LMNTRIX

BE THE HUNTER | NOT THE PREY

WHITE PAPER

INDUSTRIAL CONTROL SYSTEM SECURITY GUIDE

LMNTRIX XDR FOR INDUSTRIAL STRENGTH OT AND IOT SECURITY AND VISIBILITY

2023

LMNTRIX USA.
333 City Blvd West, 17th Floor,
Suite 1700, Orange, CA 92868
+1.888.958.4555

LMNTRIX UK.
200 Brook Drive, Green Park,
Reading, RG2 6UB
+44.808.164.9442

LMNTRIX SINGAPORE.
60 KAKI BUKIT PLACE#05-19
EUNOS TECHPARK
+65.3159 0639

LMNTRIX INDIA.
VR Bengaluru, Level 5, ITPL Main Rd,
Devasandra Industrial Estate,
Bengaluru, Karnataka 560048,
+91-22-49712788

LMNTRIX Australia.
Level 25, 100 Mount Street,
North Sydney NSW 2060
+61.288.805.198

lmntrix.com

LMNTRIX
BE THE HUNTER | NOT THE PREY

CONTENTS

EXECUTIVE SUMMARY

Industrial control system security solutions are an essential component in managing industrial risks. An industrial risk is an event with the potential to cause loss of life, environmental damage, loss of assets, financial loss, reputational damage, or other business disruption. The evolution of industrial control systems from isolated equipment with manual control to networked and automated solutions has resulted in a step change in the types of industrial risks that require management. The unintentional or deliberate misoperation of networked components or their technical failure requires advanced security solutions to provide adequate protection that reduces the risks to acceptable levels.

The challenge for industrial control system operators is balancing risk management across multiple risk types. For example, operational risks impacting production processes may need to prioritize risk treatments that assure continued operation. However, this approach may conflict with security risks, where risk treatments often look to isolate or disable components that have been compromised with malware. Industrial control system risk management requires a holistic approach that balances risks, treatments, and operational requirements.

Advanced managed intelligent industrial control system security solutions provide the answer to maximizing protection with their detect and respond strategies compatible with the organization's operating requirement. Managed detect and response services offer a turnkey technology approach for organizations looking to acquire the capability for threat detection, response, and investigation. This solution is ideal for processing and manufacturing businesses with little or no in-house cyber security protection capability. However, most managed security services are developed for information technology solutions. Operational technologies generally have significantly different characteristics and requirements. This difference is particularly significant for industrial control systems. The LMNTRIX XDR and Active Defense managed detection and response services employ architecture that provides a complete IT-OT security solution that protects the corporate network past the perimeter, the bridge between IT and OT networks and operator workstations and SCADA devices within the OT network.

This white paper explores the issues around industrial control system security solutions to help you determine your cyber security protection requirements to select the appropriate managed security solution for your operational technology systems.

OVERVIEW OF
INDUSTRIAL CONTROL SYSTEMS

GENERAL INTRODUCTION TO ICS

Industrial Control Systems (ICS) is the collective term for manufacturing and process automation systems. ICS can also be referred to as Industrial Automation and Control Systems (IACS) or Operational Technology (OT). ICS may include components standard with traditional information technology (IT) systems but with significantly different operational and management requirements.

Generally, the term ICS refers to the collection of separate control systems and components working together to automate and manage various industrial processes. For example, ICS can include distributed control systems, process control systems which include supervisory control and data acquisition systems, and safety instrumented systems.

- A distributed control system (DCS) is the term for ICS responsible for managing processes across a facility. This centralized processing system controls processing nodes distributed around the facility, each performing specific tasks.

- A process control system (PCS) is the term for ICS responsible for continuously monitoring and managing production line operations with manual interactions and interventions.

- Supervisory control and data acquisition system (SCADA) is a remote access process control system responsible for monitoring and controlling remote operations.

- A safety Instrumented System (SIS) is a dedicated safety monitoring system designed to independently monitor ICS operations and impose safe states in the event of a safety-related incident.

For developed nations, ICS are central to the operation of critical national infrastructure. However, such ICS are also typically highly interconnected and mutually dependent systems that are commercially operated and maintained, which is a challenge for making them secure against advanced persistent threats. For example, in the US, only around 15% of NCI is managed by federal and state agencies.

Each industry will utilize ICS tailored to its specific processing and manufacturing requirements. The primary purpose of the ICS is to improve efficiency through autonomous processes to replace manual inputs. Applications include industrial automation, energy production and distribution, utility supply, and facilities management.

In this paper, we will explore the cyber security issues around ICS and the measures that are taken to protect ICS against accidental circumstances, actions or events, or deliberate attacks. These threats can originate from the Internet, external networks (corporate or third party), maintenance activities, software upgrades, and unauthorized access. They can result in incidents with significant health, safety, or environmental consequences and loss of essential services.

ICS are readily available with increasing use of commercial-off-the-shelf information technology (IT) solutions and open technologies. Non-proprietary systems such as Microsoft operating systems are also increasingly being used for both control processing and user interfaces. These solutions enable connectivity and information exchange with other systems, including external corporate and third-party networks. ICS are thus increasingly merging with IT networks and systems.

While this paper focuses on ICS, the security guidance is equally applicable to other types of networked control systems, including:

- Advanced Metering Infrastructure
- Building Automation Systems
- Building Management Control Systems
- Closed-Circuit Television (CCTV) Surveillance Systems
- Digital Signage Systems
- Digital Video Management Systems
- Electronic Security Systems
- Emergency Management Systems
- Energy Management Systems
- Fire Alarm and Suppression Systems
- Intrusion Detection Systems
- Laboratory Information Management Systems (LIMS)
- Laboratory Instrument Control Systems
- Lighting Control Systems
- Physical Access Control Systems
- Smoke and Purge Systems
- Vertical Transport System (Elevators and Escalators)

The evolution of ICS is being hastened with the adoption of the Industry 4.0 philosophy. This seeks to improve production flexibility and efficiency by leveraging automation, computerization, real-time monitoring, and interconnectivity. Unfortunately, this increased connectivity and use of non-proprietary systems have exposed ICS to the same cyber threats as conventional information systems. The issue is that traditional air-gapped ICS solutions have not needed to have been designed to be secure, so security controls are immature or, in some cases, absent. This deficiency has resulted in a significant increase in incidents affecting ICS.

A typical ICS comprises control loops that control and monitor one or more processes. HMI provide the primary means of managing the process supported by remote maintenance and diagnostics tools. The ICS is built using an array of network protocols on layered network architectures. Controllers manipulate the processes using control devices such as actuators, servos, and motors based on sensor information. The controller interprets the process information and generates control commands using algorithms defining the process's theoretical operation.

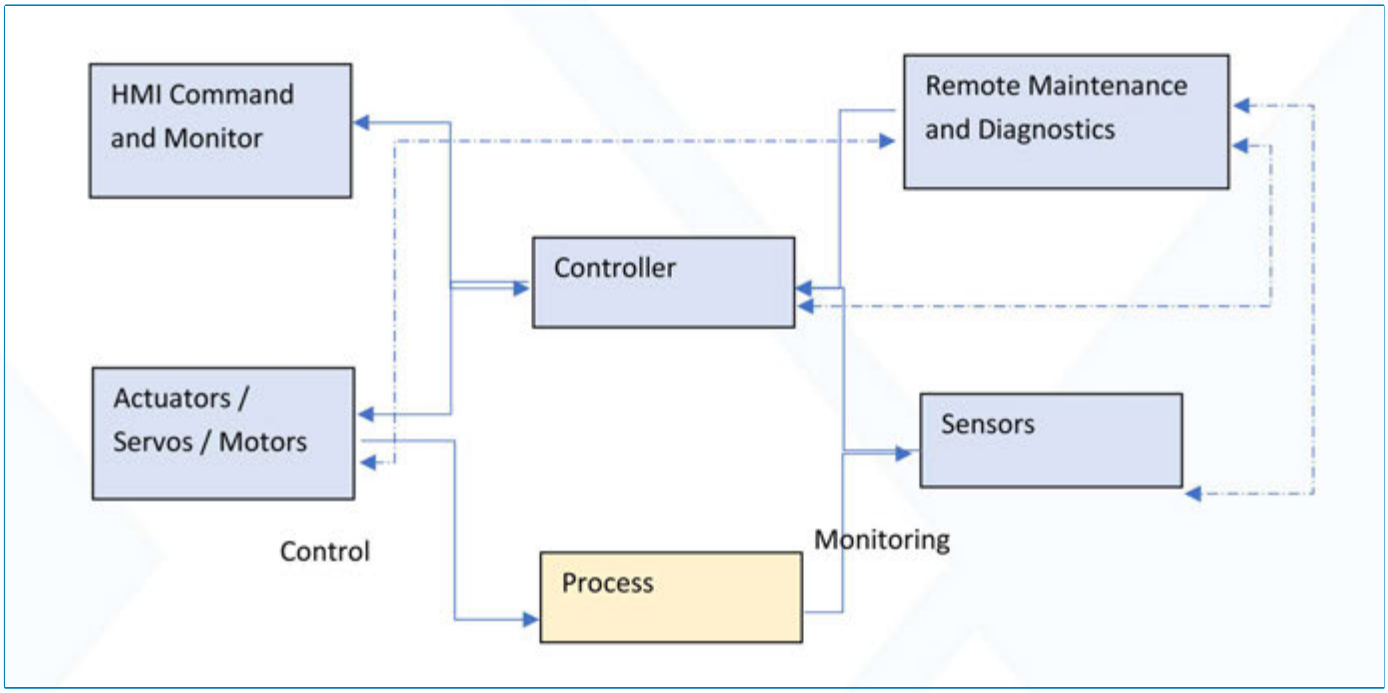

Figure 1 - Typical ICS Operating Model

ICS ARCHITECTURE

ICS architecture can range from simple programmable logic controllers (PLC) and local control systems to distributed control systems. In addition, the architecture can include features such as redundancy or independent safety monitoring depending on the application and requirements for reliability and dependability.

Complex ICS architecture can be represented using the Purdue Enterprise Reference Architecture (PERA) structural model, which includes a security layer and layers for physical processes, sensors, supervisory controls, operations, and logistics.

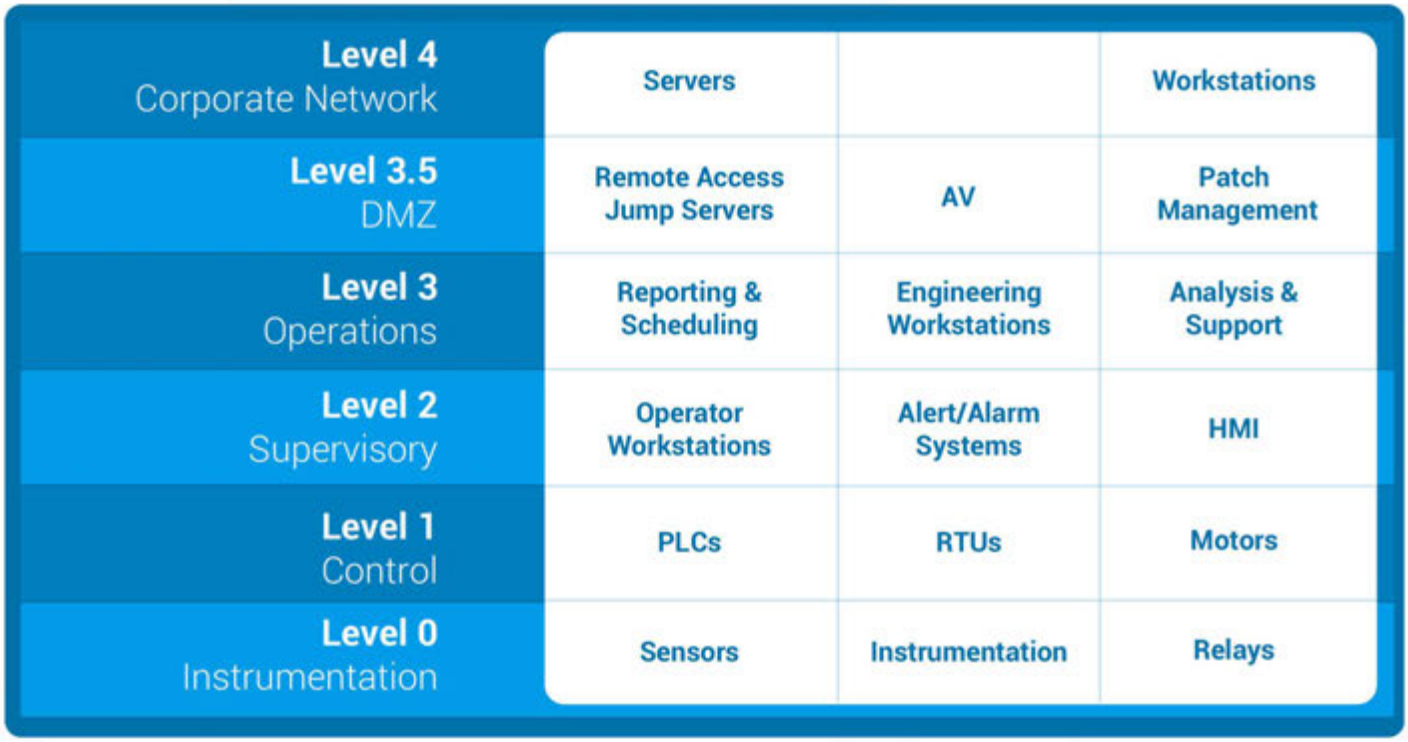

Figure 2 - Purdue Enterprise Reference Architecture Model

- **Level 0** represents the physical process managed by the ICS.
- **Level 1** represents the physical process's intelligent monitoring and control components, including sensors, instrumentation, switches, actuators, and IoT devices. Network communications are typically proprietary solutions.
- **Level 2** represents the supervisory control systems,including PLC, DCS, PCS, and SCADA, as well as the human-machine interfaces (HMI) and remote access devices. Network communications typically use Modbus or other standard ICS protocols.
- **Level 3** represents the operational management systems that control and monitor production processes, including batch management and performance monitoring. Such systems include manufacturing operations management systems (MOMS) and manufacturing execution systems (MES). In addition, this level includes record-keeping systems such as data warehousing or database solutions. Network communications typically use dedicated network infrastructure based on standard communications protocols.
- **Level 3.5** represents the ICS demilitarized zone (DMZ) that includes network security controls such as firewalls, switches, and proxies that separate the ICS from the organization's information processing systems. This layer is essential where bi-directional information flows exist between the ICS and the broader business systems.
- **Level 4** represents the business's IT systems for production management functions, including logistics and supply chain management, and includes servers for applications, databases, and file management.
- **Level 5** represents the corporate network encompassing all business IT systems, including production management and other functions such as sales, marketing, accounting, finance, and human resources.

