
Accedere
Industrial (ICS)
Cybersecurity
Services

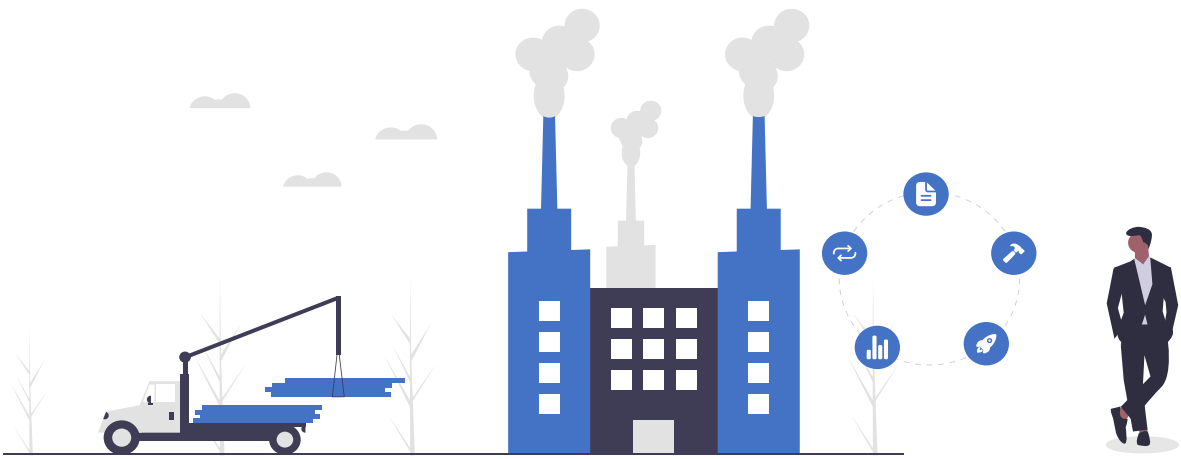
Table of Contents

Introduction to ICS

Operations technology (OT) is the term used in industrial operations and it comprises of control systems, networks, and other industrial automation components that control physical processes and assets. Industrial control systems (ICS or IACS), which are part of the OT environment in industrial enterprises, encompass several types of control systems including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC), remote terminal units (RTU), intelligent electronic devices (IED) and other field devices.

Background: In the recent past attacks such as Industroyer, Sweyntooth, and CSRF attack on Schneider Electric ION Power Meter, and many other attacks, organizations have realized the importance of safeguarding the ICS and the IT-OT converged environments. Today the world is talking about connecting everything to the internet. As the fourth industrial revolution (Industry 4.0) a term used to draw together cyber-physical systems, Internet of things (IoT or IIoT) and Internet of Services starts to find more resonance with OEMs, system integrators, and asset owners. ICS systems were originally designed for increasing performance, reliability, and safety by reducing manual efforts. Security was achieved by physical isolation, so-called airgap or security by obscurity.

Approach: A cybersecurity Governance and Management system should be implemented for the defined ICS. This should be incorporated into the site's wider management systems. As introduced by North American Electric Reliability Corporation (NERC), by staying NERC CIP compliant and adjusting your business policies to NERC regulations as they are announced, organizations will succeed in protecting its customers, critical cyber assets, and the Bulk Electric System. Other standards like IEC 62443 may also applicable in other environments.



ICS Cyber Challenges

With increasing integration of ICS with corporate network and Internet for business requirements, it is obvious that ICS is opening itself to the world of attackers. With cyber-attacks continually escalating in frequency, severity, and impact year after year it is with this concern that it is of paramount importance to ensure cybersecurity around such systems.

Three major security challenges associated with ICS:

Loss of Control: With the use of Public Cloud, organizations lose control over IT and Data. Without proper Architecture, Cloud Adoption can be daunting. IIoT data from ICS environment going to cloud can be a complicated beast that involves layers of regulations when data is stored in the Cloud.

Limited Visibility: Many Organizations have no or little control over access to cloud services. Even if they are aware of the cloud applications or environments, they have a little administrative, identity, and access control, and Security Event or Incident Management (SIEM) is minimal and it takes about 200 days to detect a breach.

