Cyber Security for SCADA and DCS systems
A summary of the current situation and Key points to consider

April 2016

Authors:

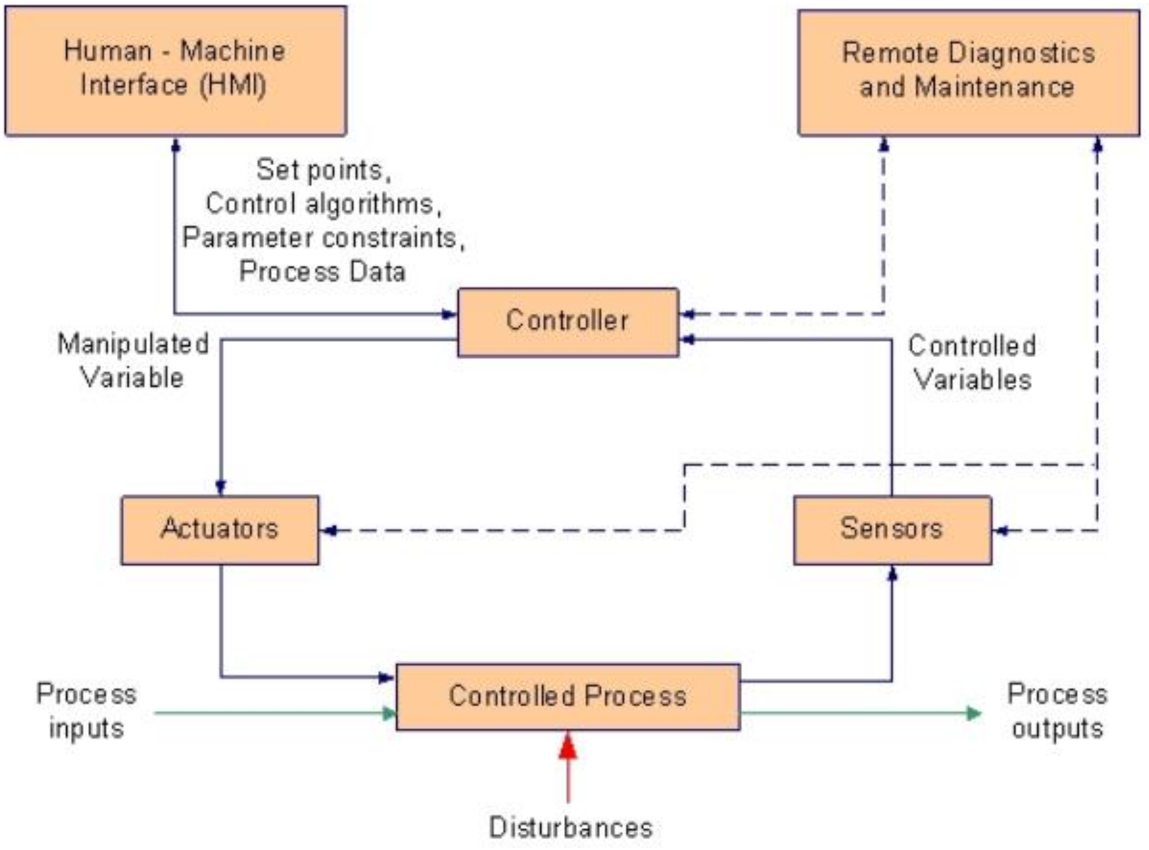
Robert Botezatu ICARE Cyber Security

Glossary

DCS	Distributed Control System
DMZ	Demilitarized Zone
HMI	Human-Machine Interface
ICS	Industrial Control System
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IT	Information Technology
LAN	Local Area Network
MTU	Master Terminal Unit
OS	Operating System
OT	Operations Technology
PDA	Personal Digital Assistant
PLC	Programmable Logic Controller
RFP	Request for Proposal
RFQ	Request for Quotation
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
WAN	Wide Area Network

ICS

“Industrial control system (ICS) is a general term that encompasses 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 skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures”, according to the National Institute of Standards and Technology.


Human - Machine Interface (HMI)
Remote Diagnostics and Maintenance
Set points, Control algorithms, Parameter constraints, Process Data
Controller
Manipulated Variable
Controlled Variables
Actuators
Sensors
Process inputs
Controlled Process
Process outputs
Disturbances

Components of an ICS can be split into two categories: Control and Network.

