting permissions based on predefined rules, and eliminating human error.
- **Oil and gas pipelines:** Managing employee and contractor access to specific segments of the pipeline based on their roles and authorization levels.
- **Transportation systems:** Securely managing access to control systems for traffic lights, railway networks, or autonomous vehicles.

3. Improved Supply Chain Security:

- **Tracking the provenance of equipment and parts:** Verifying the authenticity of components used in critical infrastructure, preventing the use of counterfeit or compromised parts.
- **Monitoring maintenance records:** Securely storing and sharing the maintenance history of critical equipment, ensuring authenticity and transparency.
- **Auditing supplier compliance with cybersecurity standards:** Implementing blockchain-based systems to track and verify suppliers' adherence to specific cybersecurity requirements.

4. Intrusion Detection and Incident Response:

- **Detecting unauthorized access:** Analyzing changes in the blockchain ledger to identify anomalies and potential intrusions into the system.
- **Verifying incident reports:** Using tamper-proof records on the blockchain to validate incident reports and facilitate faster response.
- **Facilitating post-incident analysis:** Tracing the sequence of events during an attack using the immutable blockchain record for improved incident response and forensics.

5. Decentralized Security Architecture:

- **Distributing critical control functions:** Utilizing blockchain to decentralize control of critical systems, making them less vulnerable to single points of failure.
- **Enhancing system resilience:** Leveraging the inherent distributed nature of blockchain to ensure continuous operation even if parts of the network are compromised.
- **Improving cyber defense collaboration:** Enabling secure and transparent information sharing between different organizations responsible for critical infrastructure protection.

Synergistically combining blockchain and AI holds promise for more secure and efficient cybersecurity systems. Leveraging AI algorithms, blockchain networks can be continuously monitored for anomalous activity, while blockchain ensures the immutability of AI-generated insights.

6.3.2 Risks-Challenges

While blockchain offers potential benefits for securing Industrial Control Systems (ICS), its implementation comes with inherent risks and challenges. These include the potential for compromised blockchain nodes disrupting operations, the immutability of transactions making error correction difficult, and the high computational power required for blockchain maintenance, which can strain resource-constrained ICS environments. Additionally, the relatively nascent state of blockchain technology in ICS security means established best practices and standards are still under development, leaving room for vulnerabilities in integrating this new technology with existing systems.

6.4 Digital Twins

6.4.1 Benefits

Digital twins, virtual replicas of physical objects, are revolutionizing various industries. Their applications extend from product prototyping and medical simulations to space recreation and campaign modeling. These digital representations, intricately linked to their physical counterparts, enable real-time data extraction and execution, rendering them invaluable when physical inspections are impractical. In manufacturing, digital twins provide a wealth of operational data, enabling predictive maintenance and anomaly detection, including cyberattacks. This concept can be leveraged to enhance industrial security, from design phase flaw identification to real-time intrusion detection. Digital twins are poised to transform industry operations and security.

High-fidelity digital cyber twins provide a non-invasive and automated approach to analyzing, protecting, and optimizing physical systems. These virtual replicas enable real-time assessment of infrastructure vulnerabilities, prototyping of novel integrations, training personnel for incident response, and identification of critical assets. By simulating attacks and visualizing automated system responses, digital cyber twins facilitate risk mitigation and continuous improvement.

Digital twins offer a compelling solution for enhancing *cybersecurity*, particularly in OT environments**.** These virtual replicas of physical systems provide a safe and controlled environment for conducting comprehensive security testing, intrusion detection and prevention, and system optimization. By enabling testing without disrupting real-world operations, digital twins can help organizations maintain high levels of cybersecurity while minimizing downtime and operational risks**.** Real-world security testing can be costly**,** time-consuming, and potentially disruptive. Digital twins, on the other hand, allow for automated, periodic security assessments, including penetration testing and system testing. This enables organizations to identify and remediate vulnerabilities before they can be exploited in the real world. Digital twins can also be used to train intrusion detection systems, which are critical components of OT security. These systems monitor networks for malicious activity and can take corrective actions to prevent attacks. By providing realistic data to train intrusion detection systems, digital twins can enhance their effectiveness in detecting and preventing cyberattacks.

6.4.2 Risks-Challenges

The application of digital twins for cybersecurity is still in its early stages, primarily due to limitations in data fidelity. Achieving high-fidelity data representation requires advanced computer and network engineering techniques. Additionally, organizations need to establish clear processes for integrating digital twins into their cybersecurity workflows.

Research has explored simulation techniques to mirror real-world counterparts. However, validations demonstrating the fidelity of these simulations remain scarce. Consequently, achieving a sufficiently high data resolution remains an unresolved research challenge. This impediment necessitates addressing both computer and network engineering challenges, as well as organizational considerations, before fully exploring digital twins' potential for OT security.

Organizations adopting digital twins must prioritize cybersecurity from the outset. Digital twin design and development should be adequately resourced and adhere to ethical principles, ensuring both value creation and risk mitigation aligned with regulatory frameworks. Digital twins should be treated as critical assets, warranting robust security measures similar to other network devices. Implement a zero-trust architecture, extending it beyond the perimeter to encompass the internal network through micro-segmentation, multi-factor authentication, and other effective strategies. While enhanced security may introduce additional access steps for employees, the benefits far outweigh the inconvenience.

In the interconnected world of Industry 4.0 and Industry 5.0, a single attack on a supply chain can disrupt an entire operation. Digital twins, while offering valuable security benefits, introduce additional vulnerabilities. By creating a digital replica, organizations inadvertently create a second access point for cyber adversaries. If hackers breach the digital twin, they gain access to sensitive information from the real asset, compromising classified, operational, or customer data. Organizations must carefully consider these risks when adopting digital twins, implementing robust cybersecurity measures to protect both physical assets and their virtual counterparts.

The increasing adoption of digital twins in various industries introduces new cybersecurity challenges and opportunities. As digital twins become more interconnected, the potential attack surface expands, necessitating advanced cybersecurity strategies. AI-powered threat detection, blockchain-based data security, and robust regulatory frameworks are crucial to ensure the safe and ethical utilization of digital twins. As technology advances and organizations develop best practices for integrating digital twins, these virtual replicas will play an increasingly important role in safeguarding critical OT systems.