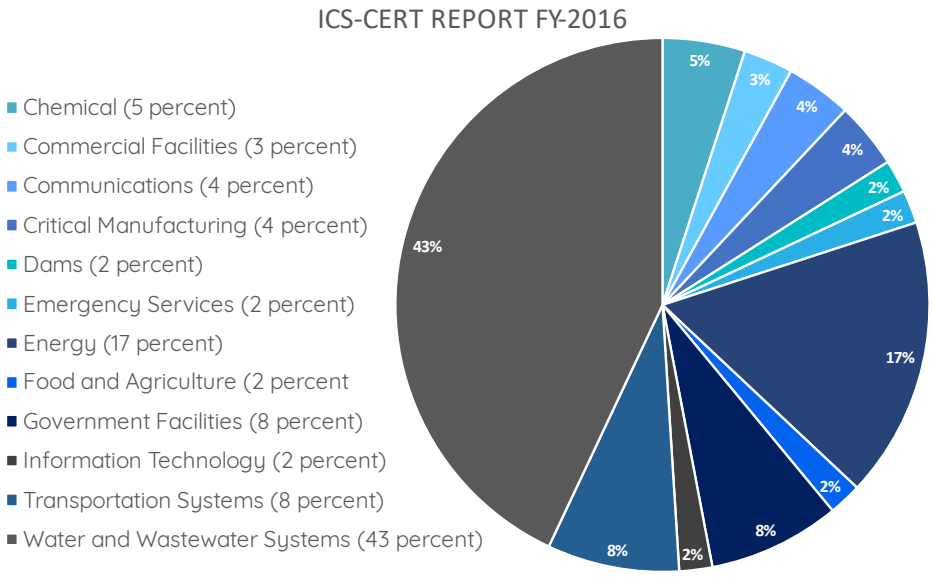
Real-time Connectivity: In many plants with ICS, engineers and their internal information technology (IT) counterparts have very different perspectives on cybersecurity. Often, they work in silos. Not surprisingly, these different perspectives often lead to conflicts when connecting an ICS to the plant's IT system.

Major ICS security threats:

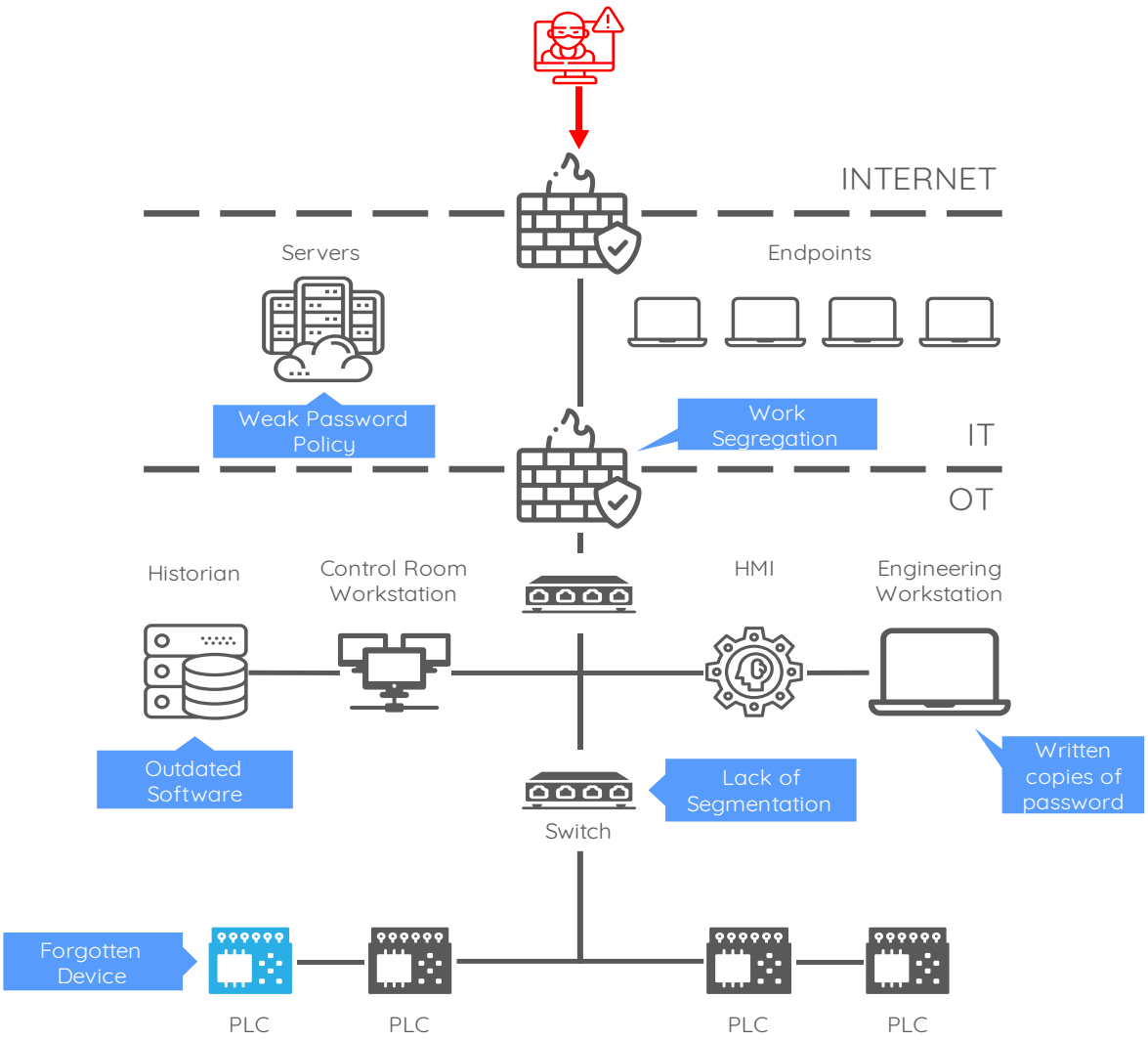
Deliberate
- Disgruntled employees
- Industrial espionage
- Cyber hackers
- Viruses and worms
- Terrorism