Control components:

- Control server: hosts the supervisory & control software.
- SCADA Server or MTU: master terminal for all RTUs.
- Remote Terminal Unit (RTU): field devices for data acquisition and control for a specific application, often equipped with wireless capabilities.
- PLC: small industrial computer, used as field devices with more flexibility than RTUs.
- IED: smart sensor/actuator.
- HMI: different software and hardware that allow operators to control and supervise the process. It can be a dedicated platform in a control centre, or just a laptop connected wirelessly.
- Data Historian: centralized database for logging all process information within an ICS.
- IO Server: collecting, buffering and providing access to process information from control sub-components such as PLCs, RTUs and IEDs. It can reside on the control server or on a separate computer.

Network components:

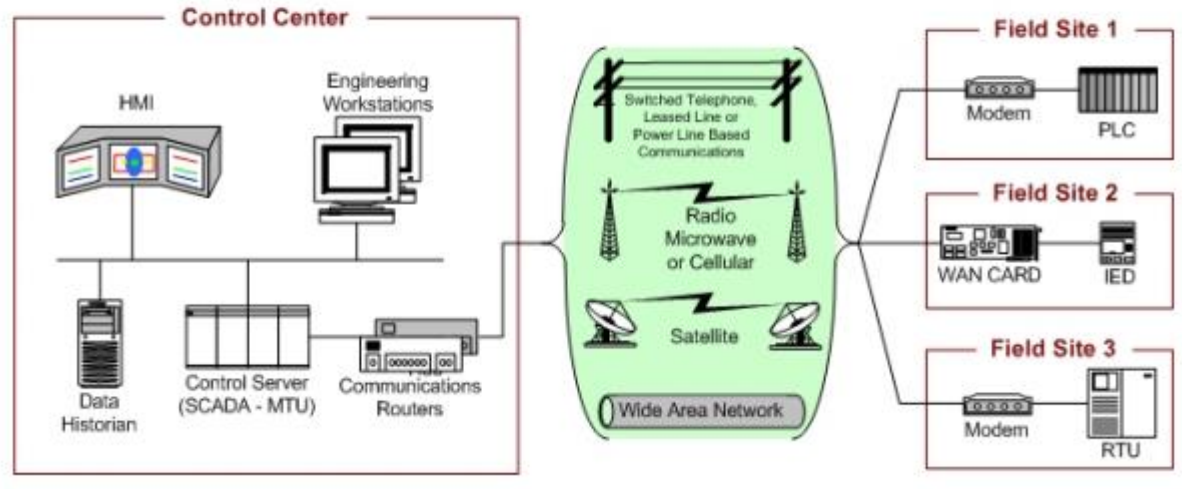
- Fieldbus network: using the fieldbus protocol, it links sensors or other devices to a controller.
- Control Network: links supervisory control elements to lower level control modules.
- Communication Router: transfers messages between two networks (LAN to WAN, or RTUs and MTUs to a long distance communication medium).
- Firewall: device to monitor and control communication with predefined filtering policies.
- Modems: convert between serial digital data and a signal suitable for transmission over a telephone line. They enable long-distance serial communications between MTUs and remote field devices.
- Remote access points: distinct devices, areas and locations of a control network for remotely configuring control systems and accessing process data (with a PDA, laptop, etc.).

SCADA vs DCS

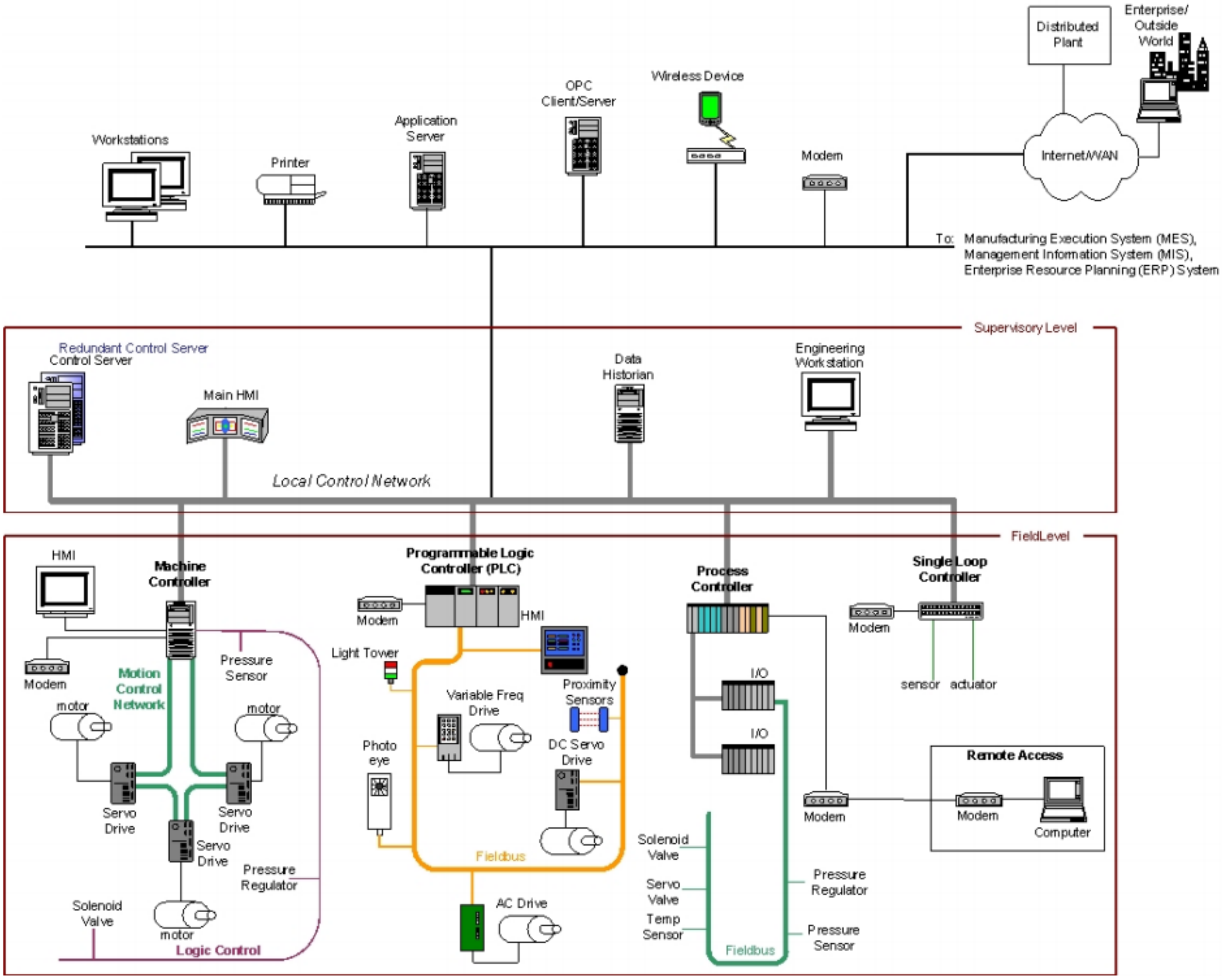
The distinction between SCADA and DCS systems is nowadays diminished, as computers got faster and bandwidth expansion allows even wide area systems to handle large amounts of data. However, most experts in the industry still characterise complex monitoring and control systems that are highly distributed, over a very wide geographic area as SCADA. Plant sized systems, even those with multiple control stations, are characterized as DCS. As an example, large power grids or pipelines fall under SCADA management, while refineries (even large ones), or power plants fall under DCS. When considering the discrete control system for a specific application, PLCs are used.

In short, SCADA represents a wide system of interconnected sensors and controls under central management. DCS represents a local collection of systems that have individual capabilities and require some orchestration.

SCADA basic general arrangement



DCS general arrangement



SCADA and DCS communication protocols

SONET/SDH (optical fibre protocols) are frequently used for large systems such as railways and power stations, but SCADA systems still retain the legacy of low bandwidth protocols. Typical legacy SCADA and DCS protocols include Modbus RTU, RP-570, Profibus and Conitel, which are very compact, send information only when the master station polls the RTU, and are vendor specific.

Standard protocols today are IEC 60870-5-101 or 104, IEC 61850 and DNP3, standardized and recognized by all major SCADA vendors. Open Platform Communications (OPC) is currently used for managing the communication of real-time plant data between control devices from different manufacturers.

Other commonly encountered process automation protocols include:

- HART which has the advantage that it can communicate over legacy wiring;
- Foundation Fieldbus which offers intelligent device management and real-time closed loop control which HART does not do;
- SIEMENS' S7;
- General Electric's Service Request Transport Protocol (GE-SRTP);
- Mitsubishi Electric's MELSEC-Q Series;
- 3S-Smart Software Solutions' CODESYS;

ICS Security Priorities

While most informatics systems follow the Confidentiality, Integrity, and Availability (CIA) priority of security rule, ICSs have the order of priority different, namely Integrity, Availability, Confidentiality, and (sometimes) Accountability (Non-repudiation).

Integrity: generally considered the most critical security requirement for ICS and especially power systems, it refers to checking that the data has not been modified without authorization, is from a valid source and the quality and time stamp of the data are checked.

Availability: depends on the nature of information trafficked, 4ms for protective relaying, subseconds for situational awareness monitoring, seconds for SCADA data, minutes for non-critical equipment, hours for long term meter reads and even days/weeks for long term data (such as power quality reports).

Confidentiality: is now becoming more and more important as corporate information, client data and market information become more available in electronic form.
A major concern for SCADA security is the fact that these systems are not designed with a primary focus on security. Many industrial communication protocols in use today are not encrypted by design. Also, many of the controllers used in these systems have FTP, HTTP or debug online capabilities, which could provide unwanted access points to the network.

ICS vulnerabilities

The total number of detected vulnerabilities has increased 20 fold since 2010, and more than half of these may allow hackers to execute malicious code while over 35% of these already have known exploits. Every component from the ICS has different vulnerabilities depending on the build, protocols used, network structure, etc. But in general, it was found that SCADA systems have twice as many vulnerabilities than HMIs, while the HMIs have more than twice as many as the PLCs. What's more worrying is that all the major manufacturers of automation solutions (Siemens, Schneider Electric, General Electric, ABB, etc.) have been found to have a number of vulnerabilities in their systems, and some of these even have known exploits. Another risk is that after the launch of the search engine Shodan and with the increasing number of sites that share information related to ICSs connected to the internet, the devices are no longer 'hidden', and can be easily found through a passive search by attackers looking for a random target.

A study from 2011 performed by the U.S. Department of Homeland Security (DHS) National Cyber Security Division's Control Systems Security Program (CSSP) identified the most common vulnerabilities for ICSs:

- 42% Improper input validation (the input content provided to an application may grant an attacker access to unintended functionality or privilege escalation)
- 30% Credential verification (attackers may be able to capture usernames and passwords sent across the network in clear text)
- 12% Improper authentication and/or insufficient verification of data authenticity (the software insufficiently proves that an identity claim is correct and/or does not sufficiently verify the origin or authenticity of data)
- 6% Permissions, privileges and access controls (missing or weak access controls can be exploited by attackers to gain unauthorized access to ICS functions)
- 6% Security Configuration and Maintenance (flaws, misconfigurations, or poor maintenance of platforms, including hardware, operating systems, and ICS applications)
- 3% Cryptographic issues (use of unencrypted plain-text network communications protocols)

The DHS-CSSP also recommends ‘as asset owners wait for vendor patches and fixes, the design and implementation of defence-in-depth security strategies that aid in protecting the ICS from attack is part of an effective, proactive security program. Such a program is a necessity because attack strategies are constantly evolving to compensate for increasing defence mechanisms.’
A very large number of ICSs are known to be vulnerable, as previously stated. As you can see in the following table, most systems in developed countries are vulnerable to attacks.

Country	Vulnerable ICS, %
Switzerland	100
Czech Republic	86
Sweden	67
Spain	63
Taiwan	60
United Kingdom	60
Russian Federation	50
Finland	50
Italy	42
United States	41
Poland	36
France	36
Netherlands	33
Austria	33
Korea	32
Canada	25
Germany	20

Network vulnerabilities in ICS

The network infrastructure is often developed considering operational requirements with less concern for security. Over time, modifications to the network can contribute to the introduction of security gaps.

A recurring problem for ICS networks is the lack of logical separation from the corporate network and a well-defined security perimeter. The lack of segmentation of the ICS network and DMZ setup also gives potential attackers the chance to control the entire system if they manage gain access through one entry point. Especially for large architectures such as SCADA systems, the setup of multiple DMZs allow added capability to separate access privileges and functionalities.

Another vulnerability often encountered is the absence of firewalls or having firewalls with improper settings (very often firewalls with the ANY-ANY rule are encountered in industrial networks). This can allow attacks or malware to spread easily between networks. There are also instances where the firewalls were found to be completely bypassed by some remote devices feeding data directly to critical databases.
Many industrial network administrators lack a proper understanding of the architecture and are missing the network diagrams, or they are out of date after a series of modifications. They are also incapable of providing efficient monitoring of the network and don’t have a well setup IDS permanently active.