6.5 Deception Technology

The rise of cyberattacks, including ransomware, data breaches, and persistent threats, significantly disrupts industrial production, business operations, and even jeopardizes the security of our digital society. Due to their simplistic architecture, ICS systems are susceptible to vulnerabilities and easy targets for attackers, particularly those employing low processing power and memory. Defending ICS from such malicious activities is challenging due to their inherent limitations, making them unlikely to receive regular security updates or patches. Installing endpoint protection agents is often impractical as well. Considering these constraints, deception strategies emerge as an indispensable component of security frameworks, offering a viable solution to enhance threat detection and response capabilities.

6.5.1 Benefits

Deception technologies constitute a proactive security defense strategy that effectively detects and mitigates malicious activities. By creating a deceptive environment of false information and simulated assets, this approach misleads attackers, leading them into traps and wasting their time and resources. This, in turn, increases the complexity of intrusion attempts and hinders attackers' progress. Furthermore, deception technologies enable defenders to gather comprehensive attack logs, deploy effective countermeasures, trace the source of attacks, and monitor attacker behavior in real time. This detailed information allows security analysts to decipher attacker TTPs, enabling them to develop robust defense strategies and regain the initiative in the cyber domain.

Deception techniques like honeypots mimic real systems to lure attackers and gather valuable information. These simulated environments allow defenders to capture malicious payloads, identify attacker IP addresses, and even extract information about their browsers in web application attacks. In addition to collecting valuable data, such as the attacker's payloads and host information, deception technologies such as ‘honey files’ can also leverage JSONP (JSON with Padding) Hijacking to identify the attacker’s social media accounts, further enhancing their effectiveness in countering cyberattacks. *Honey files*, which intentionally contain valuable data, can also be deployed to lure attackers into revealing their intentions, enabling defenders to take timely action to neutralize the threat and prevent data theft. Honey files are files that contain valuable data, such as financial records or customer information. They are intentionally left on a network to entice attackers. When an attacker accesses a honey file, they inadvertently trigger an alarm that notifies the security team. This allows the security team to take action to neutralize the attacker and prevent them from stealing the data.

While honeytokens and honeypots share similarities, they differ in their implementation and objectives. Honeypots are decoy systems designed to attract and engage attackers, mimicking real systems with apparent vulnerabilities. In contrast, honeytokens are discrete pieces of valuable data intentionally embedded within networks to entice attackers into revealing their identity and location. Honeytokens provide early detection of malicious activities, allowing security teams to gather insights into attack vectors and patterns within their systems. By analyzing attackers behavior through honeytokens, organizations can better understand adversary actions and implement effective countermeasures to enhance their cybersecurity posture. Honeytokens and honey files are more lightweight and resource-efficient compared to honeypots, making them suitable for organizations with limited resources. However, honeypots offer a broader range of intelligence, providing comprehensive information about attacker TTPs.

Honeypots, when compromised, can serve as effective detection tools to generate alerts, and divert attackers' attention away from critical systems. The value of a honeypot is primarily determined by the number of attacks it attracts. To maximize its effectiveness, honeypots must strike a balance between enticing attackers with simulated vulnerabilities and maintaining a level of security that resembles real systems. A system that stands out as significantly less secure than others in the network may raise suspicions and deter attackers from engaging with it. The amount of interaction allowed with the honeypot can also influence the attacker’s behavior and the volume of collected attack data. Ultimately, honeypots aim to gather valuable insights to strengthen network and system security measures.

Deception technology, such as honeypots, honey files, and honeytokens, can complement the limitations of traditional detection systems and significantly enhance the security of industrial control networks. These tools effectively identify, and expose cyberattacks against ICS, providing valuable insights into the overall risk landscape. By detecting actual OT vulnerabilities exploited by attackers and alerting security analysts, deception technology expedites the patching process and enhances overall network security posture. Additionally, timely alerts, such as those preceding ransomware outbreaks, can prevent significant financial losses and production disruptions. To further strengthen defense capabilities, deception technology for ICS should be integrated with emerging technologies. The ability to simulate and interact with simulated environments expands the scope of deception, providing a more comprehensive approach to threat detection and mitigation. Moreover, the attack logs captured by deception applications hold immense value for in-depth analysis. Utilizing AI or Big Data tools to process these logs enables a deeper understanding of ICS-specific threat intelligence. Deception technology plays a critical role in the rapid evolution of ICS network security, fostering enhanced threat intelligence and improved defense capabilities. While challenges remain, these technologies offer promising avenues for innovation and breakthrough advancements.

6.5.2 Existing ICS Honeypots per Interaction

Honeypots are classified based on the level of interaction they provide to attackers: high-interaction, low-interaction, and medium-interaction.

- **High-interaction** honeypots, while offering the most comprehensive attack data due to their realistic replication of real systems, come with a higher risk of compromise. These complex systems are harder to detect by attackers, allowing them more extensive interaction and increasing the potential for system infiltration. In ICS environments, deploying high-interaction honeypots necessitates using real and expensive PLC or other ICS devices. However, a single device wouldn't accurately reflect a real-world scenario, requiring multiple interconnected devices to effectively mimic true ICS data transfer, further increasing the cost and complexity.
- **Low-interaction** honeypots simulate specific devices with limited interaction, reducing risk but also limiting data collection. Acting as decoys, low-interaction honeypots mimic basic functionalities of specific industrial devices like Programmable Logic Controllers (PLCs). These decoys run on common operating systems (like Ubuntu) and offer attackers limited interaction, making them valuable tools for gathering intelligence without significant risk of compromise.
- **Medium-interaction** honeypots offer a middle ground, providing more interaction than low-interaction but less than high-interaction honeypots. They can be considered a subcategory of low-interaction honeypots. For instance, they might simulate a web server's responses to attract attackers searching for vulnerabilities, but without the high-risk of being fully compromised. However, unlike high-interaction honeypots, they don't run a full operating system, limiting the data they can gather on potential attacks. Overall, medium-interaction honeypots are less commonly deployed compared to their low and high-interaction counterparts.