Inadvertent
- Safety failures
- Natural disasters
- Equipment failures
- Human mistakes

As per surveys conducted on threats to ICS, it is very evident that attackers are finding new ways to get into systems by exploiting the weaknesses it has carried forward for a long time. Almost all critical infrastructures are being targeted:

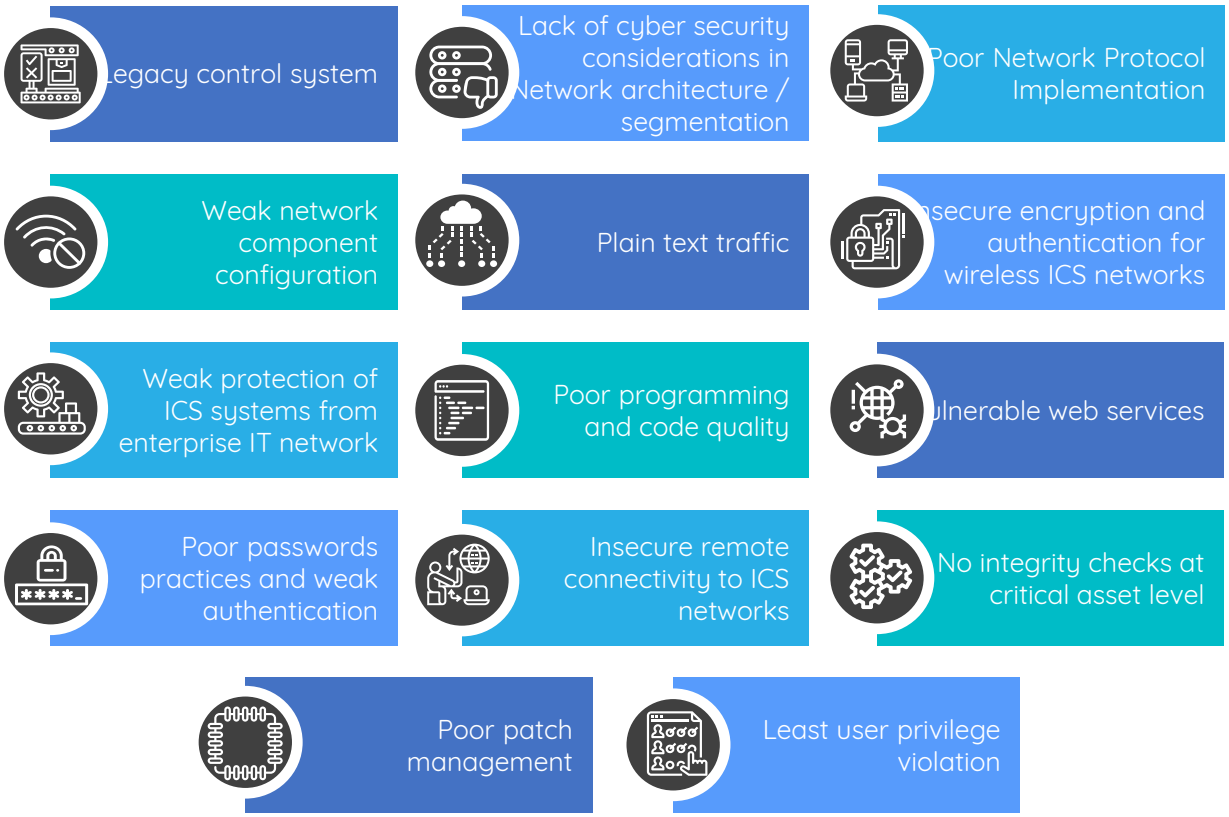


Source ICS-CERT REPORT FY-2016



ICS Attack Scenario

ICS systems consists of various weaknesses in it which makes it much easier for attackers to target:



Weaknesses in ICS Security

Diagram 3: Factors Involved

To overcome these ICS threats many government agencies, non-profit organizations and nation states have developed different standards over the years. Few standards are country specific and few are globally applicable. These standards suggest appropriate controls requirements to secure the ICS. These standards provide guidance related to secure configuration, best practices, security policy, secure network architecture and secure operating procedures.

Three factors are very critical in these standards: People, Process, and Technology; people who together are ultimately responsible for the security of the system.

Components of ICS

ICS components:

- PLC /RTU
- HMI server and clients
- Historian
- Operator Workstation
- Engineering Stations
- Drives and I/O

SCADA Applications:

- Webserver
- Web client
- Embedded Webpages
- Configuration software

Security:

- Firewall
- IPS /IPD
- Antivirus /Endpoint protection

Hardware:

- Network switches
- Gateways
- Printers

Best practices for performing the High-level risk assessment:

- Collect information about which ICS systems/packages in the organization that are to be procured and installed.

- Define on a holistic level the worst-case cyber threat scenarios based on inputs such as the corporate risk matrix, business impact assessments, etc.

- Define the business criticality/consequence of the worst-case scenarios (safety, environmental, financial, brand). Consider using input from the safety discipline work related to HAZID and HAZOP activities.

