ACCEDERE

Industrial Control Systems(ICS) Security

March 31, 2017

Industrial Controls Systems(ICS) Security

INTRODUCTION to ICS

Operations technology (OT) is the term used in industrial operations and it comprised of control systems, networks and other industrial automation components that controls physical processes and assets. Control systems are at the heart of the nation's critical infrastructures, include electric power, oil and gas, water and wastewater, manufacturing, transportation, agriculture and chemical factories.

Industrial control systems (ICS), 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.

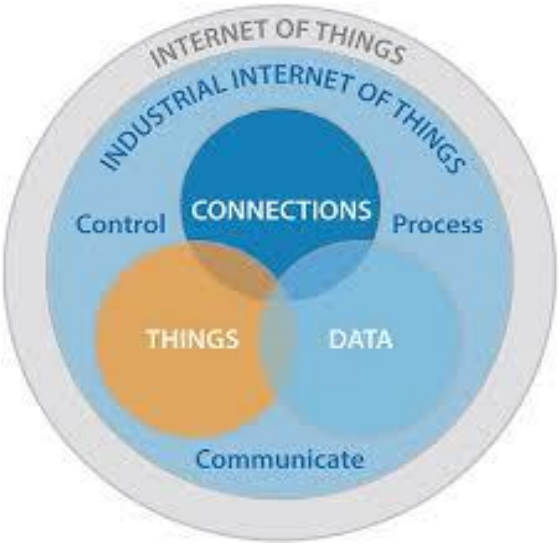
ICS systems were originally designed for increasing the performance, reliability and safety by reducing manual efforts. Security was achieved by physical isolation, so called airgap (security by obscurity).

In the recent past attacks such as Stuxnet, Shamoon and Ukarine Energy, organizations have realised the importance of safeguarding the ICS and the IT-OT converged environments. Today 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) and Internet of Services starts to find more resonance with OEMs, system integrators and asset owners, it is a matter of time that we will see lot of ICS information being routed to sophisticated applications across the enterprises through wide area network where security by obscurity is no longer a valid protection. Organizations and States have plans for connecting ICS to Internet for projects involving such as smart grids, smart cities, etc. which significantly increasing the risk of intrusion from malicious actors.

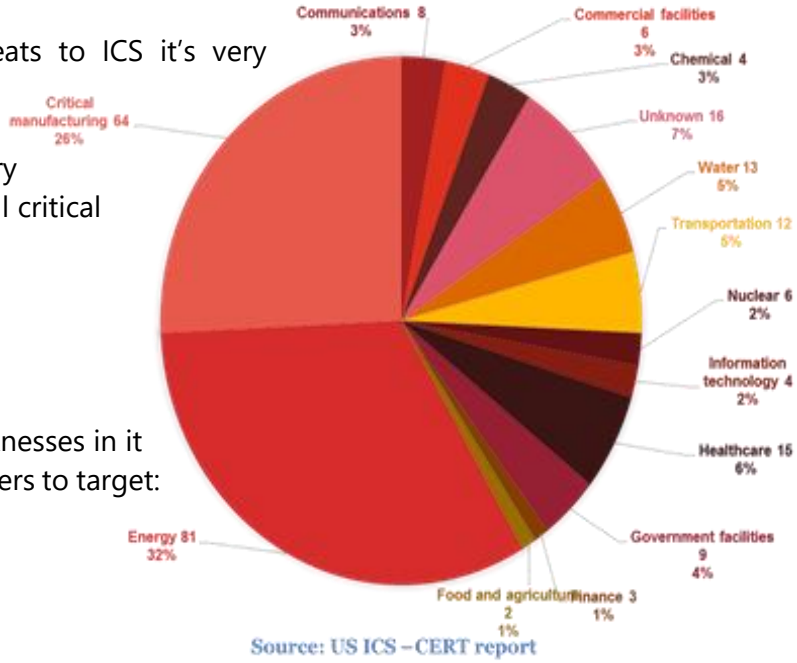
Threats to ICS

With ICS increasingly getting integrated with corporate network and Internet for business requirements, it is obvious that ICS is opening itself to the world of attackers. With cyber-attacks continue to escalate in frequency, severity and impact year after year it is with this concern that it is of paramount importance to ensure cyber security around such systems.
Majorly there are two types of security threats associated with ICS:

Inadvertent	**Deliberate**
Safety failures	Disgruntled employee
Natural disasters	Industrial espionage
Equipment Failures	Cyber hackers
Human mistakes	Viruses and worms

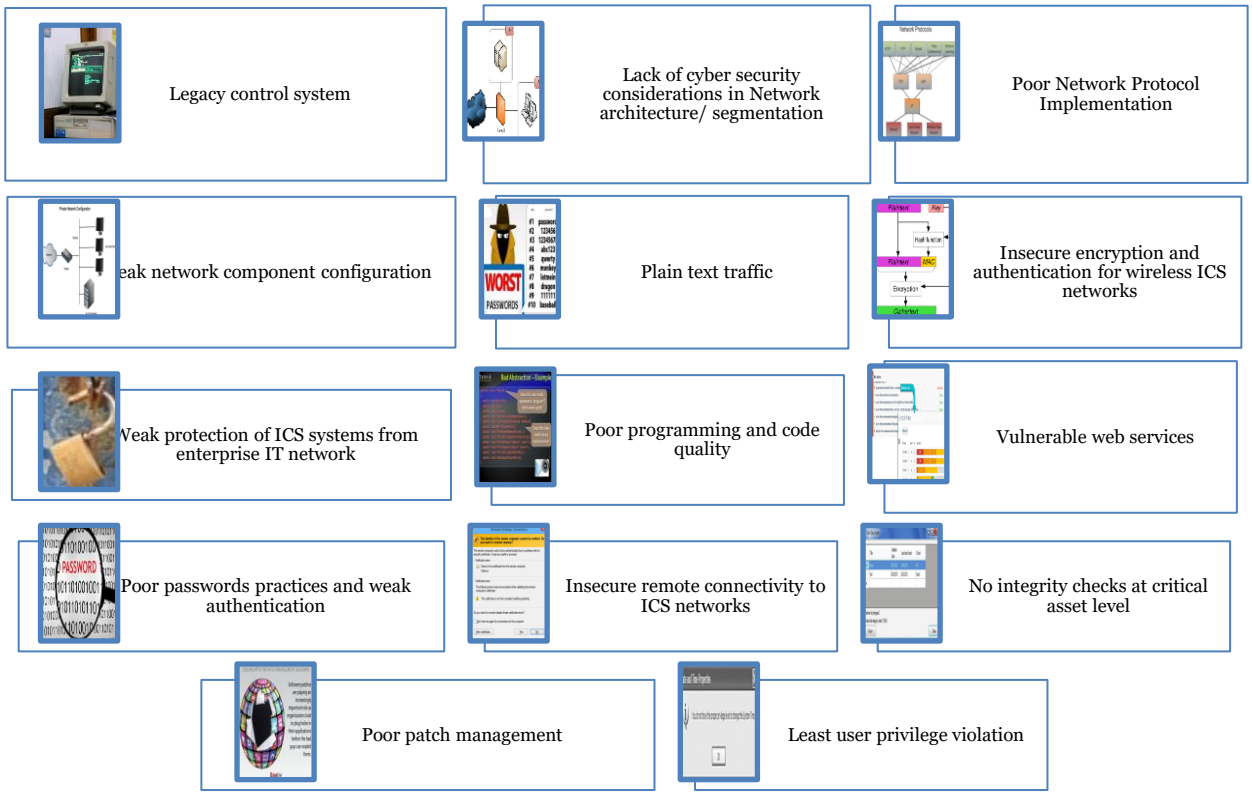


As per surveys conducted on threats to ICS it's very evident that attackers are finding new ways to get into systems by exploiting the weaknesses it has carry forwarded from long time. Almost all critical infrastructures are being targeted:



Source: US ICS – CERT report

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



To overcome these ICS threats many government agencies, non-profit organisations 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 which together are ultimately responsible for the security of the system.

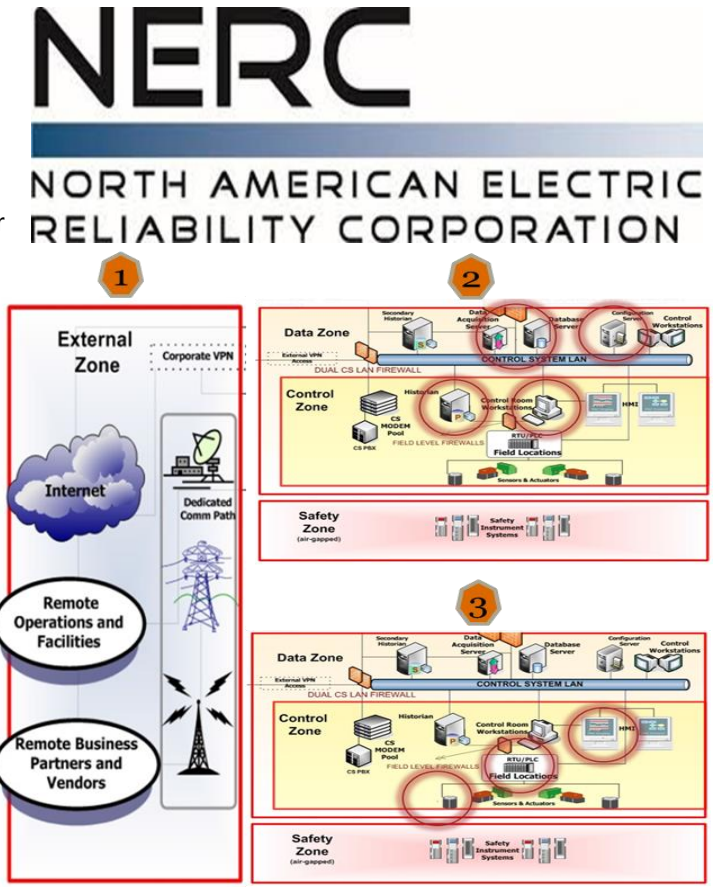
Global ICS security standards:

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

Global Standards	IEC-62443	IEC 61508	ANSSI
	NIST SP800-82	DHS - CSSP Recommended Practices	CPNI - Process Control and SCADA security
	ENISA - Protecting Industrial Control Systems	NIST - Framework for Improving Critical Infrastructure Cybersecurity	
Energy	ISO/IEC TR 27019	NISTIR 7628	DoE - 21 steps for SCADA security
	API - API 1164 Pipeline SCADA Security	NERC - Critical Infrastructure Protection	IEC 62351
	DoE - Cyber Security Procurement Language for Control Systems Version	ENISA - Appropriate security measures for smart grids	
Nuclear	IAEA- Computer Security at Nuclear Facilities	NRC - Regulatory Guide 5.71	NRC - 10 CFR - 73.54

NERC CIP Compliance

For the second time in less than a year (2016), the North American Electric Reliability Corporation (NERC) has imposed a six-figure penalty on a participant in the electric market for fundamentally failing to comply with the NERC Critical Infrastructure Protection (CIP) standards



Our services are based on the sector and its criticality. We provide cyber security services increase your security posture of your ICS/OT systems from threats. Some of them include the following:

1) ICS risk assessments

As a first step we recommend a security assessment over the ICS infrastructure and base it against the NERC CIP requirements to assess the current state vs NERC CIP requirements.

The assessment includes system's records and activities to determine the adequacy of system controls. The activities include review of

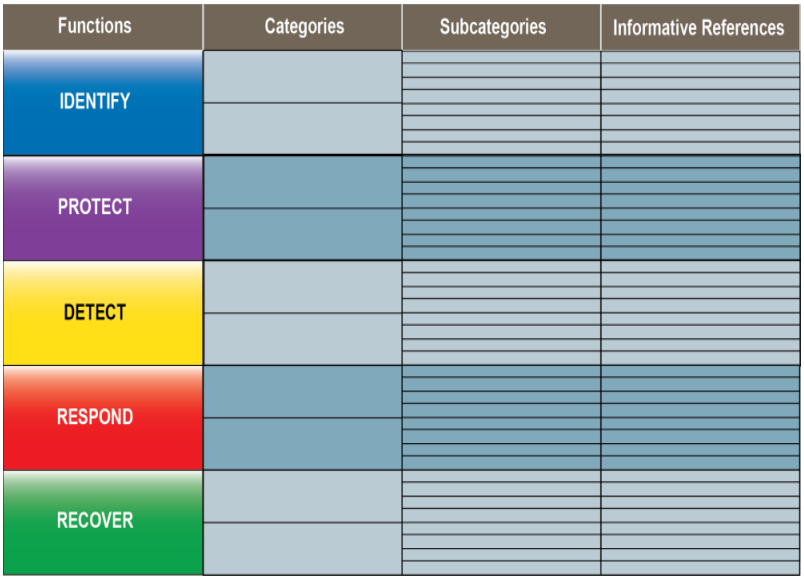
network architecture, network security systems configuration, to assess operating efficiency of technical controls.

2) ICS VA/PT

Our cyber security 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



3) Governance Framework

We can help you in adapting and complying against the NERC CIP requirements and/ or other international and any specific security standards that may be applicable to your environment or develop your own ICS standards and policies based on your risks and needs.

4) Security operations centre (SOC)

It is important to have visibility into our network. In case of an event, a SIEM tool helps you to inspect and analyse the logs to get to the source. A SOC is an essential part of today's security. We can provide services for a setting up your SOC for a combined ICS-IT environment to enable you to monitor and act upon the treats and attacks.

5) Training We can provide customized training to your team.

6) Internal Audit Prior to 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.

CSX™ CYBERSECURITY NEXUS

OUR VALUE DELIVERY

We provide end to end process for NERC CIP Compliance. With Industry 4.0 and use of IoT/ IIoT and Smart Grids as the way forward, the industrial data is moving into the Cloud and increased use of BIG DATA, Security and Privacy concerns are on the rise. We conduct integrated Cyber security engagements with privacy engagements. With more stringent fines being imposed by NERC, cost of compliance is not too high. Our team has more than 7 years of industrial cyber security and IT-OT Convergence experience having worked with major organizations across the world

Some of the advantages of working with us are:

A
- Experienced team in the area of Industrial Cyber Security.
- Project management methodology consistently applied to each engagement

B
- Efficient service delivery with no disruption to operations
- Our engagements are executed by senior experienced professionals

C
- 14 years of Information Security & Cyber Security experience
- Reduced time to complete assignments

D
- Licensed CPA, CISA for Audits & Other Security Professionals to execute projects
- Prompt services with engagements completed in record time

E
- Ongoing support. We are with you whenever you need us
- Our services are competitively priced than BIG names to provide higher ROI

To discuss your specific need please email info@accedere.us