Due to the dynamic nature of ICS operations, the deployment of a honeypot has to be extremely believable, since the goal is to capture useful data from knowledgeable attackers.

Some experts argue that the traditional interaction level scheme used to classify honeypots is not suitable for ICS honeypots due to the unique characteristics of ICS environments. This can make it challenging for the ICS defenders to select an appropriate honeypot for their specific needs. To address these problems, *ICSvertase* [62], a novel framework is implemented after being firstly introduced on ARES Conference 2023. It is a new framework that allows structural reasoning upon ICS honeypots. *ICSvertase* integrates several existing components from the ATT&CK for ICS and Engage frameworks provided by MITRE and extends them with novel elements. It also provides a novel approach helping companies and users in several real-world use cases, by choosing the most suitable existing ICS honeypot, designing new ICS honeypots, and classifying existing ones in a more refined way.

ICS systems have historically lacked robust built-in security measures due to their original design for limited access. However, recent advancements in machine learning (ML) have emerged as a promising approach to enhance ICS security. *Bhamare et al. (2020)* [63] in their survey with various applications, including risk assessment, malicious communication of ML detection, and cloud-based attack mitigation, demonstrated the potential of ML techniques to improve upon ICS security. To fully realize the potential of ML-based security solutions, a substantial amount of data is required for training and continuous improvement. Honeypots, particularly those deployed within organizations, can provide valuable real-time threat data, while external honeypots or those deployed within research environments can offer broader insights into emerging threats.

Research honeypots, which are Internet-facing, are primarily used to gather information about threat actors and their methods by luring them into interacting with simulated systems. Unsuspected attackers may continue interacting with these honeypots, and even try exploiting vulnerabilities, making them effective for detecting large-scale, indiscriminate attacks. However, they are not so effective against knowledgeable, targeted attacks.

Production honeypots, on the other hand, are typically not directly accessible and are deployed within organizational networks as part of a security solution. They are often low-interaction honeypots, which are easier to deploy but can be easily fingerprinted and do not allow attackers to interact beyond the initial login screen or the protocol handshake. High-interaction honeypots are necessary to deceive targeted attackers and gather insights into their intentions, such as modifying firmware or programmable logic.

The ICS community has embraced several open-source honeypot solutions, leveraging deception technology to enhance OT security. Deception techniques have been successfully employed in various domains, including web applications, databases, mobile apps, and the IoT. This approach has also found application in ICS honeypots, exemplified by Conpot, XPOT, and CryPLH, which effectively simulate protocols like Modbus, S7, IEC-104, and DNP3.

❖ ***Low-Interaction***

a. Conpot [64] is an open-source low-interactive honeypot that supports various industrial protocols, including IEC 60870-5-104, Building Automation and Control Network (BACnet), Modbus, s7comm, and other protocols such as HTTP, SNMP and TFTP. It is designed to be easy to deploy, modify and extend. The Conpot and Conpot-based honeypot are among the most popular ICS deception applications that have been used by researchers. They are easy to set up and scale well, making them good candidates to research internet wide scanning, however, their inability to interact with an attacker limit their utility in detecting and characterizing ICS attacks, and studies using Conpot have yet to identify any new or targeted ICS attack.

❖ ***High-Interaction***

a. **XPOT** is a pioneering software-based honeypot mimicking Siemens S7-300 series Programmable Logic Controllers (PLCs). It allows attackers to interact realistically by compiling, running, and loading PLC programs. This high-interaction honeypot supports common industrial protocols and enables building large decoy networks for broader threat detection. Additionally, XPOT can connect to simulated industrial processes, providing attackers with a realistic experience and enhancing the honeypot's effectiveness.

b. **CryPLH** is a high-interactive and virtual Smart-Grid ICS honeypot simulating Siemens Simatic S7-300 PLC. It runs on a Linux-based host and uses MiniWeb HTTP servers to simulate HTTP(S), a Python script to simulate Step 7 ISO-TSAP protocol and a custom SNMP implementation. CryPLH is constantly evolving, expanding its capabilities from individual protocols to replicating entire ICS environments, providing valuable insights into attacker behavior.

c. **HoneyPLC** [65] was introduced in the conference CCS ’20. It is a high-interaction, extensible, and malware collecting honeypot supporting a broad spectrum of PLCs models and vendors. Results from the research showed that HoneyPLC exhibits a high level of camouflaging: it is identified as a real device by multiple widely used reconnaissance tools, including Nmap, Shodan's Honeyscore, the Siemens Step7 Manager, PLCinject, and PLCScan, with a high level of confidence. For the implementation phase, HoneyPLC on Amazon AWS was deployed and recorded a large amount of interesting interactions over the Internet. Showing not only that attackers targeting ICS systems, but also that HoneyPLC can effectively engage and deceive them while collecting data samples for future analysis.

❖ ***Hybrid-Interaction***

Low-interaction honeypots can be inexpensively deployed at scale, but they are easy to identify. Furthermore, because they do not emulate the device state, they cannot be used to profile the attacker's behavior (e.g., attempts to modify programmable logic). High-interaction honeypots overcome these limitations, but can be expensive to develop, deploy, and maintain. To overcome those limitations hybrid honeypots were introduced combining the capabilities and functionality of both low-interaction and high-interaction honeypots. This hybrid approach makes hybrid interactions ICS honeypots a powerful tool for detecting and preventing cyberattacks. They can detect a wider range of attacks and provide a more comprehensive intelligence than either type of honeypot alone.

a. SecuriOT [66] developed a reconfigurable honeypot device that can operate as both a standalone emulator and a proxy to a production ICS device. This versatility makes it suitable for both research and production environments. SecuriOT's network of over 120 virtual honeypots covers over 20 countries and supports various ICS protocols, including S7comm, BACnet, SOAP, IEC-104, DNP3, and Modbus. These protocols are widely used in various industrial sectors, making SecuriOT's honeypots a valuable tool for gathering threat intelligence.

b. HoneyICS [67] is a network of honeypots forming a honeynet that can emulate the key components of OT networks: PLCs, HMIs, communication networks, and a physical plant. These components can be implemented either by using real physical devices or by employing emulation and simulation software. HoneyICS can be configured to be accessible either via a (compromised) VPN or by exposing specific devices (PLCs or HMIs) on the Internet. The architecture also includes a monitoring system and a management dashboard. The monitoring system tracks attacker activities, and the management dashboard facilitates honeynet configuration, deployment, and monitoring. The whole architecture allows the collection of valuable threat intelligence and the detection of sophisticated attacks.