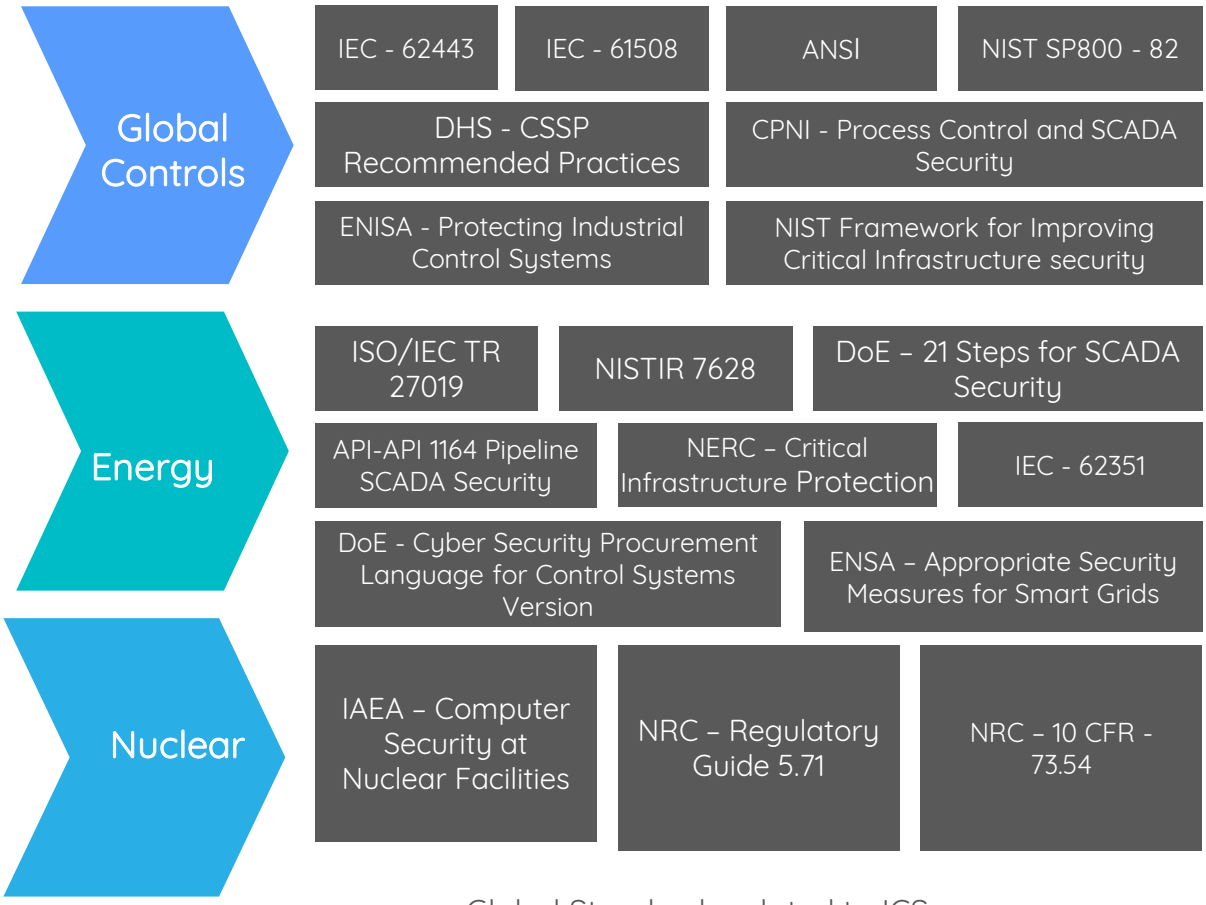
- Describe which of the ICS systems/packages that will have critical functionality needed to implement the safety systems and barriers and define the generic independent layers of protection. Consider using a bow-tie-based approach.

- Define the likelihood of the worst-case scenarios (e.g. high, medium, low). The likelihood can for example be based on the threat agent's capability, motivation and opportunity to exploit a threat vector. The opportunity is based on the vulnerabilities in the respective systems.

- Based on previous steps, conduct a relative risk ranking of unmitigated risks relating to the organizations' systems/packages.

Global ICS Security Standards

Each sector has different challenges and multiple threats associated to it, based on the specific environment, the standards varies, for example NERC CIP is applies to energy sector whereas few standards are globally applicable such as IEC 62443.

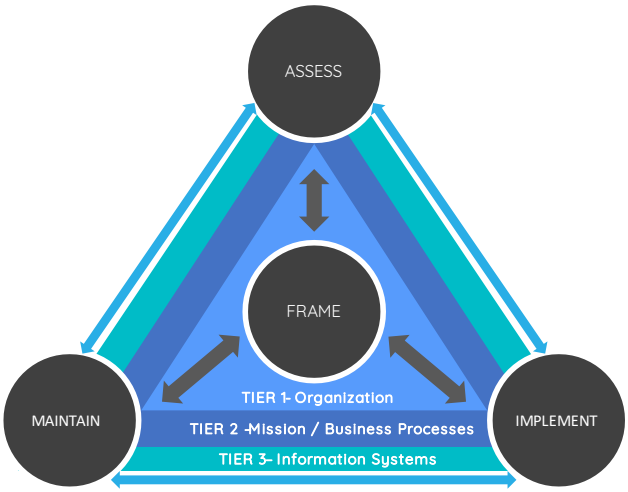


Global Standards related to ICS

NERC CIP Compliance

In 2019, the North American Electric Reliability Corporation (NERC) has imposed a penalty of $10,000,000 on a participant in the electric market for fundamentally failing to comply with the NERC Critical Infrastructure Protection (CIP) standards, in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions.