GENERAL INTRODUCTION TO SCADA AND MODBUS

AN OVERVIEW OF SCADA

A SCADA system is a network of sensing and controlling devices within an ICS connected via a centralized hub that performs data acquisition and command functions. The hub is responsible for sending instructions to all connected devices to achieve the required physical process that the SCADA system manages.

A SCADA system comprises four subsystems:

- A data communications subsystem manages data transfer between the sensing and controlling devices and the central processing hub via a local network.
- A data acquisition subsystem retrieves real-time data from all the connected sensing devices.
- A monitoring subsystem analyses the retrieved data and presents it to the operator through the HMI.
- A control subsystem generates commands for controlling devices based on automated outputs from the monitoring subsystem and manual inputs from the operator via the HMI.

A SCADA system can also include functionality for managing scheduled and predictive maintenance, fault management, and performance monitoring.

SCADA systems are designed to be reliable and robust with simple operation and maintenance, but they are not secure by design. This was not an issue with standalone systems air-gapped from other networks. However, a move from proprietary technologies to more standardized and open solutions coupled with increasing connectivity has exposed their inherent vulnerability.

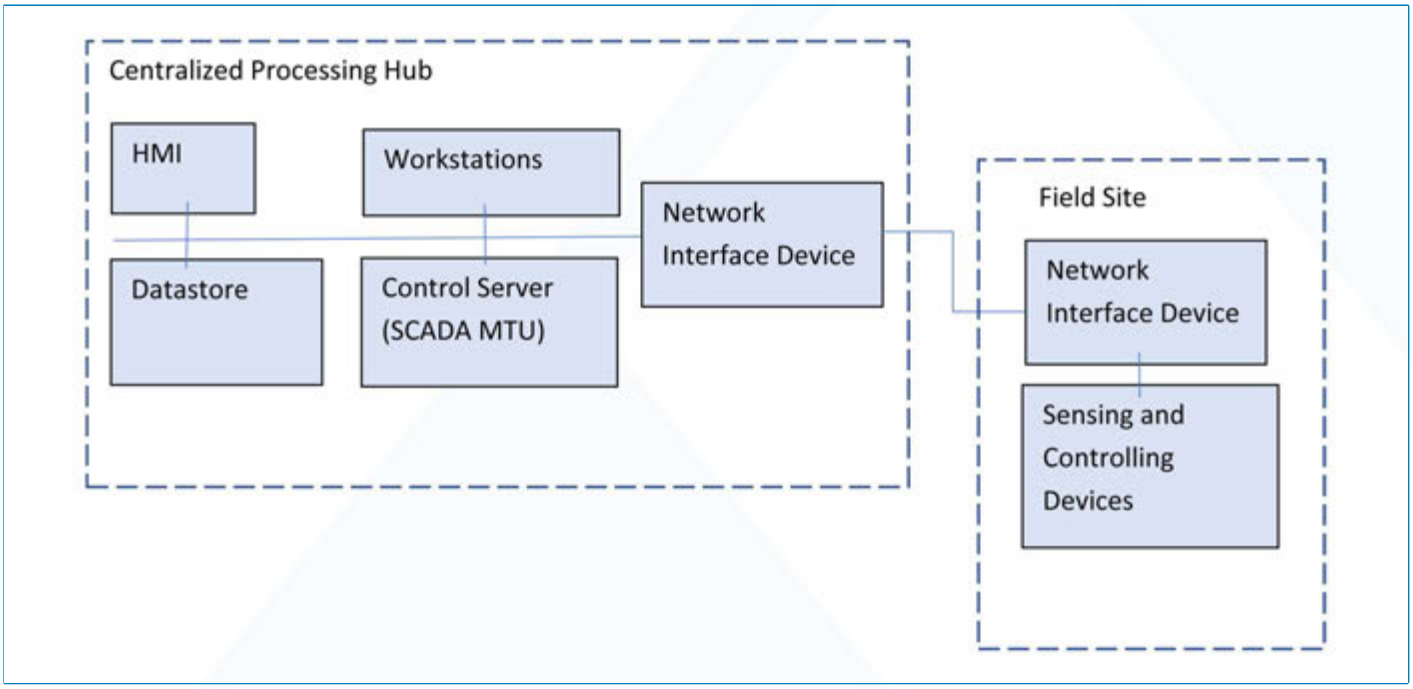

Figure 3 - SCADA General Layout

AN OVERVIEW OF NETWORKING

ICS, including SCADA, utilizes a local network to transfer data between components. Typically, this network will be a Fieldbus, one of the families of standardized networks used in automated industrial computer networks. Fieldbus is defined by the International Electrotechnical Commission (IEC) standard IEC 61784/61158.

Fieldbus was explicitly designed for real-time distributed control and can support common network topologies, including star, ring, daisy-chain, branch, and tree configurations. In addition, it is designed to deliver high availability and reliability with low installation and maintenance costs for ICS with thousands of devices over a network that can cover large physical distances in hostile environmental conditions.

There are numerous implementations of the Fieldbus standard in use, including the Controller Area Network (CAN) used in vehicles, INTERBUS used in the manufacturing industry along with ControlNet, DeviceNet, and the more commonly adopted Modbus, as detailed below.

AN OVERVIEW OF MODBUS

Modbus was developed in 1979 by Modicon to connect PLC-based field devices to industrial controllers and was the first Fieldbus implementation used in industrial automation. Modbus was initially designed for use over serial communication links using RS-232/RS-485 protocols before being adapted for use over networks using TCP/IP and Ethernet protocols.

Modbus uses a master/slave (client/server) model for communications. The master device controls all transmissions over the network and is responsible for determining when to allow each slave device to transfer data onto the network.

Modbus is limited in its application because it can only support 247 separate devices on a single data link or 256 devices for TCP connections. Modbus also uses a fixed data package size that prevents the transfer of large binary objects. Finally, it has no inbuilt security controls to prevent unauthorized communications or protect the data in transit from interception or modification.

Modbus popularity is based on its simplicity. It focuses on high availability, but this is at the expense of having zero confidentiality protection and minimal integrity protection using a simple checksum that does not prevent unauthorized modification of commands or data.

ICS MISCONCEPTIONS

Many misconceptions regarding security for ICS need to be addressed to prevent incorrect assumptions or understandings from causing disproportionate or inadequate application of security controls.

ICS IS THE SAME AS IT

ICS are not the same as traditional information technology systems; they have characteristics that affect their applicable threats and vulnerabilities that need to be considered in assessing their cyber security.

- System functionality focuses on command and control functions with data acquisition and processing operations rather than information management and messaging.
- Operating constraints focus on maintaining process operations with restrictive availability and downtime constraints. Unfortunately, this always-on approach can be at odds with security solutions that look to isolate systems in response to incidents.
- System operation is deterministic, with actions based on information content rather than context and focusing on system control.
- System architecture is more rigid, with lower rates of change, longer equipment life, and fewer gateways. This low entropy offers fewer targets for an attack but means vulnerabilities have a longer window of opportunity for exploitation.
- The physical environment typically has higher temperatures, vibration, particulate, and electromagnetic interference levels than the controlled environment found in computer rooms requiring more robust construction and enclosures.
- Component Lifecycle is typically significantly longer than standard computer components due to higher capital investment, lower innovation rates, and the adverse impact of upgrade processes on system availability. This creates issues with component obsolescence impacting maintainability.
- Component Complexity is typically significantly higher with less emphasis on modular systems with line replaceable units seen in computer systems and more use of monolithic construction techniques.

SCADA IS THE SAME AS **ICS**

The term supervisory control and data acquisition systems (SCADA) is often incorrectly used when referring to an ICS. A SCADA can often be mistakenly thought of as the whole ICS. SCADA is a process control system (PCS) that can be part of an ICS, but an ICS does not necessarily include a SCADA element. For example, in the Purdue structural model, SCADA is part of level 2, while the ICS is at level 3. There may be an ICS wholly comprised of a SCADA solution, but typically the SCADA is a component of the overall ICS.

ICS ARE ISOLATED

While ICS were traditionally isolated systems with no network connectivity, this is no longer the case. Even where ICS is air-gapped, this does not protect those systems from attacks. Look at the Stuxnet case study we've included in this paper for a great example of their vulnerability. Modern ICS will have multiple paths of network connectivity, typically management systems such as business management systems for process control and building management systems for environmental management. The components will also rely on internet connectivity through landline or mobile telephone networks for service and maintenance functions.

PROPRIETARY SOLUTIONS ARE IMMUNE

ICS components traditionally use proprietary operating systems and communications protocols immune from computer malware that cannot interact with these systems. However, where this proprietary nature still exists, ICS is now a sufficiently valuable target to warrant attackers investing resources to create targeted malware and devise attack vectors. ICS typically attract the attention of hostile or competing nation-states and organizations with the resources to develop sophisticated and advanced persistent threats. Another issue is that such proprietary systems do not tend to have built-in security controls or have not been exposed to real-world threats. This means they have not undergone continual updates to resolve identified vulnerabilities like more common open-source or non-proprietary solutions.

SECURITY CONTROLS IMPACT PERFORMANCE

ICS is generally a high-availability real-time system, and there is a general misconception that security controls will interfere with responsiveness and availability, compromising system performance. However, security solutions are widely available that protect, monitor, and respond to attacks without affecting system performance. Furthermore, these can be configured to maintain the required availability for those classes of security events where the cost of system compromise is deemed acceptable compared with the financial impact of halting the attack by impacting system availability.

A BRIEF HISTORY OF ICS

ICS typically evolved from introducing IT capabilities to control and monitor operations that manual or mechanical processes had previously managed. Efficiency and performance improvements accompanied by cost savings drove this change.

Industrialization started in the 1780s with the first industrial revolution. Water and steam power were used to drive mechanical production facilities in place of manual processes, beginning in the cotton and wool mills.

The second industrial revolution began in the 1870s with assembly lines' development and electric power's use to drive mass production.

The third industrial revolution saw the start of the ICS introduction to implement the digitization and automation of production processes. The first functional ICS was implemented in 1958 at the Texaco refinery in Port Arthur, Texas. It was built using a bespoke Ramo-Wooldridge RW-300 computer with magnetic drum memory. This system went on to be developed for use in electric power stations and nuclear power plant control systems.

The 1960s saw the development of mainframe-based computer control systems with a central control room linked to industrial systems using analog relays with miles of discrete wiring.

Minicomputer-based control systems appeared in the late 1960s and early 1970s, allowing the transition to distributed control solutions in the 1970s.

The first operational DCS was developed by Honeywell for the Yokogawa Electric Corporation of Japan in 1975 to manufacture industrial instruments.

The 1970s also saw the introduction of the SCADA system concept

The availability of PLC in the 1980s saw the introduction of true DCS, supported by the development of the TCP-IP network communication technology and Ethernet-based systems.

The 1980s also saw the widespread adoption of digital Fieldbus technology for sensor communications.

The 1990s saw the move from bespoke and proprietary UNIX-based solutions to Microsoft Windows-based environments for distributed process control systems with greater use of commercial off-the-shelf (COTS) components.

We have entered the fourth industrial revolution with robotics, IoT, and cloud technologies to automate complex tasks. As a result, production practices can now be flexible, adaptable, and scalable. The fourth industrial revolution started around 2015 with increased integration and connectivity between physical and digital processes and leveraging machine learning and artificial intelligence technologies.

OVERVIEW OF
ICS SECURITY MANAGEMENT

ICS THREAT LANDSCAPE

OVERVIEW

While ICS face threats from sophisticated targeted attacks, they also are susceptible to the same general untargeted attacks as traditional IT systems. The latter is particularly true to Internet-connected ICS, while standalone equipment or ICS architectures built on private networks will be more affected by the former.

The threat landscape for ICS is evolving, with attackers recognizing the value of intellectual property held within ICS that can be exfiltrated and leveraged for financial gain or the potential disruption of manufacturing processes resulting in loss of availability, loss of production, and physical damage. Other attack motivations include disruption to production processes resulting in manufacturing quality issues to inflict financial or reputation damage. Alternatively, attackers may seek to interfere with safety controls to cause a safety-related incident or accident for the same result.

The following sections list the currently most commonly used attacks causing severe and consequential damage.

MALWARE INFECTION VIA PHYSICAL CONNECTIVITY

Malware infection via physical connectivity occurs through the connection of devices such as removable media and external hardware to the ICS network. USB flash drives, in particular, are widely used in industrial processes to transfer information directly into production equipment. The same devices will often also be connected to other networks within the organization, and it's not uncommon for workers to use them for connection to third-party systems and even for personal use. A lack of security awareness and weak controls on the use of removable devices make these a common cause of malware infection.

Typical threat scenarios include:

- A USB flash drive infected with malware, when connected to an insecure office or personal computer, is subsequently connected to ICS equipment.
- A portable computer with internet connectivity is connected to the ICS network to perform a maintenance activity.

Best practices to countermeasure against malware infection via physical connectivity should include the enforcement of strict security policies for the use of removable media or portable computers, including:

- Physical prevention of device connection on equipment where the use of removable media or portable computers is not necessary by disabling hardware.
- Physical prevention of device connection on equipment to unauthorized personnel by installing security locks.

- Restricting use to only authorized removable media devices or portable computers issued and managed by the organization.

- Enforcing malware scanning of all removable media and computing devices whenever connected to any equipment or network access point before logical access is enabled.

MALWARE INFECTION VIA NETWORK CONNECTIVITY

Networks of all types and applications with Internet and Intranet connectivity typically use standard components such as operating systems, webservers, and applications. Such networks will also include typical applications such as file servers, datastores, e-mail clients, and browsers. New vulnerabilities for such devices and applications are discovered daily. Such vulnerabilities provide an attack vector for any remote threat agent seeking to gain unauthorized access if left unpatched. Sophisticated threat actors, such as the advanced persistent threats supported by nation-states, have the skill and capability to uncover and exploit previously unknown vulnerabilities for which there is no patching. Attackers can then use their unauthorized access to networks by uploading malware to attack the infected systems or propagate their attack toward a more valuable target.

Typical threat scenarios include:

- The exploitation of a known vulnerability that has not been mitigated by security controls such as patching or configuration changes.

- The exploitation of an unknown vulnerability using a so-called zero-day exploit that security controls cannot detect through techniques such as intrusion detection, behavioral analysis, or deception techniques.