6.5.3 Risks-Challenges

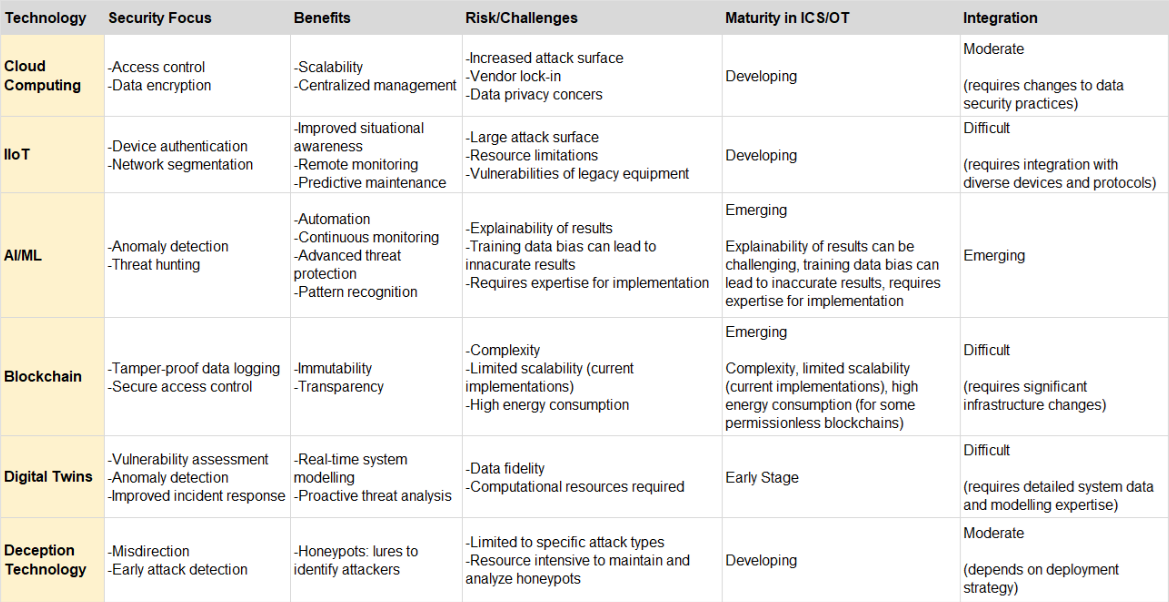
Despite advancements in deception technology for defensive use, deploying and maintaining effective deception systems in ICS environments remains challenging due to several fundamental differences between ICS and traditional IT networks. The criticality of ICS processes necessitates careful consideration, as false positives from honeypots could disrupt operations or cause unnecessary shutdowns. Additionally, the diverse range of ICS devices, including many proprietary protocols and ICS configurations, poses a significant obstacle to develop realistic deception solutions that evade detection by existing monitoring systems. Customization of honeypots and other deception tools is often required to emulate specific protocols, increasing implementation complexity and potential deployment challenges. In addition, pure virtual ICS honeypots often face limitations in their simulation capabilities, making them susceptible to detection by attackers. Finally, the potential for vulnerabilities within the deception technology itself raises concerns about unintentionally introducing new weaknesses into the overall ICS security posture.

Currently, virtual ICS honeypots primarily simulate underlying control protocols, and many are publicly available, readily discoverable through search engines like Shodan**,** Censys or Zoomeye. Gathering sufficient attack data and enhancing simulation accuracy remains a significant challenge for security researchers. High-interaction ICS honeypots incur substantial resource requirements, they are costly both in acquisition and maintenance. They often necessitate the integration of physical systems or equipment to create realistic simulation environments.

6.6 Comparative Analysis

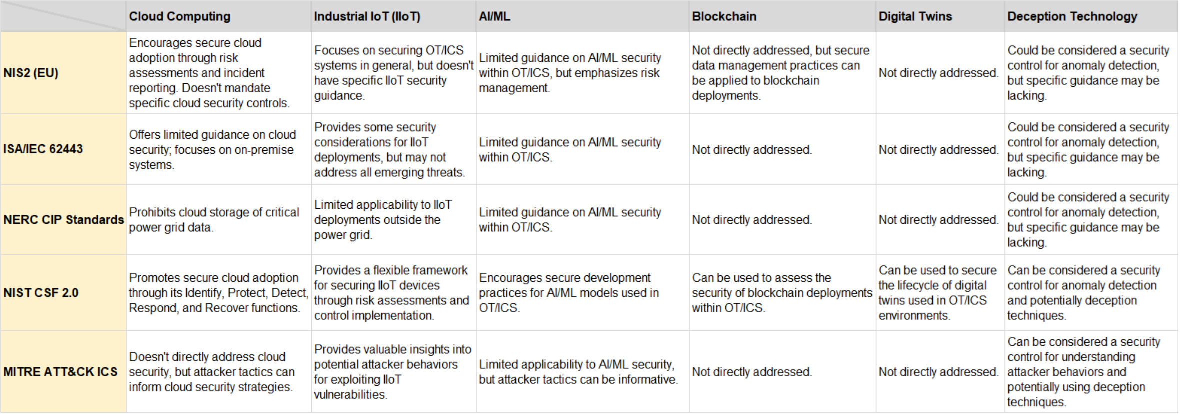
This chapter examined a spectrum of cutting-edge technologies transforming OT/ICS cybersecurity. Each offers distinct advantages. Cloud computing delivers scalability and centralized management, while IIoT bolsters situational awareness. AI/ML automates threat detection, and blockchain guarantees tamper-proof data logging. Digital twins enable proactive threat analysis, and deception technology facilitates early attack detection. However, these technologies also present hurdles. Cloud security concerns and vendor lock-in exist with cloud computing. IIoT faces issues with device heterogeneity and legacy equipment vulnerabilities. Unlocking the full potential of AI/ML in OT/ICS security requires advancements in explaining its results and mitigating bias in training data. Blockchain struggles with complexity and scalability limitations. Digital twins require high-fidelity data and significant computational resources, while deception technology is effective against specific attacks but resource-intensive to maintain. The following table Figure 47 provides a comparative analysis of these technologies across key metrics, empowering informed decision-making for securing OT/ICS environments. Definitions for each metric are provided below.