ICS Risk Assessments



As a first step, we recommend a security assessment over the ICS infrastructure and base it against the NERC CIP, IEC 62443 or other requirements to assess the current state vs specific requirements. The assessment includes the system's records and activities to determine the adequacy of system controls.

Risk assessment enables the organization to prioritize activities to secure a system. Cybersecurity is an exercise in risk management. Organizations have limited resources and can rarely afford to implement all countermeasures to fully protect the system. Thus, cybersecurity expenditures must be balanced based on potential impact.

Risk assessment involves reviewing corporate practices utilizing industry-accepted best practices, industry regulations, and applicable standards. The risk analysis uses employee interviews, site tours, and comprehensive corporate policy/procedure review. Risk assessments are typically based on accepted frameworks like NERC, NIST, or ISA 62443. It is important to note that assessments involve company processes and personnel in addition to technology. Risk assessments are typically the first step in an overall vulnerability assessment and can be followed by passive or active assessments.

Passive assessments involves discovering network devices using passive means, such as site surveys, network/architecture drawings, system logs, equipment configuration files, and network traffic analysis. The team can also review equipment data against vulnerability databases.

Active assessments involves using tools to scan the network. Examples of tools used during the active assessment include Nmap, Shodan, and Nessus. It is important to note that active assessment places traffic on the ICS network which could introduce risk.