- The exploitation of coding weaknesses in Internet-facing applications, such as cross-site scripting or injection attack techniques.

- The exploitation of weaknesses in access control and authentication processes to impersonate or steal the credentials of a legitimate user.

- The exploitation of any unrecognized network connectivity invisible to boundary security controls, such as undocumented service links using mobile telecommunications connectivity in industrial equipment.

Best practices to countermeasure against malware infection via network connectivity should include:

- Robust boundary security controls to limit authorized access.

- Intelligent security monitoring solutions capable of detecting unusual or suspicious behavior within a network.

- Segregation of networks with different criticalities and functionality using robust security controls to limit lateral movement.

- A patching policy that can minimize the window of opportunity for exploitation of known vulnerabilities within the constraints of system availability.

- Security hardening and monitoring of all network-connected equipment.

- Logical isolation of equipment that cannot be adequately secured, such as unsupported legacy equipment or unpatched devices.

INTRUSION VIA REMOTE ACCESS

ICS commonly allows remote access for third-party maintenance purposes. Historically such access has employed insecure techniques, including default and hardcoded passwords. Also, accounts may be shared across multiple organizations, and unsegregated access to the entire ICS may be provided for each remote connection. The lack of authentication, authorization, and flat network structures creates significant security risks.

Remote access by maintainers also typically includes equipment reprogramming and application patching activities. These actions can create significant challenges in protecting against malware infection or misconfiguration.

Typical threat scenarios include:

- Direct attacks on a maintenance access point to gain unauthorized access.
- Attacks on third-party service providers to gain access to the ICS using stolen credentials or malware-compromised devices
- Unauthorized access to maintenance access points using stolen devices

Best practices to countermeasure against intrusion via remote access connectivity should include:

- Enforcement of robust access control policies for remote access with comprehensive auditing.
- Strong security controls to limit authorized access.
- Secure authentication processes for remote access.
- Segregation of ICS to restrict remote access to specific components for each access point.
- Secure encryption of all data in transit over remote access connections.

SOCIAL ENGINEERING AND PHISHING

Social engineering techniques are typically used to gain unauthorized access to systems using non-technical means to obtain access credentials. These techniques exploit humans' innate traits of helpfulness, curiosity, respect, and fear of authority figures. For example, a request for urgent help or an order from a senior in the organization will often prompt users to provide sensitive information without questioning or checking if the request is legitimate. While social engineering attacks can be via telephone calls or text messages, the most common form is via e-mail, a technique known as phishing. Phishing e-mails will either attempt to extract information from the recipient or persuade them to act by clicking on a hyperlink or opening an attachment.

Typical threat scenarios include:

- An attacker sends phishing e-mails to all employees of an organization designed to persuade recipients to reveal their passwords.
- An attacker sends a spear-phishing e-mail to a targeted recipient designed to persuade the recipient to reveal specific sensitive information.
- An attacker sends untargeted phishing e-mails designed to convince recipients to open an attachment containing malware.
- An attacker gains physical access to equipment by impersonating a user or third-party service provider.

Best practices to countermeasure against social engineering attacks should include:

- Technical controls to detect and block suspicious communications.
- Robust access controls with comprehensive auditing.
- Security training and awareness programs.

TECHNICAL AND HUMAN ERROR

The nature of ICS means that equipment failures can have a significant consequence on business operations. For example, a malfunction that halts a critical production line can cause financial or reputation damage if not quickly remedied. Failures can be due to technical failures or human errors that result in misconfiguration or unintentional operations.

Typical threat scenarios include:

- Incorrect configuration of equipment results in erroneous operations.
- Incorrect configuration of equipment creates a vulnerability that an attacker can exploit.
- Accidental release of sensitive information that can be invaluable to an attacker, such as access credentials or configuration settings.

Best practices to countermeasure technical and human error should include:

- Robust maintenance and processes that support the rollback of configuration changes in the event of a subsequent failure.
- Automated system monitoring and auditing to detect equipment misconfiguration.
- Release of sensitive information on a need-to-know basis with processes for changing access credentials in the event of known or suspected disclosure to unauthorized parties.
- Security training and awareness programs.

INTENTIONAL INSIDER ATTACKS

Personnel responsible for managing ICS have the ability to inflict significant harm to business operations. Unintentional attacks are covered above by human error. The more severe form is the deliberate infliction of damage by an individual with authorized access to the system under attack. The typical motivators behind an intentional insider attack are financial reward through the theft of sensitive information, including intellectual property, an act or retaliation in response to a perceived in justice, or actions due to coercion such as physical threats or blackmail. Insider attacks are mainly an issue when a user's employment is terminated, but their system access credentials remain active, allowing revenge acts of theft or sabotage.

Intentional insider attacks may also be unintentional on the attacker's part. For example, social engineering techniques can effectively persuade a user to unknowingly perform a harmful action in the belief that they are following a colleague's or superior's instructions.

Typical threat scenarios include:

- Installation of malware.
- Incorrect configuration of equipment creates an exploitable vulnerability.
- Theft of sensitive information that can be used by an external attacker, such as access credentials or configuration settings.

Best practices to countermeasure technical and human error should include:

- Automated system monitoring and auditing to detect abnormal user behavior.
- Release of sensitive information on a need-to-know basis with processes for changing access credentials in the event of known or suspected disclosure to unauthorized parties.
- Processes for revoking access credentials for users immediately once access is not required.

DOS ATTACKS

Denial of service (DoS) attacks disrupt networks by overloading transmission capacity with rogue messages. In a typical attack, internet-facing applications send high volumes of queries that consume all available processing resources. This leaves the affected system unable to respond to legitimate queries. Blocking a single source of malicious messages is relatively simple, so a typical attack will utilize a large number of different message sources in a coordinated attack in what is termed a distributed denial of service (DDoS).

Typical threat scenarios include:

- DDoS attacks on internet-connected applications using rentable botnets compromise the availability of those applications and disrupt business operations.
- DoS attacks on networked ICS components are designed to cause that component to cease function.
- DoS attacks on externally accessible networks, such are wireless networks, to prevent legitimate use of that network.

Best practices to countermeasure against denial-of-service attacks should include:

- Robust security hardening and configuration of network access points.
- Third-party DDoS protection solutions.
- Use of dedicated cabled networks with robust physical and logical protection for critical processes
- Redundancy of critical communications using diverse technologies to prevent common mode vulnerabilities.

ICS WEAKNESSES AND VULNERABILITIES

Assessments undertaken by US Government Departments have identified the most common weaknesses and vulnerabilities in ICS and constituent components as follows:

SYSTEM VULNERABILITIES:

- The inadequate or missing security documentation.
- Inadequate software configuration management causes vulnerability to unpatched third-party applications or disabled security controls, or weak backup and restoration ability.
- System reliance on unsupported legacy systems or outdated devices that cannot be secured.
- Inadequate credentials policies, including a lack of separation of duties across critical functions or failure to terminate remote access sessions.
- Inadequate credentials management causes vulnerability to unprotected plaintext credentials in transit or storage, the use of hard-coded credentials, or ineffective credential policies, including default access credentials and weak passwords.
- Inadequate testing environment
- Network design weaknesses include lack of network segmentation, including control networks used for non-control traffic or control network services outside the control network, defined security perimeter, functional demilitarized zones or incorrectly configured firewalls or network devices, or poor port security on network equipment causing vulnerability to network attack vectors and lateral movement.
- Inadequate audit and accountability functions from insufficient logging, poor practices, lack of security assessments or audits, and weak enforcement of remote access policies cause vulnerability to undetectable attack vectors and inadequate methods of monitoring control network events.
- Insufficient disaster recovery preparation due to inadequate disaster recovery policies or directives or a lack of understanding of disaster recovery techniques.
- Inadequate ICS-specific security awareness training programs.

DEVICE VULNERABILITIES:

- Improper input validation causes vulnerability to buffer overview, command injection, cross-site scripting, and path traversal.
- Improper access controls, including incorrect default permissions and the use of insecure services in conventional IT systems, cause vulnerability to unauthorized access.
- Improper authentication, including missing authentication for critical functions, a lack of restrictions for excessive authentication requests, a lack of lockout for failed attempts, and use of client-side authentication, causing vulnerability to man-in-the-middle attacks.
- Insufficient data authenticity verification causes vulnerability from missing download integrity checks or cross-site request forgery.
- Poor coding practices cause vulnerability to NULL pointer dereferencing or information leakage from debug functions.
- Poor cryptographic implementation, including the use of broken or weak algorithms, causes vulnerability to information leakage.
- Weak controls for removable media management and connection

MODBUS COMMUNICATIONS VULNERABILITIES:

- Modbus diagnostic commands allow attackers to scan ICS for Modbus-connected devices and extract useful information.
- Modbus messages are transmitted as plain text, allowing an attacker to intercept communications.
- Modbus messages have no authentication checks within the communications protocol to protect against an attacker creating messages.
- Modbus messages have no integrity checks within the communications protocol to protect against an attacker modifying a message.
- The Modbus protocol contains inherent vulnerabilities that enable attackers to create a buffer overflow condition or perform a denial of service attack.

INDUSTRIAL CONTROL ASSESSMENT

The first step in identifying weaknesses and vulnerabilities in an ICS is conducting an industrial controls assessment. For example, the LMNTRIX ICS Security Assessment uses non-invasive methods to assess an industrial facility's overall cyber security posture. This assessment is specifically designed to meet the needs of organizations concerned about the operational risk associated with aggressive probing, scanning, software agents, or other more aggressive security evaluation techniques.

The LMNTRIX ICS Security Assessment combines a remote workshop-based ICS architecture review with a detailed technical analysis of firewall configurations and active production ICS network traffic. LMNTRIX's ICS specialists are fluent in the OT language and work directly with the engineers responsible for OT to adapt cyber security best practices appropriate for the ICS environment. We also work with IT security leaders to equip them with the domain knowledge and credibility required to engage their OT teams in practical cybersecurity discussions.

The ideal ICS assessment will include a combination of ICS staff interviews with a functional network assessment using virtual sensors deployed within the client network. Additionally, OT protocol coverage combined with Passive, Active, and AppDB scanning capabilities will deliver complete OT visibility and asset management controls.

The approach should include the following services as a minimum:

- OT asset and protocol visibility and assessment
- Review of the existing architecture diagrams, dataflow, and designs
- Network segmentation and visibility review
- Process visibility and assessment
- Security device configuration review
- Threat detection by tapping into the production ICS network
- Vulnerability assessment
- Review any existing security standards for hardware and software deployment

Modeling and visual identification of credible ICS attacks using multiple threat detection techniques will assist in prioritizing ICS control investments. This typically includes anomaly detection, operational and security behavior monitoring, and known threat assessment.

Vulnerabilities can be identified using non-intrusive methods of comparing each OT asset against a database of insecure protocols, configurations, and other known vulnerabilities. In addition, attack vector mapping and risk-based prioritization techniques should allow vulnerabilities to be prioritized for remediation.

ICS THREAT VECTORS

ICS are commonly found in critical infrastructure and other high-value targets. This makes them attractive targets for hostile nation-states and threat actors aiming to disrupt production operations and processes for industrial sabotage, extortion, or theft of intellectual property. This places ICS firmly in the sights of advanced persistent threats and well-resourced sophisticated criminal enterprises.

Recent years have seen a significant move for ICS away from isolated proprietary solutions toward connected platforms based on open architectures and standard technologies. This has led to a dramatic increase in their attack surface and the range of credible threats. Connection to the Internet, directly or through intranet or business IT systems, has enabled attackers anywhere in the world to launch attacks on ICS targets.

Analysis of successful attacks against ICS systems identifies that the most common root cause is unpatched vulnerabilities in software, primarily due to the constraint that any update rollout must not impact business-critical ICS operations.

Our research shows that the number of ICS vulnerabilities disclosed in 2020 increased by nearly 25% compared to 2019 and almost 33% compared to 2018. This increase is primarily due to increased security awareness, improving the identification of ICS vulnerabilities.

Other key points from our research were:

- Around 76% of disclosed ICS vulnerabilities did not require authentication for exploitation.
- Around 72% of disclosed ICS vulnerabilities were remotely exploitable.
- Around 47% of disclosed ICS vulnerabilities affected Levels 1 and 2 of the Purdue Model.

Our research found that critical manufacturing, energy, water and wastewater, and commercial facilities were the sectors reporting the most ICS vulnerabilities:

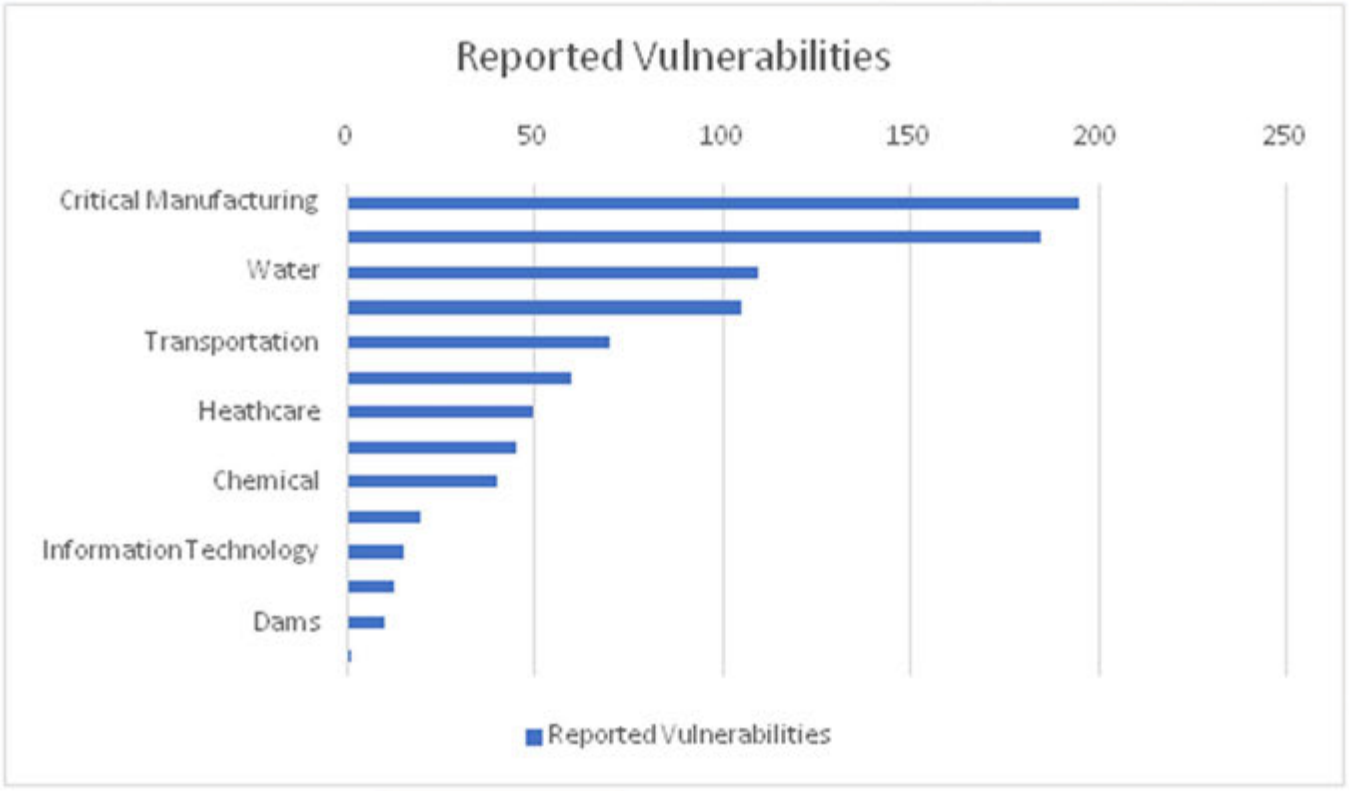

Figure 4 - ICS Vulnerabilities by Sector

ICS THREAT ACTORS

ICS Threats come from numerous sources, which can be classified as hostile, accidental, structural, and environmental. The following table provides examples of known threat actors for ICS.