- ❖ **Security Focus:** describes the primary security area the technology addresses in ICS/OT systems.
- ❖ **Benefits:** describe the benefits of each technology in an ICS/OT cybersecurity context.
- ❖ **Risks/Challenges:** describe the challenges of each technology in an ICS/OT cybersecurity context.
- ❖ **Maturity in ICS/OT:** indicates how established and widely adopted the technology is within the ICS/OT industry. Terms like "Emerging," "Developing," and "Established" can be used.
- ❖ **Integration:** describes how easily the technology can be incorporated into existing ICS/OT infrastructure without causing disruption or compatibility issues.
- ❖ **Regulation:** considers how well the technology aligns with relevant industry issuing bodies (regulations, directives, frameworks) and compliance requirements for ICS/OT cybersecurity.



Technology	Security Focus	Benefits	Risk/Challenges	Maturity in ICS/OT	Integration
Cloud Computing	-Access control -Data encryption	-Scalability -Centralized management	-Increased attack surface -Vendor lock-in -Data privacy concers	Developing	Moderate (requires changes to data security practices)
IIoT	-Device authentication -Network segmentation	-Improved situational awareness -Remote monitoring -Predictive maintenance	-Large attack surface -Resource limitations -Vulnerabilities of legacy equipment	Developing	Difficult (requires integration with diverse devices and protocols)
AI/ML	-Anomaly detection -Threat hunting	-Automation -Continuous monitoring -Advanced threat protection -Pattern recognition	-Explainability of results -Training data bias can lead to innacurate results -Requires expertise for implementation	Emerging Explainability of results can be challenging, training data bias can lead to inaccurate results, requires expertise for implementation	Emerging
Blockchain	-Tamper-proof data logging -Secure access control	-Immutability -Transparency	-Complexity -Limited scalability (current implementations) -High energy consumption	Emerging Complexity, limited scalability (current implementations), high energy consumption (for some permissionless blockchains)	Difficult (requires significant infrastructure changes)
Digital Twins	-Vulnerability assessment -Anomaly detection -Improved incident response	-Real-time system modelling -Proactive threat analysis	-Data fidelity -Computational resources required	Early Stage	Difficult (requires detailed system data and modelling expertise)
Deception Technology	-Misdirection -Early attack detection	-Honeypots: lures to identify attackers	-Limited to specific attack types -Resource intensive to maintain and analyze honeypots	Developing	Moderate (depends on deployment strategy)

Figure 46 Comparative Analysis of Cutting-Edge Technologies for ICS application



	Cloud Computing	Industrial IoT (IIoT)	AI/ML	Blockchain	Digital Twins	Deception Technology
NIS2 (EU)	Encourages secure cloud adoption through risk assessments and incident reporting. Doesn't mandate specific cloud security controls.	Focuses on securing OT/ICS systems in general, but doesn't have specific IIoT security guidance.	Limited guidance on AI/ML security within OT/ICS, but emphasizes risk management.	Not directly addressed, but secure data management practices can be applied to blockchain deployments.	Not directly addressed.	Could be considered a security control for anomaly detection, but specific guidance may be lacking.
ISA/IEC 62443	Offers limited guidance on cloud security; focuses on on-premise systems.	Provides some security considerations for IIoT deployments, but may not address all emerging threats.	Limited guidance on AI/ML security within OT/ICS.	Not directly addressed.	Not directly addressed.	Could be considered a security control for anomaly detection, but specific guidance may be lacking.
NERC CIP Standards	Prohibits cloud storage of critical power grid data.	Limited applicability to IIoT deployments outside the power grid.	Limited guidance on AI/ML security within OT/ICS.	Not directly addressed.	Not directly addressed.	Could be considered a security control for anomaly detection, but specific guidance may be lacking.
NIST CSF 2.0	Promotes secure cloud adoption through its Identify, Protect, Detect, Respond, and Recover functions.	Provides a flexible framework for securing IIoT devices through risk assessments and control implementation.	Encourages secure development practices for AI/ML models used in OT/ICS.	Can be used to assess the security of blockchain deployments within OT/ICS.	Can be used to secure the lifecycle of digital twins used in OT/ICS environments.	Can be considered a security control for anomaly detection and potentially deception techniques.
MITRE ATT&CK ICS	Doesn't directly address cloud security, but attacker tactics can inform cloud security strategies.	Provides valuable insights into potential attacker behaviors for exploiting IIoT vulnerabilities.	Limited applicability to AI/ML security, but attacker tactics can be informative.	Not directly addressed.	Not directly addressed.	Can be considered a security control for understanding attacker behaviors and potentially using deception techniques.

Figure 47 Cutting-Edge Technologies for ICS applications aligned with relevant issuing bodies

7 Conclusions & Future Work

7.1 Conclusions

The year 2023 saw a surge in cyberattacks targeting critical infrastructure and manufacturing (OT/ICS) globally. Ransomware, particularly through RaaS models, has become a major threat, causing financial losses, operational disruptions, reputational damage, and even physical harm. The convergence of IT and OT systems necessitates a holistic defense strategy built on strong governance and a multifaceted security approach. Key challenges include inherent vulnerabilities in OT/ICS environments, weaknesses within supply chains, and the complexities of legacy systems. Furthermore, the rise in geopolitical tensions increases the risk of aggressive cyberattacks by state-sponsored actors or politically motivated groups. The effectiveness of tactics used by these groups, like the "living-off-the-land" techniques employed in Volt Typhoon, underscores this concern. Security personnel must leverage their system knowledge and establish baselines to accurately assess potential threats. When creating detection logic, it's crucial to consider the variability of command string arguments, as elements like used ports can differ across environments. Additionally, attackers' ability to camouflage themselves within legitimate Windows operations further complicates defense strategies traditionally reliant on IT Endpoint Detection and Response (EDR) tools.