Note: *Active assessments are done mostly on a testbed environment.*

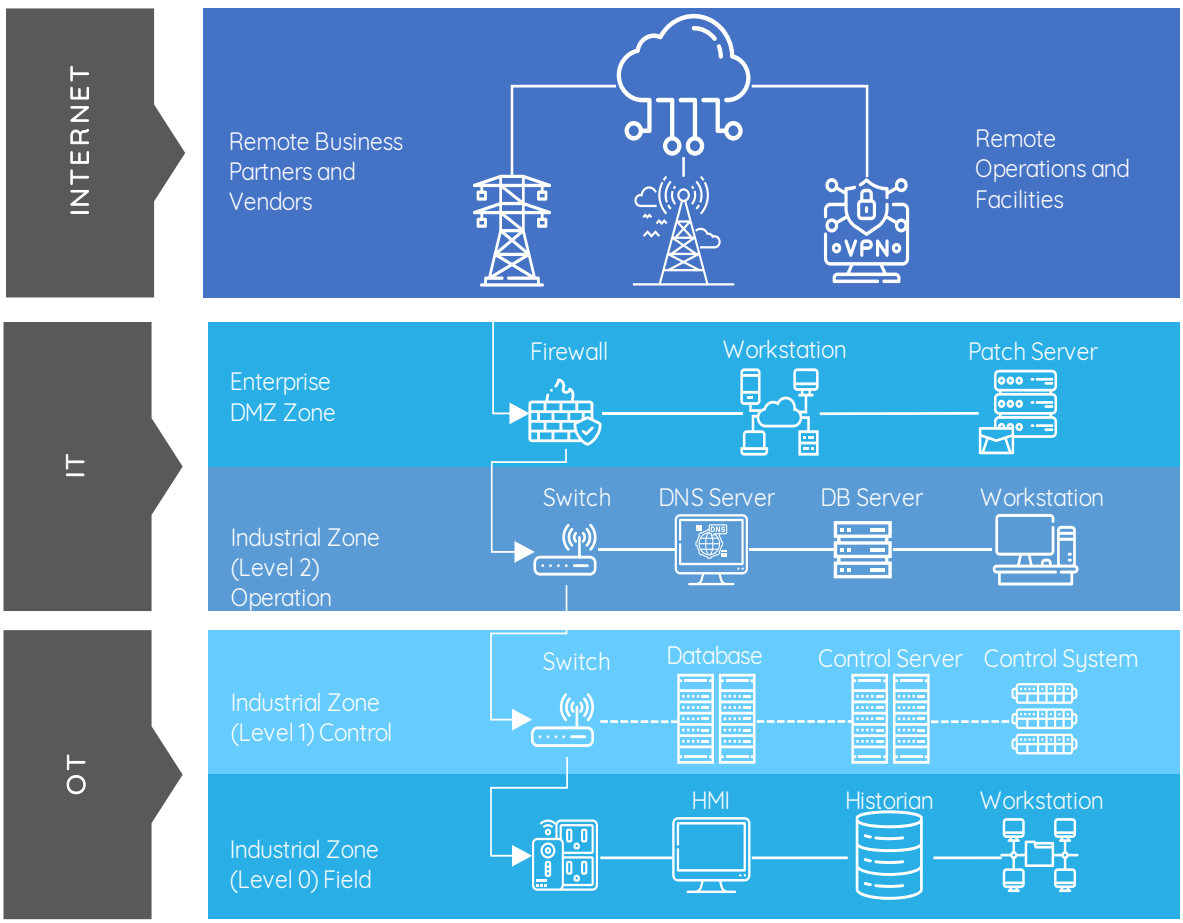
ICS VA/PT

Penetration testing is the follow-on step to the prior steps. In penetration testing, attempts are made to exploit known and unknown security vulnerabilities discovered by the earlier steps using exploit tools and techniques. Penetration testing can be used to validate vulnerabilities and test the effectiveness of countermeasures.