THREAT SOURCE	DESCRIPTION
Hostile Threats • Ad hoc or established groups • Competitors • Criminal Organizations • Customers • Individual Hackers • Insiders • Nation-States • Suppliers • Trusted or Privileged Insiders	These are individuals, groups, organizations, or nation-states seeking to exploit ICS's weaknesses and vulnerabilities. Motivations include sabotage, theft of sensitive information, extortion, and revenge.
Accidental Threats • Trusted or Privileged Users • Users	These are unintentional erroneous actions by individuals undertaking their regular duties.
Structural Threats • Communications Devices • Control Devices • Environmental Control Equipment • IT Equipment • Networks • Operating Systems • Power Supplies • Processing Devices • Sensing Devices • Software Applications • Storage Devices • User Interfaces	Failure of equipment, software, or utilities due to aging, wear and tear, inherent faults or use outside their defined operating envelope.
Environmental Threats • Earthquake • Explosion • Fire • Flood • Contamination • Storm/Hurricane/Typhoon • Terrorism • Utility Supply Failure	These are natural and manufactured disasters affecting the ICS operating environment, including failures of external infrastructure on which the ICS depends.

Table 1 - Threat Sources

State-sponsored hackers are the primary threat observed attacking organizations in the energy and utility sectors, particularly oil and gas production and distribution, water facilities, and electrical generation and distribution.

The Xenotime group has been active since 2014 and is linked to attacks on oil and gas companies. For example, it is believed that Xenotime was responsible for the Trisis/Triton malware and was involved in the attack on the safety instrumented system at a Saudi Arabian petrochemical plant. You can find more details of this attack in the case studies. Xenotime has been particularly active, expanding activities in 2019 to the US, Australia, and Europe.

The Magnalium and Chrysene groups have been active since 2017 and are linked to attacks on oil and gas companies. The Allanite group has been active since 2017, linked to attacks on electric utility companies in the US and the UK.

Around 2017 the North Korea-linked Covellite group emerged though it focuses on information gathering rather than disruptive attacks. Specifically, it has been seen targeting networks associated with the electric generation and distribution facilities across the US, Europe, and East Asia.

The Hexane group has been active since 2018 and is linked to geopolitical tensions in the Middle East. Its typical attack vector starts with third-party companies such as telecommunication providers as the starting point for a supply chain attack.

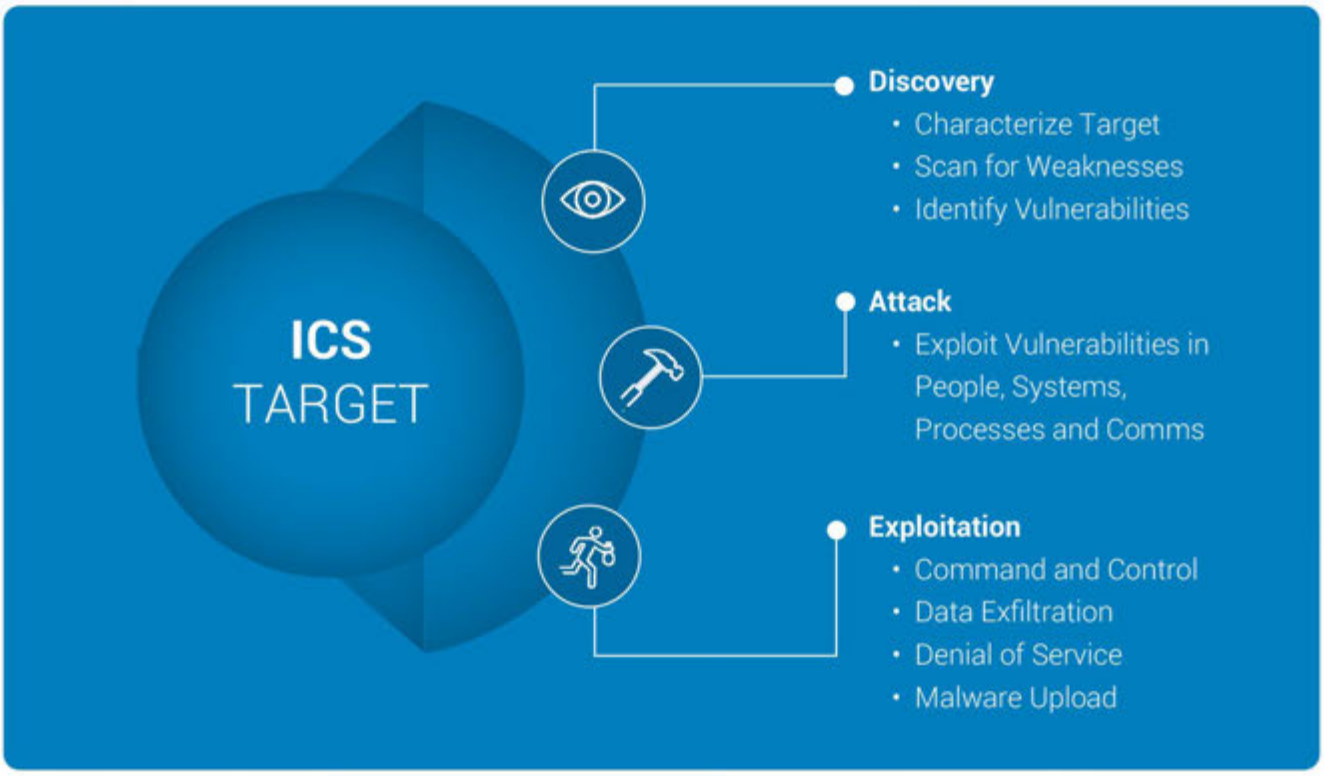

Figure 5 - Threat Actor Attack Phases

ICS SECURITY CONTROLS

The National Institute of Standards and Technology (NIST) provides guidance for recommended security controls. These controls are organized into 18 security-related categories:

- **Access Controls** manage the process of granting or denying specific requests for obtaining and using information, services, or physical access to areas within the ICS environment. Role-based access controls are particularly applicable for managing access in an ICS environment when supported with robust authorization mechanisms to manage the process.

- **Awareness and Training** policies and procedures ensure ICS users are given the required security training appropriate to their role. This security awareness and training should include ICS-specific information for ICS equipment and applications.

- **Audit and Account** ability processes manage the independent review and examination of records and activities to monitor the adequacy of system controls and establish compliance with applicable policies, procedures, regulations, and legislation. Processes should include identifying deficiencies and areas for improvement with tracking and reporting corrective actions with documented change impact analysis and authorization records.

- **Security Assessment and Authorization** processes provide assurance that security controls are implemented correctly, operating as intended, and producing the desired outcome. Ideally, evidence will be through formal certification of controls to a recognized standard to demonstrate control acceptability.

- **Configuration Management** policies and procedures control all modifications to hardware, firmware, software, and documentation to protect against improper or accidental modifications. In addition, a formal change management program integrated into risk management processes will minimize the risk of any changes causing undesirable effects or unintended consequences.

- **Contingency Planning** policies and procedures ensure business operations are maintained to an adequate level during system failures, emergencies, or disasters, and normal operations can be restored within required timeframes. Plans should be subject to periodic review and testing to ensure effectiveness.

- **Identification and Authentication** processes verify the identity of users, services, or devices using credentials such as passwords, tokens, and biometrics as a prerequisite for granting access to ICS resources. In addition, processes should ensure that default or hardcoded credentials are removed from ICS components before incorporation into an operational environment.

- **Incident Response** policies and procedures manage incident response training, testing, handling, monitoring, reporting, and support services. Incident response procedures should document the predetermined instructions for detecting and responding to any intentional or unintentional incident necessary to limit consequences to the ICS services. ICS incident detection is typically characterized by symptom identification, including unusual resource usages such as network bandwidth, data storage, and processor usage. Other symptoms include abnormal user behavior, abnormal failed access attempts, log file tampering, or unplanned software changes.

- **Maintenance** policies and procedures manage all maintenance and diagnostic processes, including access controls for tools and the authorization and management of remote connections.

- **Media Protection** policies and procedures ensure secure media handling, including access, usage, labeling, transportation, storage, sanitization, and disposal. In addition, protections should logically or physically prevent removable media from being connected to ICS equipment unless explicitly authorized.

- **Physical and Environmental Protection** policies and procedures manage access control to locations, facilities, and equipment. Also, environmental controls for conditioning (e.g., temperature, humidity) and emergency provisions (e.g., shutdown, power, lighting, fire protection) should be protected.

- **Planning** policies and procedures manage the development and maintenance of ICS security planning through assessments, specifying and implementing security controls, assigning security levels, and responding to incidents.

- **Personnel Security** policies and procedures manage recruitment, screening, transfer, termination, and disciplinary processes for all staff, including third-party personnel.

- **Risk Assessment** policies and procedures manage the process of identifying and managing risks to operations, assets, and individuals. Assets include process and control information within the ICS and flowing outside the ICS to corporate networks and third-party connections.

- **System and Services Acquisition** policies and procedures manage the allocation of resources for ICS security throughout the operational life cycle based on risk assessment results. Where ICS elements are outsourced, this includes contractual management of organizational security.

- **System and Communications Protection controls** protect ICS network data transmission components. However, it's essential to recognize that encryption techniques may introduce communications latency within the ICS environment from the message encrypt, decrypt, and authenticate process and create key management issues.

- **System and Information Integrity** policies and procedures maintain the system and information integrity to ensure that sensitive data cannot be modified or deleted in an unauthorized and undetected manner. Typical ICS controls include malware and intrusion detection solutions.

- **Program Management** policies and procedures manage the organizational level security program, including ICS security planning.

RISK ANALYSIS
AND PREVENTION

OVERVIEW

Risk analysis should systematically analyze and evaluate functional and security-specific ICS resources to identify and prioritize credible threats and mitigate these using technical and organizational countermeasures.

However, the fundamental differences between traditional IT systems and ICS solutions mean that general IT security standards, risk analysis, and prevention guidelines do not produce adequate results. A risk-based assessment methodology that draws on industrial cybersecurity best practices and most used standards is necessary to address specific ICS requirements. However, there is a constraint that such a methodology needs integration with risk assessments for IT systems connected to the ICS.

One of the most significant security issues facing ICS operators is that security risk management requires specific processes tailored to operations and reliability in common with other areas of industrial risk management. Unfortunately, most organizations lack the expertise to address industrial security risk management.

ICS RISK MANAGEMENT

It is important to recognize that ICS security risk management is one component of an organization's overall corporate governance. As shown below, security risks are part of the governance picture and cannot be treated in isolation from other risks.

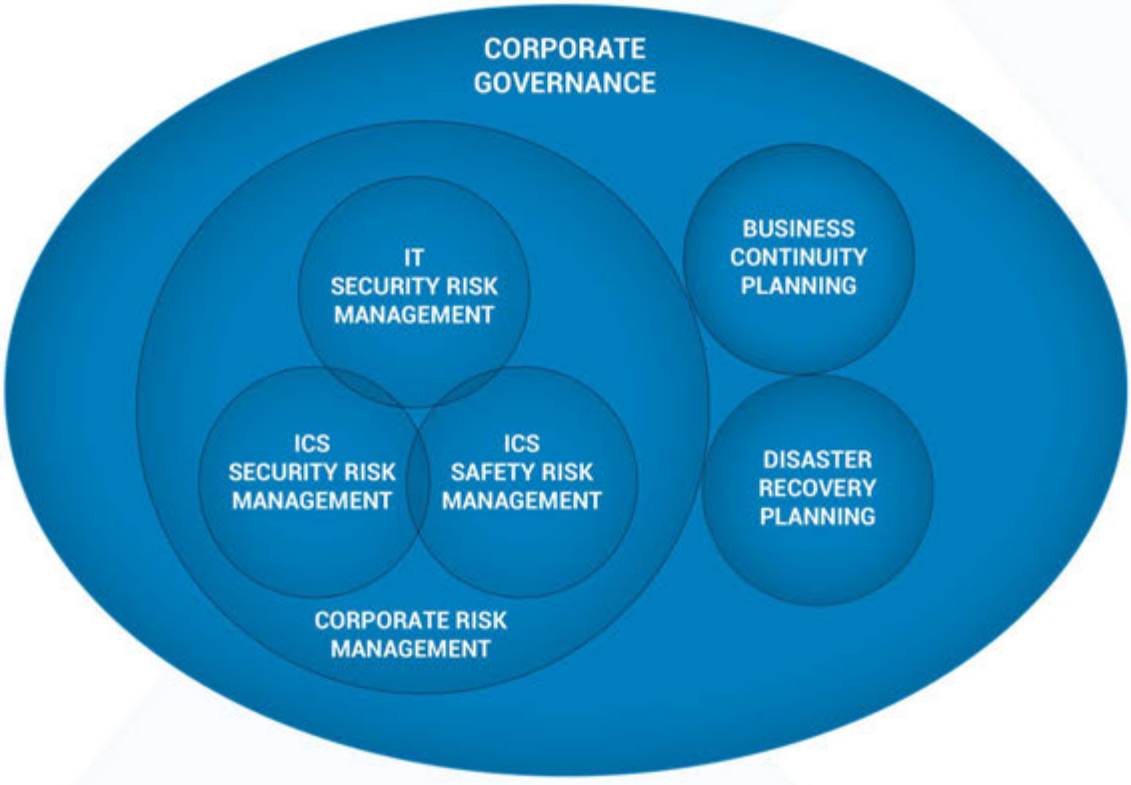

Figure 6 - Corporate Governance Activities

ICS RISK ASSESSMENT PREPARATION

SYSTEM DEFINITION

The first step of any assessment process is to define the scope of the assessment and its required goals. For example, the ICS risk assessment scope can look at the ICS as an integrated component of the organizational business systems or be treated in isolation with the assessment confined to within the ICS network boundaries.