Critical infrastructure faces a constantly intensifying cyber threat landscape, demanding a fundamental change in security strategies. The industrial control system (ICS) landscape is constantly under siege by ever-more sophisticated cyberattacks. While preventative measures remain a crucial first line of defense, a truly robust security posture requires a more holistic approach. Organizations neglecting detection, response, and recovery capabilities expose themselves to attackers capable of bypassing preventative controls.

The following key phases, explored in detail within this thesis, serve as a valuable roadmap to fortify operational security.

1. **Risk Management Plan:** Assess current industrial cyber risk by correlating threats and vulnerabilities with the potential impact on operational issues like loss of view, control, or safety, driving risk-based decisions throughout the security lifecycle.

2. **Cyber Defense Strategy Plan (development):** Assess the current network architecture in terms of security and design modifications for fortifying the core operations based on the required integrations (internal-external). Provision necessary equipment for preparation of the following step.

3. **Cyber Defense Implementation (deployment):**
   a) Deploy and integrate equipment to fulfill passive and active defense mechanism
   b) Implement procedural controls to accompany the defensive technology stack.

4. **Network Segmentation** in OT/ICS cybersecurity minimizes attack surface by isolating critical systems and simplifies threat detection/containment, making it a crucial and cost-effective security control

5. **Supply Chain Risk Assessment:** Ultimately, a comprehensive supply chain risk assessment strengthens the overall security posture of ICS/OT systems by ensuring all components are evaluated and secured, leading to a more resilient critical infrastructure. By evaluating potential vulnerabilities within the entire supply chain, organizations can identify and mitigate risks before they manifest as security breaches. This type of assessment will lead to collaborative engagement with OT/ICS providers, as it fosters an open communication and transparency, allowing for joint efforts to address identified weaknesses. This proactive approach delves into the security practices of OT/ICS vendors and their subcontractors, that is vital for building efficient defense mechanisms and providing sufficient incident response and mitigate actions.

This recommended structured methodology can empower organizations to effectively manage ICS/OT security risks in the face of evolving threats. For organizations struggling with ICS/OT security, the five critical controls offer a valuable starting point. These controls serve as a roadmap for building tailored security programs, but their effectiveness is contingent on an organizational culture that prioritizes cyber risk at all levels. A "team sport" approach, combining agile controls and defined processes, is crucial to keep pace with evolving threats. Implementing the right framework empowers critical infrastructure organizations to proactively defend against malicious actors.

Mature facilities recognize the distinct needs of IT and ICS/OT environments, implementing dedicated ICS-aware technologies, trained security personnel, and targeted security efforts. A well-designed with layered defense, ICS-oriented program, is no longer optional, but rather essential. However, mere prevention is insufficient. Proactive measures are crucial for effective ICS security. Cybersecurity defenders and leaders must act proactively, assuming defense-in-depth controls may be bypassed. Their focus should shift towards proactive threat hunting within the ICS environment and implementing measures that reduce the ability of adversaries to "living-off-the-land".

The current cyber threat landscape demands a revamped approach to securing critical infrastructure. This thesis emphasizes and advocates the transformative power of cutting-edge technologies like AI/ML, blockchain, digital twins, and deception technology for industrial cybersecurity. By harnessing AI's real-time threat detection and anomaly identification capabilities, organizations can proactively counter evolving cyberattacks. Blockchain's secure and transparent record-keeping bolsters data integrity, while digital twins offer safe environments to test security measures and identify vulnerabilities before they become real-world problems. Deception technology further strengthens defenses by diverting attackers from critical assets and gathering valuable intelligence on their tactics. Integrating these advancements fosters a proactive, multi-layered security posture, significantly enhancing the resilience of critical infrastructure against persistent cyber threats. As the threat landscape continues to evolve, embracing these cutting-edge technologies is crucial for safeguarding critical infrastructure and ensuring the smooth operation of our vital societal systems.

The ICS security market anticipates substantial growth fueled by the escalating need to protect critical infrastructure across diverse sectors. Close collaboration between governments, industries, and cybersecurity experts is vital to establish comprehensive standards and regulations, ensuring a minimum-security baseline for ICS environments. Additionally, continuous research and development are crucial to remain ahead of evolving threats and vulnerabilities. By continuously refining security controls, embracing cutting-edge technologies, and fostering a culture of proactive security awareness, organizations can significantly enhance the resilience of their critical operations and safeguard them from the ever-evolving threat landscape.

7.2 Future Work

The proposed initiatives outlined in this thesis offer a significant step forward in fortifying OT/ICS security through a multi-layered approach leveraging AI and other cutting-edge technologies as also embracing communities' collaboration. However, the ever-evolving threat landscape necessitates continual exploration and adaptation. A future work should delve into potential areas for further research that can build upon the established foundation. Here, we explore ways to enhance collaboration within the OT/ICS community, investigate the integration of AI with other emerging technologies, and address ethical considerations surrounding AI-powered defense mechanisms. Additionally, the importance of continuous evaluation and adaptation of security strategies is emphasized to ensure long-term effectiveness.

The below action items and research initiatives focus on how defenders can significantly improve the understanding of evolving threats specific to OT/ICS systems and leverage the potential of AI to strengthen their overall cybersecurity posture. This will ultimately lead to a more secure and resilient critical infrastructure landscape.

- Developing a collaborative threat intelligence sharing program (database) for OT/ICS stakeholders, including vendors, operators, and security researchers.
- Conducting red teaming tabletop exercises specifically focused on OT/ICS environments to identify novel attack vectors. Throughout the process document findings as well as technical and operational deficiencies.
- Conducting research on the exploitation of emerging technologies (e.g., cloud computing, AI/ML) within OT/ICS environments for malicious purposes.
- Developing pilot projects to test and evaluate the effectiveness of AI-powered tools in real-world OT/ICS environments
- Developing AI algorithms specifically tailored to identify anomalies in industrial control data and network traffic.
- Fostering collaboration between AI security researchers and OT/ICS domain experts to ensure the practical and effective application of AI technologies.
- Addressing the skills gap in the OT/ICS workforce by developing training programs focused on emerging threats and AI-powered security solutions.