Our cybersecurity team is well versed with the ICS environment, its challenges, and subject matter experts in VAPT of ICS components.

A three-step approach is followed to examine the ICS security posture:

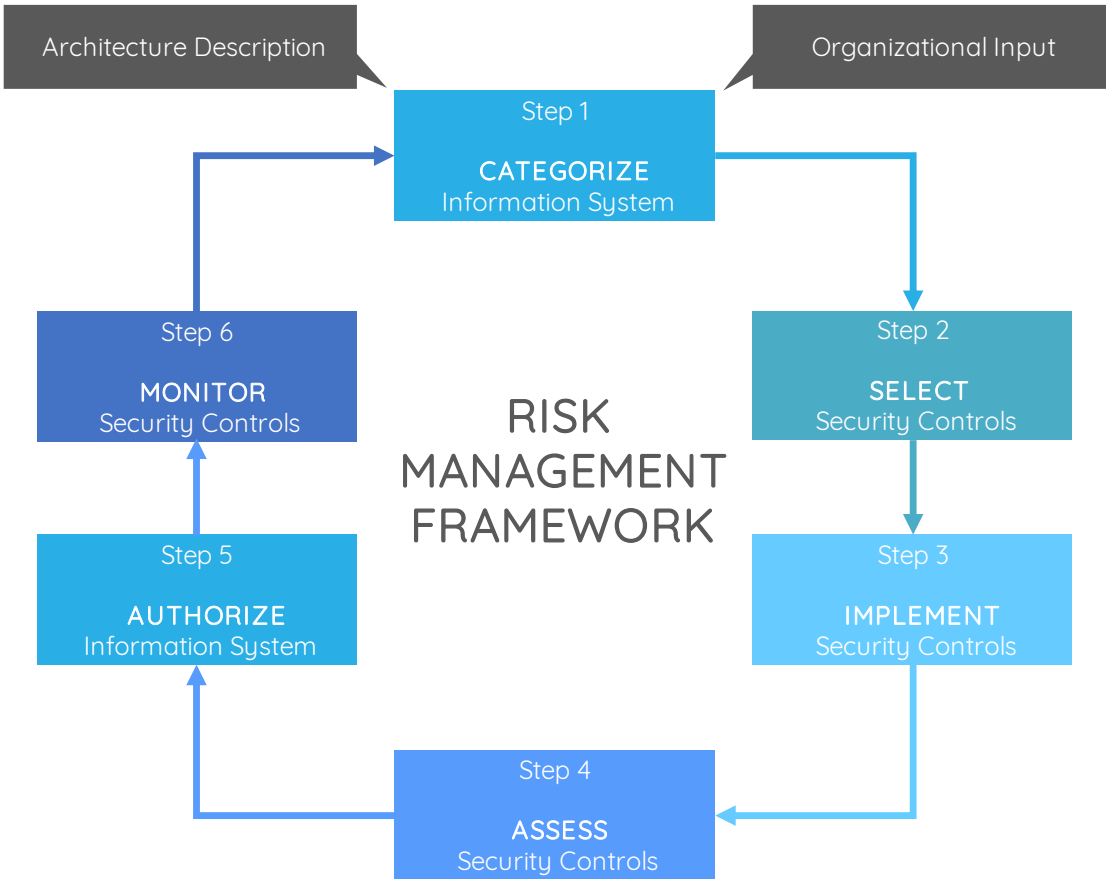
- Test ICS network from the Internet
- Test ICS network from IT
- Testing selected offline ICS systems for vulnerabilities