A vulnerability that is specific to ICS networks is the lack of updates to ICS threat signatures and the avoidance to apply patches. This is because the system being updated is not running during that update, which might cascade to having a whole installation taken offline. This is of course too expensive for most large scale industrial plants, so over 90% of them carry on without an effective informatics security, antivirus, antimalware, etc.

SCADA threats

A study conducted by the Idaho National Laboratory in 2006 showed that for over half of the over 120 confirmed cyber-attacks that the researchers were able to obtain information on, the damages or financial loss was around 1 million USD. 41% of the companies were forced to interrupt production and 29% lost control or the ability to view the plant data.

The major threats today can be split into targeted attacks, such as Aurora, Duqu, Shamoon, and non-targeted (or semi-targeted) attacks, such as Stuxnet, where the malware is released through several points that might spread and gain access to a desired victim. Malware that forces its way through security is not the only way these attacks can be carried out. Very often trick e-mails are used to gain passwords, user names, etc. by posing as messages from legitimate sources and asking for a reply, or the execution of an attachment. Remote control can be gained and used by an attacker outside office hours, and often the goal of the intrusion is to create a new set of credentials so the network can be accessed at any time.

Some of the main threats exposed in the past are still active today, as can be seen in the following.

Vulnerabilities and threats exposed in the past

The Texas City Refinery explosion from 2005 is often used as an example where a combination of human error and safety failures led to one of the worse disasters in the American petroleum industry. This was not the cause of a cyber-attack, but it was all connected to the ICS of the site. It started with an operator inputting the wrong control command, and escalated when a safety system sensor failed and another triggered as a result of an automation scenario unforeseen by the designers of the DCS. All these steps could have been caused and exploited by a hacker wanting to achieve an explosion of the cracking tower, since all the commands that lead to the incident came through software connected to the network.

Another example often cited is when Idaho National Laboratory ran the **Aurora** Generator Test in 2007, to demonstrate how a cyber-attack could destroy physical components of the electric grid. This vulnerability is now referred to as the Aurora Vulnerability and stems from the fact that many pieces of grid equipment use legacy communication protocols that are designed without security.

The Northeast blackout of 2003 was a widespread power outage that occurred throughout parts of the Northeastern and Midwestern United States and the Canadian province of Ontario. This was also not a cyber-attack, but it was caused by a software memory leak in an alarm server which stopped the server from processing alarms for 30 minutes. Some experts believed this to be caused by a **Blaster Worm** attack, but the final official report ruled that out.

In 2003 a worm infected the US CSX Transportation system and caused a shutdown of around 12 hours of all passenger and freight traffic.

The “**Slammer**” Worm disabled the entire computerized safety monitoring system of the Davis-Besse nuclear power plant in Ohio. The worm bypassed the plant’s firewalls because it gained access through an infected laptop owned by a repair contractor.

Probably the most famous threat for ICS is the **Stuxnet** worm. By most experts it is a worm designed to target Iran’s uranium enrichment program by caused the centrifuges to function at self-destructive parameters. It exploited 5 Windows zero day vulnerabilities (it was taking advantage of security holes in Windows that were unknown to Microsoft). It managed to circulate for up to a year before being identified. Unlike the Aurora attack, a Stuxnet attack is not targeted at a specific organization, Stuxnet is designed to attack any ICSs using the Siemens S7 PLCs software that match a certain set-up. It is able to spread through USB and removable media as well, so it can jump any ‘air gaps’. It is even signed with legitimate, stolen RealTek and JMicron software certificates. A related piece of malware thought to be connected to the Stuxnet is the Duqu malware discovered in 2011.

Another major threat became known in 2012, when 30,000 Saudi Aramco workstations were infected by **Shamoo** (Disttrack), local files were uploaded to the attacker, while making the devices unbootable, thus causing the company to spend a week restoring their services. RasGas in Qatar also had its informatics system knocked offline by an unknown virus that some believe to have been Shamoo.

A disgruntled employee has managed to hack into the Maroochy Shire in Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a local hotel. He was an ex-employee of the company that installed the management system.

SCADA and DCS in the electrical industry

“Electric power is often thought to be one of the most prevalent sources of disruptions of interdependent critical infrastructures. As an example, a cascading failure can be initiated by a disruption of the microwave communications network used for an electric power transmission SCADA system. The lack of monitoring and control capabilities could cause a large generating unit to be taken offline, an event that would lead to loss of power at a transmission substation. This loss could cause a major imbalance, triggering a cascading failure across the power grid. This could result in large area blackouts that affect oil and natural gas production, refinery operations, water treatment systems, wastewater collection systems, and pipeline transport systems that rely on the grid for power.” US National Cyber Security Division’s Control Systems Security Program.

Electric utilities are for this reason seen as likely targets for attacks and special steps have been taken to protect them. However, researchers have demonstrated several weaknesses in vendor implementations of communication protocols in a number of products that leave field devices for electrical substations vulnerable, thus providing an access point through which visibility throughout the grid can be knocked out. Even more worrying, some systems were found vulnerable to a complete loss of control, as hackers would’ve been able to access the master terminal through some field equipment.

Initiatives such as smart grids also move intelligence from substations into new areas, where the devices are not as well protected from a physical point of view. These may provide entry points to the whole system, and often are unsupervised, and unfenced, a lock pick away from intrusion.

This is why a holistic multi-layered approach to security, cyber and physical, needs to be implemented to ensure the safety of electrical generation and distribution systems. Any vulnerabilities in the SCADA devices, the software they employ, the network components, physical barriers to access points, human operation protocols, or even Windows and Linux operating systems may be found, exposed and taken advantage of by attackers.

Two approaches

When it comes to dealing with cyber security threats, 2 key approaches can be considered. The retrofit option is essentially targeted at existing environment and can be mainly addressed with a non-invasive approach. For new processes, we highly recommend the Cyber by design approach aimed at taking the right measure right at the design stage.

Checklist for a retrofit approach

1. How are files passed to the critical network? Do you have a file sanitation procedure? If so, is it the same methodology for all file types?
2. Remote access to critical infrastructure or critical devices. Do you have a secure architecture and procedure to fully monitor the supplier/user contacting to the elements in the critical system, processes such as two-way factor authentication or biometrics, encrypted tunnelling, password protection, monitoring and recording, etc.
3. Are your connections between the critical infrastructures to the public network secured via unidirectional gates?
4. Do you monitor and parser SCADA protocols in order to recognize abnormal behaviour of the SCADA system / cyber events?
5. Do you use white list technologies on operating systems and protocols?
6. Do you enforce compliance monitoring and hardening policies on your devices/ work stations/ servers/ network servers/ etc.?
7. Do you implement any network segmentation on the various level of network devices/ protocols / ports?
8. Do you collect logs and events from your critical infrastructure into a central security operation centre?
9. Do you have full network visibility?
10. Have you implemented network access control on your critical network?
11. Do you have a first response team for cyber events? What is their training and what is the entire company's training for cyber events?

Cyber by Design:

The Cyber by Design Methodology was developed to ensure that your operations are secured from Day One. It defines a process that begins from the earliest stage of control and system development, encompassing the design and planning stages as well as the testing, implementation, operation and maintenance phases.

You will require an on-site Security Manager that has an understanding of cyber security.

Step 1: Security Manager Training:

- Threat Vectors
- Defence Tactics
- Information Security

Step 2: Analysis:

- Architecture
- Project goals

Step 3: Implementation:

- Define security requirements into the project architecture
- Insert into the equipment / project RFQ / tenders the information security requirement
- Define the security requirements compliance
- Mapping of the various Services

Step 4: Verification prior to going live:

- Testing Environment: all equipment/ software/ hardware are tested and compared with the special requirements defined
- Penetration testing

A few Key Facts in Summary

1. When it comes to Cyber Security, there is no 100% Guarantee. You have to be trained on detecting and preventing as early as possible.
2. Get your visibility back. If you can’t see what is going on in your networks, you can’t prevent it.
3. The Correlation of IT and OT for Logs and Traffic is one of the key measure to get the right visibility on the activities and behaviours.
4. A lot can be done to secure Industrial Control Systems with None-Intrusive measures.
5. Reduce Suppliers Risk. Embed Cyber requirements in RFQ, RFP’s for critical components.
6. Investment in Cyber usually results in a better availability of the Network. Hardening and Supply chain flexibility is not incompatible.
7. You can’t just solve it with Technology. It’s the People, Process, Technology, Organization that make or break the security of a company.