Building upon the proposed initiatives, future research can delve deeper into specific areas. Standardizing threat intelligence sharing formats and establishing secure communication channels within the OT/ICS community would further enhance collaboration and expedite threat response. Additionally, exploring the integration of AI with other emerging technologies like blockchain could offer novel avenues for securing OT/ICS environments. Furthermore, investigating the ethical considerations surrounding AI-powered defense mechanisms, particularly regarding potential biases and the explainability of AI decisions, would be crucial for responsible implementation. Finally, continuous evaluation of the effectiveness of these initiatives and adaptation based on real-world deployments will ensure a future-proof security posture for critical infrastructure.

In the face of a constantly evolving ICS cyber threat landscape, unwavering commitment to cybersecurity is paramount. Malicious actors will inevitably adapt their methods alongside technological advancements. However, by remaining informed, implementing established best practices, and engaging in continual assessment and improvement of the security posture, the site is fortifying the digital assets and upholding the integrity of sensitive information. While cyber threats remain a persistent reality, proactive knowledge and preparation offer the means to diminish their impact and secure operations of our critical infrastructures. Driven by an increased awareness of critical infrastructure vulnerabilities and the growing adoption of digital transformation, robust ICS security is no longer an option but a necessity to safeguard operations, economic stability, and public well-being.

References

Online Links / Research Papers / Journal Articles

[1] Cyber Security Infrastructure Sectors, CISA,
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[2] ICS Cybersecurity Guide, Nozomi,
https://www.nozominetworks.com/blog/ics-cybersecurity-guide

[3] Cyber Risk Management for Cyber Physical Systems (CPS), Claroty,
https://web-assets.claroty.com/cps-cyber-risk-management-(1).pdf

[4] IT/OT Convergence-The Essential Guide, Industrial Cyber,
https://industrialcyber.co/analyst-corner/the-essential-guide-to-it-ot-convergence/

[5] NIS DIRECTIVE (EU) 2016/1148
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

[6] EU Cybersecurity Act,
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

[7] NIS2 Directive (EU)) 2022/2555
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227

[8] Directive (EU) 2022/2557, Resilience of Critical Entities
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

[9] COMMISSION DELEGATED REGULATION (EU) 2023/2450, List of Essential Services
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302450

[10] Cyber Resilience Act
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

[11] Cybersecurity Framework, NIST
https://www.nist.gov/cyberframework

[12] How to Effectively Implement ISA 99/IEC 62443, Forescout,
https://www.forescout.com/resources/how-to-effectively-implement-isa-99-iec-62443-lp

[13] Overview of the ISA/IEC 62443 Standards & Effective IACS Security, Dragos
https://www.dragos.com/blog/isa-iec-62443-overview/

[14 International Society of Automation, ISA
https://www.isa.org/

[15] NIST SP 800-82 Rev. 3, NIST
https://csrc.nist.gov/pubs/sp/800/82/r3/final

[16] NIST SP 800-207, NIST
https://csrc.nist.gov/pubs/sp/800/207/final

[17] NIST SP 800-161 Rev.1, NIST
https://csrc.nist.gov/pubs/sp/800/161/r1/final

[18] ICS Techniques, MITRE ATT&CK
https://attack.mitre.org/techniques/ics/

[19] North American Electric Reliability Corporation. NERC
https://www.nerc.com/Pages/default.aspx

[20] Standards, NERC CIP
https://www.nerc.com/pa/Stand/Pages/default.aspx

[21] Security Directive-Pipeline-2021-01, US Transportation Security Administration (TSA)
https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2023/08/sdpipeline202101tsa.pdf?rev=ec9d6aa8bfe84826b95b699d7d6d7eba&hash=51F7B3A50971824BFA075CBB5A1392F2

[22] Pipeline Security Guidelines, Transportation Security Administration (TSA)
https://www.dwt.com/-/media/files/blogs/privacy-and-security-

blog/2023/08/pipeline_security_guidelines.pdf?rev=c3ebfb8def904591ace555b550a83903&hash=92B24409916069EEDE7F3A09AA22429F

[23] Security Directive Pipeline 2021-02D, US Transportation Security Administration (TSA) https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2023/08/tsasdpipeline202102dwmemo_07_27_2023.pdf?rev=7c936d94d515493d88b4b2f50c1a89ea&hash=A3FCFF2C73427AD6CE21383F717F94FF

[24] Cyber Resilience of ships, UR E26, IACS https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf

[25] Cyber Resilience of on-board systems and equipment, UR E27, IACS https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103853/UR-E27-Rev.1-Sep-2023-CLN.pdf

[26] MSC.429(98)/Rev.1 , IMO https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.429(98)%20Rev.1.pdf

[27] GUIDELINES ON MARITIME CYBER RISK MANAGEMENT, IMO https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

[28] UR E22 Rev.3 , IACS https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e22-rev2-cln-2

[29] Improving Safety Onboard Ships: IACS Puts Cybersecurity on the Roadmap, ABS Group https://www.abs-group.com/Knowledge-Center/Insights/Improving-Safety-Onboard-Ships-IACS-Puts-Cybersecurity-on-the-Roadmap/

[30] The Crisis of Convergence: OT/ICS Cybersecurit in 2023, Annual Report, TXOne Networks https://media.txone.com/prod/uploads/2024/02/TXOne-Annual-Report-OT-ICS-Cybersecurity-2023-v.pdf

[31] Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Eric M. Hutchins, Michael J. Clopper, Rohan M. Amin, Lockheed Martin Corporation (2011) https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[32] SANS ICS Cyber Kill Chain, and the MITRE ATT&CK Framework for ICS, Dr Diarmuid Ó Briain https://www.obriain.com/training/otsec2/odt/Topic_2-Cyber_Kill_Chain-MITRE_ATT&CK_for_ICS_odt.pdf

[33]The Industrial Control System Cyber Kill Chain, Michael J.Assante and Robert M.Lee (2015), https://www.sans.org/white-papers/36297/