Sample ICS Architecture

Governance Framework

An effective Governance Framework helps in compliance. It is important for organizations to adapt and monitor the maturity of Risk Mitigation measures thru this Governance Framework. For effective complying against the NERC CIP, IEC 62443 or other requirements or specific security standards that may apply to your environment..



Security operations center (SOC)- is important control to have visibility into your network. In case of an event, a SIEM tool helps you to inspect and analyze the logs to get to the source. SOC is an essential part of today's security. Your SOC for a combined ICS-IT environment to enable you to monitor and act upon the threats and attacks.

Training/Awareness-You will also need to have a customized training to your team members based on their job profiles.

Internal Audit Before your NERC CIP Audit-Our team can conduct an Internal Audit for your environment to reduce your risks on the main audit thus saving you with fines and penalties.

Our ICS Security Approach for Compliance or ISO 27001 Certification

We provide Industrial Cybersecurity services for NERC CIP Compliance, IEC 62443 Compliance or ISO 27001 Certification and to improve the security posture of your ICS or OT systems from threats. Following procedures are followed for ICS Security Assessments:

- ICS Architecture, network topology review
- Vulnerability Assessment of Network Devices
- ICS Hardware review
- Vulnerability Assessment for Applications
- Vulnerability Assessment at Perimeter
- Vulnerability Assessment for OT-IT Integration
- Provide Recommendations
- Review and re-test if required
- Audit Report or ISO 27001 Certification as applicable

Network Assessment

External Penetration Testing

System Baselining

Recommendations

A critical element of any cybersecurity risk management program is the network assessment. It provides insights to Cybersecurity risks that could affect the achievement of the entity's operational objectives.

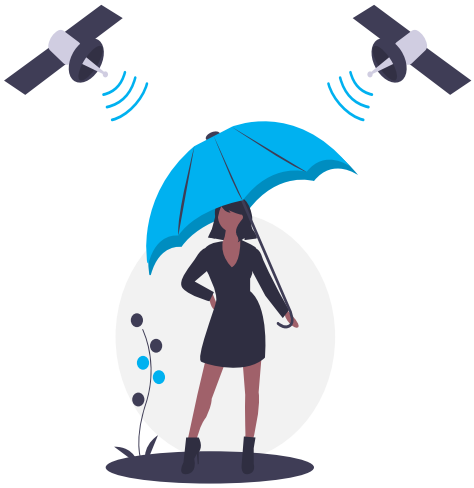
Our assessment includes activities like Internal Vulnerability Assessment, and External Penetration Testing, IT-OT connectivity testing and more

Our assessment shall include open ports, open services and provide hardening guidelines for ICS based on best practices.

Post Assessment we shall provide you with a draft report with recommendations on the way forward in lines with ICS best practices. We also offer ISO/IEC 27001 Certification service for ICS environments.

We Can Help With Your ICS Compliance

We provide end to end ICS Audit and Assessment for compliance with NERC- CIP, IEC 62443 and other standards. We can cover all key requirements to provide an assurance of your compliance with ICS security mandates and best practices. In an ICS Audit engagement, we can additionally cover ISO/IEC 27001 Certification for ICS environments to address your needs. Our unique delivery method improves timelines and thus reduces costs of your compliance. Our proven methodology saves times as well as costs thus giving you the benefit of timely assurance towards privacy compliance with reasonable costs.



Our Value Delivery

1. Experienced team in the area of Cyber Security..
2. Licensed Auditors, registered with PCAOB and Cloud Security Alliance and others. ISO/IEC 27001 Certification Providers.
3. Project management methodology applied to each engagement. These engagements are executed by senior professionals.
4. Prompt services with engagements completed in record time.
5. Ongoing support. We are with you whenever you need us.
6. Our services are competitively priced to provide you a higher ROI.