Where ICS architectures include both critical and non-critical systems, the scope of the risk assessment may be limited to those critical elements where there is adequate segregation between parts.

SYSTEM DECOMPOSITION

Typical ICS have complex architectures and large numbers of diverse types of connected devices. The risk assessment process can be facilitated through the logical and physical decomposition of the overall ICS architecture into manageable elements. The assessment will address the functionality of each component and the interfaces between elements.

NETWORK SEGREGATION

Where the ICS includes connections to other networks, the risk assessment process must consider the security of network segregation and the risks associated with threats traversing boundaries.

Where connected networks have risk assessments available, the results of these assessments should be integrated into the ICS risk assessment to demonstrate the mitigation of known risks.

Segregation requires developing and enforcing rulesets that define which communications are permitted to transverse a boundary. The rules are typically defined using source and destination identity and message content. Various methods and technologies are available, including:

- Physical network separation, known as air-gapping
- Logical network separation is enforced using encryption or network device-enforced partitioning, including Virtual Private Networks (VPN), Virtual Local Area Networks (VLANS), or unidirectional gateways such as data diodes
- Network traffic management is enforced using techniques such as IP filtering, state-based filtering, port filtering, protocol filtering or application-level firewalls, proxies, and content-based filtering

INFORMATION GATHERING

An ICS risk assessment cannot be complete with unrestricted access to all necessary information.

This includes:

- A comprehensive inventory list of all ICS assets, including detailed hardware, firmware, and software information
- An asset list that records criticality, asset owner, management responsibilities, and organizational value

- A business impact analysis or hazard analysis for each ICS asset
- Vulnerability information for each ICS asset
- Up-to-date threat information relevant to the ICS
- ICS network diagrams that identify all interfaces and the criticality of components and information flows
- A risk register listing all known risks, current risk treatments, the residual risk levels, and a record of decisions and justifications for risk acceptance
- A list of all stakeholders identifying their responsibilities and accountability for ICS security

ICS RISK ASSESSMENT PROCESS

Security risks must be balanced against threats to reliability, efficiency, and safety when identifying and managing risks. This places constraints on the security risk assessment process to ensure no adverse impacts can compromise critical ICS functionality. This is especially critical where ICS availability precludes security controls that disable functionality in the event of threat detection.

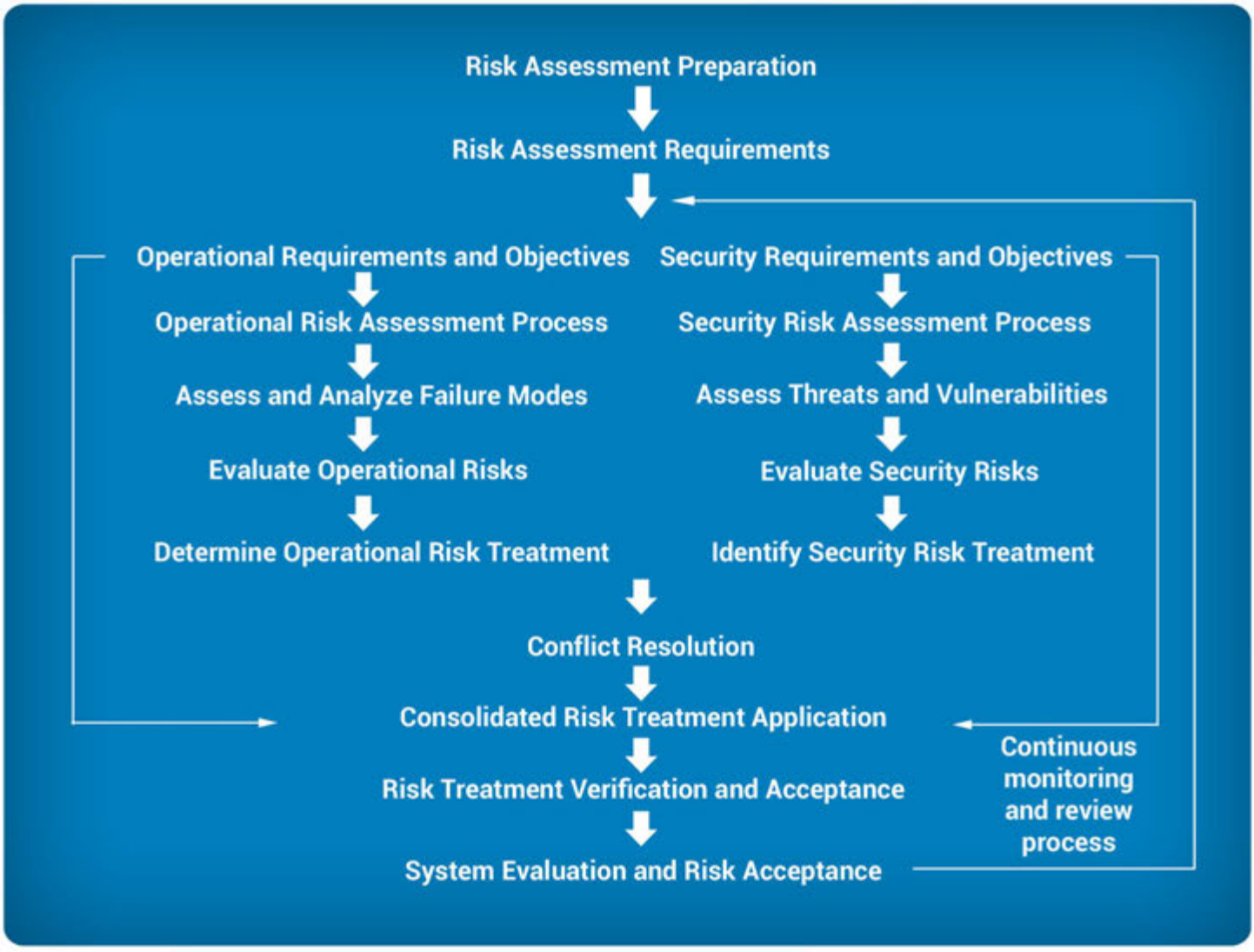

Figure 7 - ICS Risk Assessment Process

The risk assessment process needs to consider and combine the results of operation risk and security risk assessment processes with risk treatments driven by the operational and security requirements. First, appropriate ICS stakeholders analyze and evaluate operational and security risks separately. Then, analysis of the frequency and severity of risks can be used to identify which risks require further management and which are within acceptable limits determined by the organization's risk appetite.

Component failure modes are typically used to identify operational risks, while information security risks are assessed by analyzing threats and vulnerabilities. Cost-benefit analysis can be used to determine if risk treatment is economically viable within the constraints of the operational and security requirements.

SECURITY RISK ASSESSMENT PROCESS

The security risk assessment process starts with the identification of credible threats. These can include the following, though the actual list will depend on a broad range of factors, including the nature of the ICS, its purpose, its geographic location, and the value of inherent information:

- Accidental or unintentional user actions
- Denial of service attacks
- Direct external hacking attacks
- Environmental damage, including fire and flooding
- Insider attacks
- Malware, including ransomware, viruses, and worms
- Password cracking attacks
- Physical attacks, including theft and vandalism
- Social engineering attacks
- Technical failure
- Theft of physical access controls, including tokens and badges
- Third-party connectivity external hacking attacks

Threats will materialize into security risks through the presence of vulnerabilities and weaknesses in the ICS. As an example, these can include:

- Default accounts and passwords
- Inadequate access controls
- Inadequate security awareness or training
- Insecure network connections
- Poor configuration management
- Poor logical security
- Poor malware protection
- Poor network segregation
- Poor physical security
- Security policy and procedural deficiencies
- Unpatched firmware/software
- Unpatched hardware
- Unsupported firmware/software
- Unsupported hardware
- Weak authentication controls
- Weak encryption
- Weak network protocol security

Risks can be managed through several options, risks can be reduced through the application of controls, or risks can be transferred onto another party, such as taking out an insurance policy, or risks can be accepted.

The organization may choose to accept without treatment those risks assessed as being within the risk appetite of the organization. Where controls are required to reduce risks to an acceptable level, diverse options are available:

- Preventative controls will reduce the frequency or impact of a risk to lower the risk level by preventing the exploitation of a vulnerability
- Deterrent controls lessen the frequency of attacks on a vulnerability by discouraging threat actors where a known vulnerability cannot be removed
- Compensating controls provide additional strength in depth protection where an existing security control has itself an inherent vulnerability that cannot be resolved
- Corrective controls lessen the impact of attacks by improving post-incident recovery capabilities
- Detective controls provide alerting of attacks for use in conjunction with response and recovery capabilities

RISK **PREVENTION**

Treatments to deal with operational and security risks must be integrated to ensure that any proposed treatment satisfies all requirements. Any conflicts, such as a security risk treatment such as isolating network connectivity that adversely impacts an operational requirement such as system availability, must be reviewed and resolved to ensure all requirements are satisfied.

Conflict resolution will often require prioritization of requirements to determine the most pragmatic solution. Usually, ICS operational requirements will have higher priority than security requirements. If security risk treatment negatively impacts the availability, the operational risk treatment will be selected when conflict occurs.

Comprehensive risk assessment activities will generate multiple treatments to manage the identified risks. These treatments should be prioritized based on the risk level derived from the likelihood and severity of each risk. The following risk matrix provides an indicative example of a risk classification technique.

Severity /Likelihood	Negligible	Minor	Moderate	Severe	Catastrophic
Highly Likely	Medium	Medium	High	Very High	Very High
Likely	Low	Medium	Medium	High	Very High
Possible	Low	Medium	Medium	Medium	High
Unlikely	Very Low	Low	Low	Medium	Medium
Highly Unlikely	Very Low	Very Low	Low	Low	Medium

Table 2 - Risk Matrix

Categorizing severity is typically based on assessing the impact on the range of possible affected items.

The following table provides examples of typical categorization:

AFFECTED ITEMS / SEVERITY	PRODUCTION	PERSONNEL	INFRASTRUCTURE	NETWORK	INFORMATION ASSETS
NEGLIGIBLE	Loss of production less than one hour	No injuries	No damage to facilities or equipment	No network loss	No information loss
MINOR	Loss of production for less than one day	Minor injury	Minor damage to facilities or equipment	Minor impact on network CIA	Minimal loss or disclosure of information
MODERATE	Loss of production for less than one week	Multiple minor injuries	Moderate damage to facilities or equipment	Moderate impact on network CIA	Significant loss or disclosure of information
SEVERE	Loss of production for less than one month	One or more significant Injuries	Severe damage to facilities or equipment	Severe impact on network CIA	Recoverable loss of sensitive information
CATASTROPHIC	Permanent loss of production	Loss of Life	Destruction of facilities or equipment	Unrecoverable loss of network CIA	Unrecoverable loss of sensitive information

Table 3 - Risk Severity Categories

The categorization of likelihood typically is based on assessing the frequency that risk may materialize based on quantitative calculations of rates or qualitative assessments where data is unavailable.

The following table provides examples of typical categorization:

Likelihood	Quantitative Rates	Qualitative Guide
Highly Likely	Once each operating hour	At least once per day
Likely	Less than 1 in 100 operating hours	Less than once per week
Possible	Less than 1 in 1,000 operating hours	Less than once per month
Unlikely	Less than 1 in 100,000 operating hours	Less than once per year
Highly Unlikely	Less than 1 in 1,000,000 operating hours	Less than once per decade

Table 4 - Risk Likelihood Categories

Categorizing risk treatments based on risk level will depend on the organizational risk appetite and the prioritization of resourcing for corrective actions at the corporate level.

The following table provides examples of typical categorization:

Risk Level	Risk Treatment Prioritization
Very High	Risk requires immediate attention to resolve,including continuous monitoring and reporting of treatment status until the risk is reduced to an acceptable level.
High	Risk must be managed as a matter of urgency subject to resource constraints, including regular monitoringand reporting of treatment status until the risk is reduced to an acceptable level.
Medium	Risk should be reduced to an acceptable level unless a cost-benefit analysis justifies risk acceptance. The decision-making process must be formally documented and periodically reviewed to ensure the argument for the risk acceptance remains valid.
Low	Risk within corporate risk appetite requiring no treatmentbut must be periodically monitored to ensure no increase in risk level
Very Low	Risk does not require treatment but should be periodically monitored to ensure no change to the risk level

Table 5 - Risk Treatment Priorities

Risk treatment verification is necessary to ensure that security controls do not adversely impact operational performance before implementation into a production environment. Security risk treatments must be first implemented in simulation or test environments where operators can observe and verify the influence of the treatment on the ICS.

A system evaluation exercise will then ensure that the implemented operational and security risk treatments correctly manage identified risks and that no additional risk treatment is required to manage residual risks.

SECURITY IMPLEMENTATION

OVERVIEW

The implementation of ICS Security should follow a process of fully understanding the problem, acting on the results, and monitoring the solution.

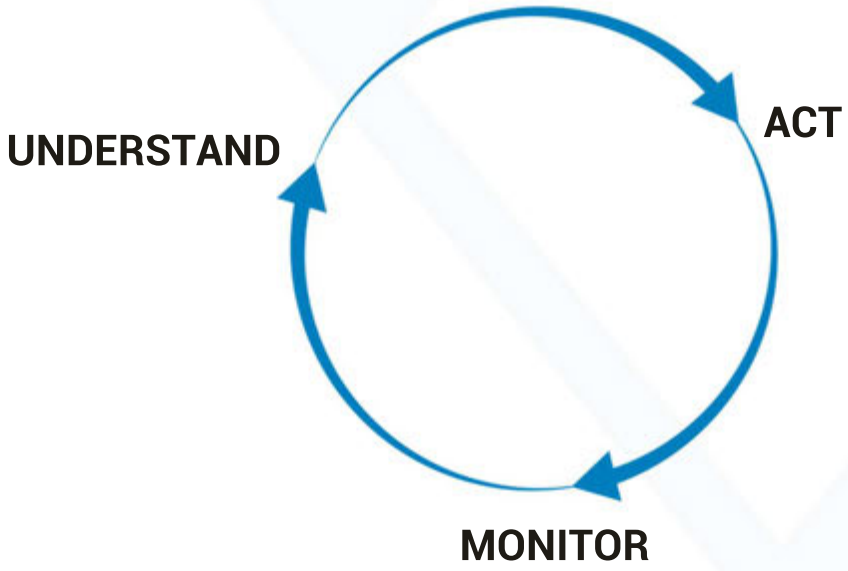

Figure 8 - ICS Security Cycle

ICS security understanding comes from gathering knowledge about the ICS operating environment and the credible threats it currently faces and can be expected to face in the future. Novel and emerging threats, plus discovering, and disclosing new vulnerabilities, pose the most significant challenge for ICS security defenses.

Therefore, ICS security understanding can include the following activities:

- Risk assessment, including periodic reviews, network vulnerability assessments, testing, and post-incident analysis
- Policy management, including the definition of roles, responsibilities, and authorizations
- Threat intelligence assessments to gain insights into emerging threats

ICS security action represents the deployment of security controls to mitigate the risks from identified threats to an acceptable level.

Security controls cover tools and techniques to detect threats and recover from attacks, including the following types of controls:

- Boundary protection solutions, including firewalls, malware scanning, content filtering, and intrusion prevention and detection services
- Network security monitoring solutions for intrusion detection including network forensic (packet capture) and NDR solutions

- End-point security solutions, including behavioral analysis and malware scanning
- Deception solutions as a post breach strategy and for the detection of lateral movement

ICS security monitoring covers the management of security controls to ensure they remain effective in the event of changes to the ICS environment, the threat landscape, business operations, and corporate risk appetite.

ICS security monitoring can include the following activities:

- Policy compliance, including compliance assessment and corporate governance
- Patch management for vulnerability removal cognizant of operational availability constraints
- Backup and disaster recovery processes for business continuity and incident recovery
- Managed detection and response services for round-the-clock real-time monitoring, alert management, investigation, containment and recovery practices

DETECTION

The Detection step is your backup plan. Detection entails monitoring of your ICS internal network and endpoints, detecting malware and attackers that bypass your ICS perimeter controls or hiding in your network. This step includes the use of advanced techniques such as Threat Intelligence, Adaptive Response, Analytic Monitoring, and Deceptions. Any Detection strategy for ICS networks needs to take into consideration all threat vectors that could possibly target an ICS network. This includes network and host based threats as well as encrypted attacks, lateral movement, and post breach strategies.

For threats targeting the ICS hosts, the LMNTRIX XDR ENDPOINT SECURITY lightweight endpoint sensors provide rapid deployment of detection capabilities that minimize the impact on ICS operations. Endpoint monitoring captures detailed state information and prevents exploits, malware, file-less attacks, malware-less attacks, phishing, injection, macro-based attacks, ransomware, credential theft, and adversary tradecraft prevention.

Effective threat detection must also be capable of detecting known and unknown threats that bypass traditional perimeter controls across the entire ICS network. The LMNTRIX XDR NDR network sensors are deployed out of band using SPAN/TAP and deliver integrated, multi-layer detect-in-depth capability. These can be deployed as virtual sensors or physical appliances at network choke points and high-value assets/servers. This flexibility offers a scalable solution able to support ICS networks of any size and complexity.

Any ICS threat detection strategy must also incorporate a post breach strategy that is capable of detecting lateral movement. The LMNTRIX XDR DECEPTIONS obscures your ICS assets, every endpoint, server and network, in a deceptive environment. This environment immobilizes attackers, who unable to determine real from fake and make reliable decisions are drawn to interact with the dummy digital assets.

Using intercepted communications between Threat Actors to identify TTP's before they're used in anger and identify when threat actors test POC code on smaller more obscure targets before attempting it on higher value larger targets, allowing us to at times be ahead of the threat. The proprietary technology behind LMNTRIX XDR INTELLIGENCE allows us to deliver earlier detection and identification of adversaries in your organization's network. This is achieved by making it possible to correlate over 800 million threat indicators against real-time network data deployed deep within customer ICS networks.

ICS networks need to also consider the use of network forensics as a post breach forensic capability to give ICS networks a 'photographic memory' with full fidelity packet capture, optimized and stored for up to a year, you will know with absolute certainty if events have impacted your environment. The LMNTRIX XDR Network Forensics sensor uses network packet capture technology to deliver extensive visibility, high performance threat hunting and unrivalled incident response by augmenting our CDC with User and Entity Behavior Analytics (UEBA) technology.

RESPONSE

Most enterprises have no response plan at all. For example, after Yahoo was breached in 2014, the attackers sifted through the company network, downloaded proprietary software and massive databases, and gained the ability to access a billion user accounts. Two years later, when Yahoo made this information public, they basically shrugged their shoulders and said, "It happens, what can you do?"

Well, here's what you can do: Use an MDR to implement advanced Response and Recovery capabilities. An effective response plan should contain and mitigate an attacker in your network, patch the discovered security hole, prevent the spread of malware, and recover stolen data. You should quickly and efficiently remove the threat from your network (which you will be able to do, because you've also implemented Detection), figure out exactly what the attacker did while connected to your network, and quickly notify affected parties so they can ensure their privacy and security if necessary (change passwords, alert banks, etc.).

With this approach, you keep hackers away from your secure, sensitive information and rapidly reclaim your fortress.

Advanced MDR vendors offer so much more than is possible for any SOC, MSSP, SIEM or perimeter control. As the security game advances, prevention-based security is hopelessly insufficient and outclassed. We know attackers have become more advanced, and we know that even the most expensive legacy security controls have consistently failed to protect organizations. MDR vendors are making the push into next-generation security, bypassing multi-million-dollar SOCs and SIEMs in effectiveness and countering even the most advanced threats.

The LMNTRIX Active Defense MDR service combines information from the endpoint and network detection services. The Cyber Defense Center monitors activity, conducts adversary hunting and baiting, validates breaches, and investigates, contains, and remediate threats. Additionally, intrusion analysts delve deep into endpoints operation to expose anomalous behaviors.

LMNTRIX employs various techniques, including live memory analysis, direct physical disk inspection, network traffic analysis, and endpoint state assessment. Instead of relying on signatures or rules that advanced persistent threats can circumvent, the service leverages unique endpoint behavioral monitoring and advanced machine learning. This enables better analysis and identification of zero-day exploits and hidden threats missed by other endpoint security solutions.

When an attack is detected, intrusion analysts can instantly find similarly infected endpoints and quickly expand their visibility into the full scope of a compromise. Once an intrusion is confirmed, LMNTRIX XDR disrupts malware-driven tactics, techniques, and procedures (TTP) and limits attacker lateral movement by quarantining and blocking the threat on the host as well as on all ICS perimeter controls.

SECURITY BEST PRACTICES

Compared to business IT systems, ICS have different performance and reliability requirements. In addition, they often use diverse operating systems and bespoke applications that are unconventional to systems managed by a typical IT support team.

Furthermore, the goals of reliability, efficiency, and safety can sometimes conflict with security in the design and operation of ICS that focus on reliability and availability. Therefore, security controls must not compromise critical ICS functionality.

The differences between ICS and IT systems create the need for increased sophistication in applying cyber security controls and operational strategies. In addition, successful implementation requires a complete understanding of the reliability impact of the installation, operation, and maintenance of security solutions in conjunction with ICS operation.

The following best practices address common deficiencies observed in ICS environments.

SECURITY ORGANIZATION

Details of organization structure and resourcing necessary to manage ICS security, including:

- Definition of security roles with responsibility and accountability for the security of ICS
- Corporate management role
- Governance for security functions
- Adequate budgeting
- Change management and configuration control
- Staff awareness and business culture

An ICS cybersecurity program should be built on a compelling business case for the organization's unique needs. The business case should capture the business concerns of senior management and provide the business impact and financial justification for creating an integrated security program.

The organizational security plan should define the policy and procedures required to implement security controls, consistent with applicable laws, directives, legislation, regulations, standards, and guidance.

The security plan must contain sufficient information to enable an unambiguously compliant implementation with the plan's intent and a subsequent determination of risk to organizational operations, assets, individuals, and other affected parties.

DOCUMENTATION SET

List of minimum documentation set required to support the safety organization, including:

- Security policies, processes, and procedures
- Risk and vulnerability analysis
- Physical and logical network diagrams
- Network management
- Network and device configuration records
- Access management records

SYSTEM DESIGN

The ICS network security perimeter should be logically separated from any corporate network on physically separated network devices with documented access points, defined security perimeters, and the necessary network security controls to prevent intrusions. Network segmentation aims to create security zones that provide access control by separating systems with different security and access requirements.

Good cyber security practices for ICS network design include the designation of demilitarized zones and the use of security controls such as firewalls and intrusion detection capabilities throughout the ICS architecture.

ICS design should support the concept of least privilege for all services to minimize unauthorized access to system resources and the window of exposure and impact criticality in the event of disclosed service vulnerabilities.

ICS solutions should include physical access controls to prevent unauthorized physical access to equipment, including cabling and utility supplies, where interference can disrupt ICS operations. Typical controls include location in secure areas, access barriers, guards, and locks.

ICS solutions should include robust logical access controls with comprehensive authentication processes at both ends of any communications channel with encryption and strong authentication for communication protocols as necessary to protect data in transit.

Port security should be implemented to limit connectivity to ICS hardware interfaces. The static nature of ICS environments allows port security to be used to ensure new devices cannot be introduced to a network without security approval.

ICS design should support patching and updating processes to resolve disclosed vulnerabilities promptly with no system disruption or performance degradation.

ICS design should allow the creation of different accounts for functions that require additional privileges and support the concept of least privilege for users with defaults configured to the minimum rights necessary for each account type.

ICS design should include consideration of redundancy or graceful degradation modes for critical operations along with fail-safe mechanisms to ensure no single failure of a vital component or process can lead to total loss of ICS operations.

CODE HYGIENE

Applications should be developed using robust coding practices and follow available guidelines for secure web development, such as the Open Web Application Security Project.

Application coding should include validation of all input data and resistance to buffer overflow attacks using a philosophy of accepting only known good values. Data checks should include ICS protocol traffic that can be intercepted and modified in transit using data bounds and integrity-checking techniques. In addition, all pointers that can be changed should be checked before use to prevent NULL pointer dereferences.

Development processes should prevent the use of hard-coded passwords or any other practices that do not support secure authentication. Instead, techniques should encourage using cryptography or other secure methods to protect credentials from unauthorized interception or retrieval.

All custom-developed applications should undergo a thorough code review using manual and automated techniques to identify and resolve security weaknesses and vulnerabilities as an integrated part of the development process.

Applications should be developed using the least privilege principle with segregation between normal, privileged, and administrative functions. Authentication must be applied across all communication channels using robust processes with client-side checks duplicated on the server side. Where sessions or user states persist across multiple connections or channels, authentication and appropriate credential management must be used throughout.

ICS web applications should only use reputable and fully validated third-party web servers that can securely handle malformed inputs and other vulnerabilities with the potential to compromise the ICS web server.

The design of ICS-specific network protocols should include strong authentication and integrity checks.

All IT products should be subjected to rigorous security review before deployment on an ICS network, ideally during procurement. In addition, where applications are downloaded, cryptographic signatures should be used to validate the authenticity and integrity of the downloaded code.

CONTINGENCY PLANNING

Business continuity and disaster recovery planning requires for disruption management and restart processes with structured re-commissioning of ICS systems. Techniques for secure and uninterrupted operation during maintenance, upgrade and servicing actions, and threat scenarios must be adhered on a regular cycle.

The frequency of system backups and the transfer rate of backup information to alternate storage sites must be consistent with the organization's recovery time and recovery point objectives. In addition, the business continuity and disaster recovery processes should ensure system backup information's integrity, availability, and confidentiality.

DEFENSE IN DEPTH

No single cyber security countermeasure provides absolute protection, particularly against novel threats and vulnerabilities, including zero-day exploits. Reducing risks requires implementing multiple organizational, protective, and detection and response countermeasures to eliminate, where possible, any single points of failure.

- Organizational Countermeasures include Governance, Risk Management, Asset Management, Supply Chain Management, Policy and Procedures, Competence, and Awareness.
- Protective Countermeasures include Identity and Access Control, Data Security, System Security, and Resilience.
- Detection and Response Countermeasures include Security monitoring and incident response.

COMPLIANCE WITH RECOGNIZED STANDARDS

Compliance with recognized standards, particularly certification by an independent accreditation body, provides assurance that security best practices are not only applied but are maintained. This continuous review is necessary to counter evolving and novel threats and frequently discover new vulnerabilities in applications, components, and technologies.

Common international standards and guidelines that apply to ICS include:

- IEC 62443 Security for industrial automation and control systems
- ISO/IEC 27000
- ISA-TR84.00.09-2013- Security Countermeasures Related to Safety Instrumented Systems
- ISA-TR99.00.01-2007, Security technologies for industrial automation and control systems
- IT baseline protection based on ISO 27001
- VDI/VDE 2182 IT-security for industrial automation
- National Institute of Standards and Technology (NIST) Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security

ICS THREAT DETECTION AND RESPONSE

There is a wide range of threat detection and response solutions available; however, not all are fully compatible with the unique requirements of ICS architectures and components.

The LMNTRIX Active Defense MDR and XDR solutions use architecture and tech stacks that support ICS using customized solutions tailored to specific requirements. This includes network sensors, packet captures, endpoint agents and deception solutions specifically designed for operational technology. This includes threat detection and network forensics sensors that use protocol decoders designed for ICS protocols.

This compatibility results in the LMNTRIX architecture and technology stack providing complete support for ICS/SCADA environments. The following image demonstrates how LMNTRIX's solution dovetails into the standard PERA structural model for ICS.

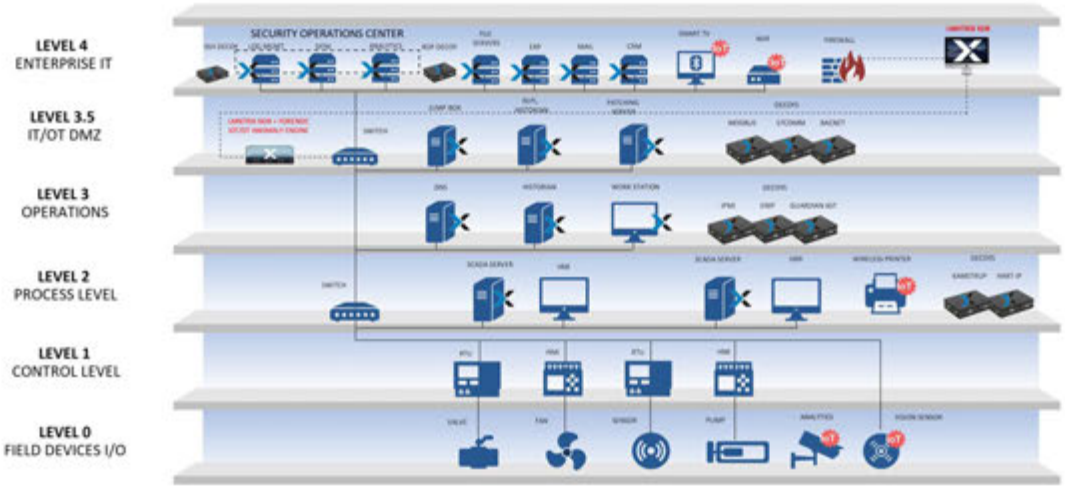

Figure 9 - LMNTRIX and the PERA structural model

The LMNTRIX multi-vector and holistic architecture detects any threat to the SCADA application, process, or network, providing granular visibility of SCADA traffic and facilitating attack forensics:

- We monitor and record all SCADA activity out-of-band and independent of the ability of SCADA devices to send logs
- We baseline normal behavior and alert on deviations from the baseline to prevent undesired network operations based on policy
- With our integrated network and endpoint threat forensics, together with deceptions everywhere, we reveal the entire sequence of an attack event
- All security and events related to our architecture are centrally managed, providing a complete view across your enterprise and control networks
- We support the industry's most extensive support of ICS/SCADA-specific protocols, including BACNet, DNP3, IEC-60870-5-104, IEC 60870-6 (ICCP), IEC 61850, MMS, Modbus, OPC, Profinet, S7 (Siemens) and many others
- We detect and prevent exploits of ICS vulnerabilities with SCADA IDS signatures and on the endpoint using exploit prevention using hardware-assisted control flow integrity (HA-CFI), closing the window of exposure between vulnerable and patched systems.
- We detect lateral movement using SCADA-specific deceptions
- We recommend our software component (agent) be installed on all Corporate endpoints in Prevention Mode. Software component (agent) installed on all PCN endpoints (Control/HMI Servers) in Detection Mode only – Not prevention.
- It can be installed on any permitted device that supports Windows, Linux, Mac, and Solaris. Recommended but not required on Control Servers and HMIs. It is not recommended on any other PCS components.
- Our network sensors can utilize a full range of threat detection capabilities, including deceptions, IDS, anti-malware, and sandboxing to detect inbound threats to SCADA networks

The LMNTRIX architecture provides a complete IT-OT security solution that protects the corporate network past the perimeter, the bridge between IT and OT networks, operator workstations, and SCADA devices within the OT network.

FUTURE ICS
SECURITY TRENDS

ICS SECURITY FOCUS

Recent high-profile cyber attacks on industrial control systems, such as the extensive disruption to the operation of the Colonial Pipeline in the US, have resulted in an increased focus on cybersecurity posture.

In the past year, there has been a significant increase in attacks on industrial infrastructure and manufacturing facilities worldwide. As a result, protecting ICS assets from attack is expected to remain an essential focus on ICS development for the foreseeable future, while advanced persistent threats continue to gain demonstrable benefits from successful attacks.

ICS AND IT CONVERGENCE

IT development and deployment processes have seen significant advancements in recent years. Initiatives such as secure by design and secure out of the box are looking to ensure that minimum effort is required by users to implement secure solutions, boosting the overall security of the IT ecosystem. In addition, the promotion of security to be an integral part of agile development through DevSecOps (development, security, operations) processes seek to enhance the security of the deployed solution further.

Now there is a move to incorporate these processes into ICS applications and equipment development as ICS development mirrors IT processes to leverage the competitive and financial benefits these bring. Increasing levels of integration and information exchange between ICS and IT systems support this convergence.

- Cloud-native IT development tools, including API technology, are being adopted for ICS application development processes. This technology, including virtual commissioning techniques, allows developers to assess security robustness as part of the development process, promoting a secure-by-design culture with the development team.

- ICS application development incorporates the use of mainstream programming languages and solutions in place of traditional bespoke development environments. One benefit is this trend will see greater adoption of conventional IT development metric-based quality assessment processes. This also opens ICS application development to a wider pool of experienced resources, improving code quality and boosting maintainability.

- IT and OT companies are collaborating on integrated solutions to boost the productivity of resource-constrained IoT devices. These solutions implement secure connectivity for device management. This trend creates opportunities for hardening IoT devices through connection security controls.

The benefit of better-implemented security controls at the application and equipment level is that fewer resources are required for security management of endpoint breach detection, and effort can be better focused on advanced persistent threat detection at the system level.

ICS AND IT INFORMATION SHARING

Containerization technology pioneered in IT solution development and cloud-based deployment is in use for the collection and processing of machine and manufacturing processing data into cloud-based and on-premise information management solutions. Big data processing solutions allow businesses to leverage inherent information to improve manufacturing processes through optimization and issue detection techniques. In addition, the application of IT data processing solutions creates opportunities for enhanced security control of data flows.

While big data analytical processing and information sharing offer ICS significant benefits, from a security point of view, it creates additional risk. Threat actors can better hide their activities from sight by hiding transactions within the increased network traffic. This requires the application of more capable network traffic analysis and behavioral monitoring techniques to detect malicious activity within information flows.

ICS VIRTUALIZATION

IT virtualization technology offers the capability to create hardware-agnostic programmable logic devices that replace bespoke ICS hardware devices with commoditized server-based solutions to deliver flexibility and scalability to ICS solutions. In addition, this has the security benefit of allowing the deployment of established IT detection and response solutions in place of bespoke endpoint monitoring.

An additional benefit to virtualization is the application of low-code and code-less solutions for ICS applications, reducing security vulnerabilities associated with bespoke device application development and maintenance.

ICS SECURITY ARCHITECTURE

IT architectures are moving to “zero trust” security principles to address increasingly sophisticated and persistent cyber security threats. One of the main drivers is the US Government's Federal Zero Trust Strategy. This approach is expected to also become more common in ICS architecture.

Zero Trust Architecture is a significant philosophical change for managing security controls. It imposes a “Defense-in-Depth” strategy using the principle of least-privilege access. Access rights are granted on proof of legitimate need and are subject to periodic review by automated access management processes for continued need. Trust must be earned before access to an ICS is granted, and there is no assumption of authenticated trust within ICS boundaries. Access attempts are assumed suspect until proven legitimate. The adoption of Zero Trust architectures in ICS will require a corresponding adoption of threat detection and response solutions that can operate effectively within this environment.

EXAMPLES OF SUCCESSFUL ATTACKS

ICS INSIDER ATTACK – THE MAROOCHY SEWAGE SPILL

At the beginning of 2000, nearly one million liters of untreated sewage were released into the rivers and coastal waters of Maroochydore in Queensland, Australia. This unauthorized release resulted from a disgruntled ex-employee performing an insider attack on a SCADA system. Using a stolen wireless radio, SCADA controller, and control software, the attacker accessed the sewerage system, altering data to affect operations across several sewerage pumping stations using his inside knowledge of system behavior.

The affected ICS comprised around 150 pumping stations that transport sewerage to treatment plants. Each pumping station used a Hunter Watertech PDS Compact 500 computer as a remote terminal unit networked to a central control center. The ICS network was used to send control messages to stop and start pumps from the control center to each pumping station and send flow data and alarm signals back from each pumping station to the control center. The ICS network was implemented using a private two-way radio system.

The attack was carried out over several days, with pumps being incorrectly commanded, alarm signals being disabled, and communications with some pumping stations being disabled. These were initially interpreted as system faults before the attack was recognized. However, the presence on the network of a bogus pump station sending messages that were corrupting system operations raised the alarm. The attacker was then observed to gain computer access to the ICS and adversely affected the operations at pumping stations by preventing the central computer, in its role as SCADA master, from exercising proper control.

The attack culminated with a pumping station overflowing, which caused raw sewerage to escape into the local water course. The release polluted over 500 meters of an open drain in a residential area and flowed into a tidal canal. This led to the loss of marine life and distressed affected residents due to its unbearable odor. Cleaning up the released sewage took days and required the deployment of considerable resources.

The attacker, Vitek Boden, launched the attack after being turned down for a full-time job with the local council body responsible for the facility. Hunter Watertech had previously employed Vitek as a site supervisor on the SCADA installation project. This gave him insider knowledge to access the control systems by exploiting weaknesses in access control and authentication processes.

Using a private radio communications system required the attacker to be physically near a network access point which contributed to the swift halt of the attack. Additionally, the attacker was identified as a person of interest to law enforcement officers who spotted his vehicle and discovered the equipment used to access the ICS remotely.

The key ICS security takeaway is that this ex-contractor should not have been able to access the system remotely. Robust access control and authentication processes would have prevented this attack.

AIR-GAPPED ICS ATTACK - STUXNET

In 2010, International Atomic Energy Agency Inspectors visiting the Natanz nuclear facility in Iran observed a significant number of uranium-enriching centrifuges had failed. It is believed that at this time, the Iranian operators had sought the help of computer security specialists from Belarus to examine the computer systems controlling these centrifuges in their investigations.

This investigation led to the discovery of multiple malicious files that were identified as the Stuxnet worm. In total, more than fifteen Iranian facilities were attacked and infiltrated by the Stuxnet worm. Current estimations are that the Stuxnet worm destroyed more than 980 uranium-enriching centrifuges, leading to around a 30% decrease in enrichment efficiency and putting a significant delay in the Iranian nuclear program.

The attack is believed to have started when a malware-infected USB drive was connected to a computer terminal on one of the air-gapped ICS. This may have been a deliberate act or achieved by an employee unknowingly using an infected drive.

The Stuxnet malware looks for the presence of specific models of programmable logic controllers (PLCs) manufactured by Siemens on the infected network. If none are found, the malware remains dormant and relatively undetectable to standard security controls. Where target PLCs are present, the malware carefully alters the PLCs' programming to affect their operation. In the case of the centrifuges, the malware caused them to be spun irregularly. This action led to damage and, in some cases, destruction. During the attack, the PLCs are programmed to create and return false data indicating routine operation, which prevents detection of the erroneous operation until after the damage has been done.

This attack was undertaken in such as manner as to hide the malicious actions and allow the end failure to appear as a regular component failure mode rather than a deliberate attack, allowing the attack to last a significant period before suspicions were eventually raised.

This malware operated using multi-phase attacks. Initially, Windows-based networks and computer systems were compromised using four zero-day exploits; a Windows Shortcut flaw, a print spooler flaw, and two escalations of privilege vulnerabilities.

The malware then compromised specific Siemens PLCs using a combination of a zero-day exploit and a known vulnerability previously exploited by the Conficker virus.

Once established, the malware switches to behave as a worm; that is, it continually replicates itself on all accessible networks and devices. This includes the ability to infect any removable media, such as a USB drive, when connected.

Then the malware infected instances of Windows-based Siemens Step7 software, which is commonly used in industrial computing networks for ICS control and was used by the affected Iranian nuclear enrichment facilities.

Compromising the Step7 software allowed the malware access to the industrial program logic controllers enabling control of connected equipment and the ability to exfiltrate sensitive operating information.

While the attacker was never identified, the sophistication points to one or more nation-states specifically targeting the ICS-based facilities of the Iranian nuclear development program.

The key ICS security takeaway is that air-gapped systems are not secure by default and require the same level of protection as networked systems. Robust removable media processes and intelligent system monitoring solutions may have prevented this attack.

COORDINATED ICS ATTACK – UKRAINIAN POWER DISTRIBUTION

On December 23, 2015, the control centers of three Ukrainian electricity distribution companies were remotely accessed in a coordinated attack. As a result, the attackers could take control of the SCADA systems at each facility using established network hacking techniques to exploit remote access vulnerabilities and steal operator credentials. This access enabled them to operate circuit breakers across approximately 30 distribution substations in Kyiv and the surrounding region.

The power outage lasted up to six hours. During that period, the attackers launched a denial of service attack on the customer services phone lines to create confusion and reduce central visibility of the extent of the disruption. The malware also allowed attackers to affect support equipment at the control centers, disrupting network recovery operations.

This was the first of a series of attacks launched on Ukrainian critical industrial infrastructure and has been linked to Russia-based cyber-criminal groups operating under state control. This malware has also been found on the ICS of a Ukrainian mining company and a state-owned railway operator.

The first attack in 2015 is believed to have been undertaken by the Sandworm Team, a Russia-based group that targets industrial control systems. The attack was traced by the presence of the BlackEnergy3 trojan.

The original BlackEnergy malware was first used in 2007 to launch Distributed Denial of Service (DDOS) attacks on ICS. A second version, BlackEnergy2, undertook more sophisticated and targeted attacks on ICS HMI. BlackEnergy3 is the latest known evolution that uses plugins to tailor its actions for each specific ICS target. The malware is typically delivered using spear-phishing e-mails to gain a foothold on the target system. Once successfully delivered, the malware creates a backdoor to enable the exfiltration of system information and access for further attacks into the ICS.

One of the subsequent attacks on the Ukrainian electricity distribution companies was the use of the BlackEnergy3 infection to deliver the Killdisk malware that deletes system files and corrupts the operating system to prevent rebooting.

In a follow-on attack on a Ukrainian transmission substation in 2016, the Sandworm Team employed a new malware named Industroyer. Also known as CrashOverride, this malware is a significantly more sophisticated development of BlackEnergy3, again designed for manipulating ICS. It can exploit vulnerabilities in communication protocols to directly control remote equipment without the need to infect the ICS control software, making detecting malware infections harder to identify.

The key ICS security takeaway is that hostile nation-states will target critical national infrastructure with the resources and capabilities to launch sophisticated, coordinated attacks that are challenging to resist. Therefore, a comprehensive suite of security solutions providing strength in depth is vital when facing advanced persistent threats.

SIS ATTACK – SAUDI ARABIAN PETROCHEMICALS

In 2017 an outage occurred at a petrochemical plant in Saudi Arabia that was believed at the time to be a mundane mechanical failure of plant equipment. However, a second incident prompted investigators to look at the ICS, which uncovered the presence of Triton malware, also known as Trisis. The names derive from the malware specifically targeting the Triconex safety controller model produced by Schneider Electric.

This malware is designed to remotely take control of the physical controllers and the control software for a plant's safety instrumented systems. This allows the attackers to disable or disrupt safety controls such as shutoff and pressure venting valves that prevent plant failures from creating a safety-related or safety-critical incident. In addition, if the plant's ICS were also compromised, this would allow attackers to create a safety incident and prevent the safety systems from preventing failure leading to loss of life or other catastrophic consequences. The worst-case scenarios for the affected petrochemical plant included the potential for releasing toxic hydrogen sulfide gas or a significant explosion of flammable gases.

The malware was detected due to a coding error that initiated safety system actions that resulted in the plant's shutdown. The first shutdown in June 2017 was treated as a typical system failure. However, this was followed by a series of events that led to another shutdown in August 2017. The investigation into the cause of the second shutdown revealed the presence of malware.

Investigations concluded that the attack had started three years earlier, in 2014, with the compromise of the business's IT network using a vulnerability in the perimeter security controls. As a result, the attackers were able to undertake undetected reconnaissance and lateral movement until they eventually gained access to the business's ICS and obtained login credentials for an engineering workstation. At this point, they were able to exfiltrate system information, including details of the systems' hardware controllers and firmware versions.

It is believed that the attackers replicated the target SIS using identical equipment to identify a zero-day vulnerability in the Triconex firmware and develop malware code to exploit this weakness and compromise the SIS components by injecting code directly into each affected controller.

Analysis of the malware code identified credible links to the Central Scientific Research Institute of Chemistry and Mechanics in Moscow, a government facility involved in industrial safety research. Government involvement seems likely given the effort required to produce malware that would only work on a specific controller model with a particular firmware version and hence very limited possible industrial facilities.

This attack has demonstrated the vulnerability of ICS components to a determined and sophisticated threat actor with the resources and motivation to target a specific facility.

The key ICS security takeaway is that attacks on operational technology do not always target obvious elements such as supervisory process controls. Instead, advisory components of industrial control systems may also be targeted to launch multi-faceted attacks intended to maximize damage. This is particularly true where the attacker has the resources and capabilities to launch sophisticated, coordinated attacks that are challenging to resist. Therefore, a comprehensive suite of security solutions providing strength in depth is vital when facing advanced persistent threats.

SCADA REMOTE ATTACK - BOWMAN AVENUE DAM

In 2013, the SCADA system controlling the Bowman Avenue Dam in New York was attacked using an insecure cellular modem connection as the entry point. The attackers were able to compromise the SCADA system undetected remotely. The attacker was able to access status information, including water levels, and control the status of the sluice gate, which is responsible for regulating the water flow rate through the dam.

The attack was detected when US intelligence agencies monitored the activities of Iranian hackers with a record of attacking American corporations. As a result, they were able to alert the dam operator and halt the attack. However, for the duration of the attack, the sluice gate was offline for maintenance, so the attacker could not perform any malicious activity.

The Bowman Avenue Dam is a small and relatively insignificant facility, so uncontrolled water release would not have catastrophic consequences. However, given the limited nature of the effects of the attacker interfering with the sluice gate operation, the belief is that the attack was possibly a test to prepare for an attack on a more significant facility. Alternatively, it may have been mistaken for the much bigger Bowman Dam in Oregon.

The key ICS security takeaway is that attacks can be launched on any target, not just those that may cause severe damage or generate the most newspaper headlines. Systems of all shapes and sizes may be attacked, and the purpose of the attack may be to gain knowledge that can be subsequently exploited on larger targets. Therefore, all operational technology should be protected with adequate and proportional security controls, irrespective of size and perceived importance.

REMOTE ACCESS ATTACK - OLDSMAR WATER TREATMENT FACILITY

In 2021, an attacker gained remote access to the ICS controlling the Oldsmar water treatment plant in the Tampa Bay area of Florida. The plant had installed the TeamViewer software package to allow remote access to the ICS during the Covid pandemic. The attacker exploited a vulnerability in this TeamViewer commercial software package to gain remote access to the ICS HMI. This interface allowed the attacker to alter the dosing rate of Sodium Hydroxide (NaOH) in the water during the treatment process. This chemical is used in small doses to adjust pH and alkalinity. However, high doses can be hazardous.

The attack was detected and halted by an on-duty operator at the plant observing the attacker's actions on their HMI monitor, including raising the NaOH dosage to a noticeably elevated level. As a result, the operator was able to reverse the attacker's actions quickly enough to prevent any hazard to consumers.

This attack was halted by chance. For example, suppose an operator had not been monitoring the HMI at the time of the attack. In that case, unsafe quantities of a hazardous chemical could have entered the consumer's water supplies before the ICS's inbuilt controls raised the alarm. Also, suppose the attacker had been more competent. In that case, they could have hidden their actions fairly easily by altering the HMI displays for the duration of the attack and choosing to increase NaOH dosing sufficiently to affect water safety without triggering monitoring alarms.

The attack highlighted two critical weaknesses in the ICS. Firstly, the attacker could gain complete control of the ICS through a vulnerability in an Internet-connected remote access tool that is not intended for use in critical applications. Secondly, the HMI accepted and actioned a command to increase NaOH dosage to an unsafe level.

The key ICS security takeaway is that all applications that allow remote access should employ robust access control and authentication processes to prevent unauthorized access through compromised user credentials or exploitable vulnerabilities.

ABOUT **LMNTRIX**

Often times, the difference between preventing a cyber attack or suffering a crippling loss is simply knowing where to look for the signs of a compromise. Even the most advanced attackers leave traces of their presence so an effective defense must not only be vigilant, but also ever-adaptive in response to changes in attacker tactics. A critical element in this age of constantly evolving threats is a detailed view of an organization's entire potential attack surface. Log collection solutions are simply outgunned against today's advanced threat actors as they either lack the data, or the ability to analyze their data in a manner that allows rapid attack detection.

LMNTRIX has reimagined cyber security, turning the tables in favor of the defenders once again. We have cut out the bloat of SIEM, log analysis, false positives and associated alert fatigue and we created new methods for confounding even the most advanced attackers. We combine deep expertise with cutting-edge technology, leading intelligence, and advanced analytics to detect and investigate threats with great speed, accuracy, and focus. We believe that in a time of continuous compromise you need continuous response – not incident response. Our approach turns inward and assumes that you're already breached and that you're continually going to be breached, so we take a pro-active, offensive, hunting, adversarial pursuit stance as opposed to a reactive, defensive, legacy stance with analysts staring at a SIEM console wishing they could detect an APT. As a company we stand in defiance of the unwanted human presence within corporate networks by attacking the root of the problem—the adversary's ability to gain entry and remain undetected. Our real-time hunt operations identify signs of planned and active attacks and take action to neutralize them, forming the basis of our comprehensive Active Defense approach to limiting security exposure.

LMNTRIX Active Defense is a best in class Managed Detection & Response (MDR) service that detects and responds to advanced threats that bypass perimeter controls. The outcomes we deliver clients are validated breaches that are investigated, contained and remediated. All incidents are aligned to the kill chain and MITRE ATT&CK frameworks and contain detailed investigative actions and recommendations that your organisation follows to protect against the unknown, insider threat and malicious attacker.

We are a partner which becomes an extension of your internal team, can augment your MSSP, or be a full-service SOC as a service security solution.

LMNTRIX Active Defense is a three-tier outcome-based solution (Gartner refers to it as Managed Detection & Response (MDR) and our platform Extended Detection & Response (XDR).

(1) LMNTRIX XDR (AWS Data Lake and Platform)
(2) LMNTRIX TECHNOLOGY STACK (Deployed deep within Customer Networks)
(3) LMNTRIX CYBER DEFENSE CENTRE (Security Analyst Driven).

LMNTRIX XDR natively unifies Machine and Underground Intelligence, NGAV, EDR, NDR, Network Forensics, MTD, CSPM, CDR, UEBA, and Deception Everywhere with completely automated attack validation, investigation, containment and remediation on a single, intuitive platform. Backed by a 24/7 Managed Detection and Response service – at no extra cost – LMNTRIX provides comprehensive protection of the environment for even the smallest security teams. It is a single investigative platform for insights into threats on enterprise, cloud, hybrid, and industrial control systems (ICS) networks. The LMNTRIX XDR delivers unique advantages over current network security solutions. It is a holistic and multi-vector platform with unlimited retention window of full-fidelity network traffic, innovative security visualizations, and the ease and cost-savings of an on-demand deployment model.

LMNTRIX XDR is based on multiple detective, responsive, and predictive capabilities that integrate and share information to build a security protection system that is more adaptive and intelligent than any one element. The constant exchange of intelligence, between the Active Defense components and the wider cybersecurity community enables LMNTRIX to keep abreast of the tactics techniques and procedures (TTP's) of the most persistent, well-resourced, and skilled attack groups.

Figure 10 - LMNTRIX XDR

LMNTRIX TECH STACK is a powerful, proprietary threat detection stack embedded within the client environment, behind existing controls. TECHNOLOGY STACK comprises multiple detective systems, combining threat intel application and correlation, static-file analysis, user and entity behavior analytics (UEBA) and anomaly detection techniques to find threats in real-time. It eliminates 'alert-fatigue' determining which alerts to escalate through multi-platform consensus.

Figure 11 - LMNTRIX XDR – A Comprehensive Threat Prevention, Detection & Response Platform

LMNTRIX CYBER DEFENSE CENTER (CDC) A global network of Cyber Defense Centers comprising trained and certified hunters and intrusion analysts, provides constant vigilance and on-demand analysis of your digital assets and networks. Our intrusion analysts actively probe and monitor your networks and endpoints 24x7, using the latest intelligence and proprietary methodologies to look for signs of compromise. When a suspected breach is detected, the team performs an in-depth analysis of potentially affected systems to confirm the breach. When data theft or lateral movement is imminent, our endpoint containment feature makes immediate action possible by quarantining affected hosts, whether they are on or off your corporate network. This significantly reduces or eliminates the consequences of a breach.

Figure 12 - LMNTRIX Cyber Defense Centre

SECURITY POSTURE
SELF-ASSESSMENT

The following questions have been provided to enable you to complete a high-level self-assessment of the security controls in place for your ICS. The results should offer an indicative insight into the current security posture of your ICS to guide your next steps in improving the robustness and coverage of security controls.

Complete the questionnaire as best as possible and add up all scores to obtain your company's security readiness rating. The result provides an assessment of your protection against the most common and critical ICS threats.

Please note that this questionnaire does not replace the need for a comprehensive security risk assessment, and the results should be used simply as guidance for the best route to achieving secure systems,

- Score 0 to 49 - Based on your answers, your ICS does not appear to have adequate security controls and is vulnerable to disruption from the broad range of threats currently targeting ICS. You should, as a matter of urgency, initiate a comprehensive security risk assessment to identify all credible threats to your systems and identify the appropriate security controls to manage these risks.

- Score 50 to 89 – Based on your answers, your ICS has some security controls in place but remains vulnerable to disruption from unmanaged threats. You should prioritize completing a comprehensive security risk assessment to identify those risks to your systems that are not currently adequately managed and identify any additional security controls required to manage these risks.

- Score 90 to 100 – Based on your answers, your ICS has comprehensive security controls in place for the most common and critical ICS threats. We still recommend undertaking a security risk assessment to ensure that all credible risks to your systems are adequately identified and managed and that existing security controls remain effective.

	NOT IMPLEMENTED	PARTLY IMPLEMENTED	FULLY IMPLEMENTED	NOT APPLICABLE
Malware Infection via Physical Connectivity, including Removable Media and External Hardware				
Connection of removable media is prevented	0	2	5	5
Use of any unauthorized hardware is prohibited.	0	2	4	4
Removable media scanned for malware before use.	0	2	4	4
Policies are in place to control the connection of third-party hardware.	0	1	2	2
Malware Infection via Network Connectivity, including Internet and Intranet				
ICS network is separated from business IT networks.	0	2	5	5
Malware protection is in place on network devices and ICS network boundaries.	0	2	4	4
ICS network devices are hardened to disable unneeded services and connections.	0	2	4	4
Robust ICS network boundary security controls are in place.	0	2	4	4
ICS network is air-gapped from the Internet.	0	3	6	6

	NOT IMPLEMENTED	PARTLY IMPLEMENTED	FULLY IMPLEMENTED	NOT APPLICABLE
Intrusion via Remote Access				
Strong authentication and encryption are employed on all remote access.	0	2	4	4
Remote access is only granted when required and to specific ICS components.	0	2	4	4
Only trusted and certified third-party service providers are allowed remote access	0	1	2	2
Remote connections are timed out after use.	0	1	2	2
Policies are in place to impose security controls on remotely connecting equipment, including anti-virus protection.	0	2	4	4
Social Engineering and Phishing				
All employees receive regular awareness training.	0	1	2	2
Policies are in place for the acceptable use of ICS.	0	1	2	2
Technical security controls enforce compliance with policies.	0	2	4	4

	NOT IMPLEMENTED	PARTLY IMPLEMENTED	FULLY IMPLEMENTED	NOT APPLICABLE
Technical and Human Error				
ICS implements robust monitoring and critical system redundancy to manage technical failures.	0	2	4	4
Access controls grant the least privilege for ICS services to limit the impact of human error.	0	2	4	4
Backup and recovery processes allow the restoration of services and the rollback of erroneous changes.	0	2	4	4
Logging records include sufficient information for the investigation and correction of errors.	0	1	2	2
Technical controls monitor system configurations and health.	0	1	2	2
Insider Attacks				
Sensitive ICS information is released on a need-to-know principle.	0	1	2	2
Access controls grant the least privilege for ICS services to limit the impact of deliberate malicious actions.	0	2	4	4
Backup and recovery processes allow the restoration of services and the rollback of erroneous changes.	0	1	2	2
Technical controls monitor system configurations and health.	0	1	2	2

	NOT IMPLEMENTED	PARTLY IMPLEMENTED	FULLY IMPLEMENTED	NOT APPLICABLE
Dos Attacks				
Network monitoring and alerting reports and responds to significant traffic changes.	**0**	**2**	**4**	**4**
External connections of critical systems include redundancy using different communication technologies.	**0**	**2**	**4**	**4**
Boundary security controls include protection against denial of service attacks.	**0**	**2**	**4**	**4**

Total Score (Maximum 100)