[34] Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline, Chainalysis, https://www.chainalysis.com/blog/ransomware-2024/

[35] LoLockbit cybercrime gang says it is back online following global police bust, Reuters https://www.reuters.com/technology/cybersecurity/lockbit-cybercrime-gang-says-it-is-back-online-following-global-police-bust-2024-02-26/

[36] CVE-2023-3824, NIST NVD, https://nvd.nist.gov/vuln/detail/CVE-2023-3824

[37] To Kill a Centrifuge, A Technical Analysis of What Stuxnet's Creators Tried to Achieve, Ralph Langner (2013) https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

[38] Triton Malware Spearheads Latest Attacks on Industrial Systems, Thomas Roccia, Trellix https://www.trellix.com/blogs/research/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/

[39] Trisis analysis report by Dragos, https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

[40] APT Cyber Tools Targeting ICS/SCADA Devices, CISA Advisory https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a

[41] INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems, Mandiant, https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool

[42] Cybersecurity Risk, NIST, https://csrc.nist.gov/glossary/term/cybersecurity_risk

[43] Industrial Cyber Risk Management, Jason D.Christopher, Dragos
https://hub.dragos.com/hubfs/Whitepapers/Industrial-Cyber-Risk-Management-2021March.pdf?hsLang=en

[44] Common Criteria for Informational Security Evaluation, Wikipedia,
https://en.wikipedia.org/wiki/Common_Criteria

[45] Improving OT Defense and Response with Consequence-Driven ICS Cybersecurity Scoping, Dragos
https://www.dragos.com/wp-content/uploads/ConsequenceDrivenICSCybersecurityScoping_Dragos-1.pdf

[46] Operationalizing MITRE Engage: Deception Opportunities with APT Cyber Tools Targeting ICS/SCADA Devices, MITRE Engange
https://medium.com/mitre-engage/operationalizing-mitre-engage-deception-opportunities-with-apt-cyber-tools-targeting-ics-scada-fcf5150705e8

[47] ICS Cybersecurity Requires Passive and Active Defense, ARC Advisory Group
https://www.arcweb.com/blog/ics-cybersecurity-requires-passive-active-defense

[48] The Sliding Scale of Cyber Security, Robert M.Lee, SANS
https://sansorg.egnyte.com/dl/GJEumszLQX

[49] Purdue Enterprise Reference Architecture, Wikipedia,
https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

[50] Defense-in-Depth, Imperva
https://www.imperva.com/learn/application-security/defense-in-depth/

[51] The Intelligence Cycle and its Importance in the Competitive Intelligence Practices, Thandra Consulting
https://www.thandraconsulting.com/blogs/post/the-intelligence-cycle-and-its-importance-in-the-competitive-intelligence-practices

[52] Bringing Military Intelligence to Business Intelligence through Cognitive Artificial Intelligen, Arwin Datumaya Wahyudi Sumari, Edi Nuryatno, Ika Noer Syamsiana
https://www.researchgate.net/publication/356891886_Bringing_Military_Intelligence_to_Business_Intelligence_through_Cognitive_Artificial_Intelligence

[53] SANS addresses ICS/OT Cyber Defense, SANS
https://www.sans.org/blog/sans-addresses-ics-ot-cyber-defence/

[54] Purple Teaming and Threat-Informed Detection Engineering, Jorge Orchilles, SANS
https://www.sans.org/blog/purple-teaming-threat-informed-detection-engineering/

[55] Consequence-Driven ICS Risk Management, Deans Parsons, SANS,
https://www.sans.org/blog/consequence-driven-ics-risk-management/

[56] NIST.SP.800-61r2, Computer Security Incident Handling Guide, Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone,
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[57] CIP-008-6 — Cyber Security — Incident Reporting and Response Planning
https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf

[58] Critical Infrastructure and the Cloud: Policy for Emerging Rrisk, Tianjiu Zuo, Justin Sherman, Maia Hamin, and Stewart Scott (2023),
https://dfrlab.org/wp-content/uploads/sites/3/2023/07/critical_infra_and_the_cloud.pdf

[59] SolarWinds: "IT's Pearl Harbor", Steven Vaughan-Nichols
https://www.csoonline.com/article/573767/solarwinds-its-pearl-harbor.html

[60] Hacking of Government Email Was Traditional Espionage, Official Says, The New York Times
https://www.nytimes.com/2023/07/20/us/politics/china-hacking-official-email.html

[61] CISA Roadmap for Artificial Intelligence (2023),
https://www.cisa.gov/sites/default/files/2023-11/2023-2024_CISA-Roadmap-for-AI_508c.pdf

[62] ICSvertase: A Framework for Purpose-based Design and Classification of ICS Honeypots, Stash Kempinski, Shuaib Ichaarine, Savio Sciancalepore, Emmanuele Zambon (2023),
https://dl.acm.org/doi/pdf/10.1145/3600160.3605020

[63] Cybersecurity for industrial control systems: A survey (2019), Deval Bhamare, Maede Zolanvari, Aiman Erbad, Rajeev K. Jain, Khaled Khan, Nader Meskinhttps://www.sciencedirect.com/science/article/abs/pii/S0167404819302172

[64] http://conpot.org/

[65] HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems, Efrén López Morales, Carlos E. Rubio-Medrano, Adam Doupé, Ruoyu Wang, Yan Shoshitaishvili, Tiffany Bao & Gail-Joon Ahn (2020)

[66] Using Global Honeypot Networks to Detect Targeted ICS Attacks, Michael Dodson, Alastair R.Beresford, Mikael Vingaard (2020), https://ccdcoe.org/uploads/2020/05/CyCon_2020_15_Dodson_Beresford_Vingaard.pdf

[67] HoneyICS: A High-interaction Physics-aware Honeynet for Industrial Control Systems, Marco Lucchese, Francesco Lupia, Massimo Merro, Federica Paci, Nicola Zannone, Angelo Furfaro (2023, https://dl.acm.org/doi/pdf/10.1145/3600160.3604984

[68] Cross-Sector Cybersecurity Performance Goals, CISA, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals