Industrial Control Systems
Cyber-Security Readiness

Introduction

Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) systems, are utilized in process, manufacturing, transport and several other facilities. These systems centrally supervise and control local and remote industrial equipment such as motors, valves, pumps, relays, etc…

A different approach to risk assessment for process environments is necessary, as these environments tend to be more vulnerable to computing disruption then standard office computing environments. This is due to historical precedence where production systems are changing from the older proprietary, obscure and isolated systems they used to be to the standard, documented and interconnected systems we generally encounter today. In addition, those production systems are generally changed or upgraded after 10 to 15 years of service, compared to more regular 5-year life spans of office computing equipment. These factors allow for a large number of security vulnerabilities to coexist on process systems environments, making them prone to cyber security threats.

The primary concerns governing a process environment is the necessity to maintain component and system integrity and ensure availability. The level of securitization (effort and budget) of these systems will depend on several variables linked to the following topics:

- What is the criticality of the system within the facility?
- What will be the impact should the system not function normally or not be available?
- Do these systems run in a stand-alone environment or are they interconnected in a digital network?
- What is the level of risk posed to these systems from cyber-threats?
- How well are they protected against human error and malware?

We translate the above concerns into 5 measurable categories to better understand the degree of vulnerability and the recoverability of systems should these be disrupted. The categories are:

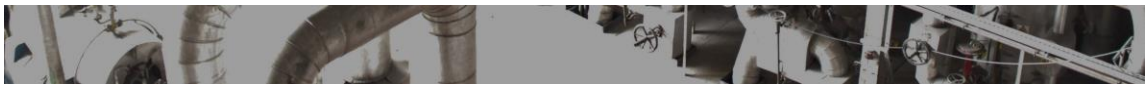
1. **Security Management (Governance):** Application and compliance to best practices
2. **Criticality:** of the process systems and their components
3. **Accessibility:** to computing devices in the process environment
4. **Recoverability:** of computing devices in the process environment
5. **Vulnerability:** of computing components software in the process environment

Potential Vulnerabilities and Threats

Networked systems pose a much greater security threat than standalone systems due to a lack of some basic security principles:

- Individual machines are not always patched (updated to reduce security holes), nor do they always run anti-malware software to block viruses and other such malware;
- The network to which these machines are connected (the process network) is itself usually interconnected to the office network. This means that ICS machines may be easily accessible by anyone from the office network.
- The networks are utilized not only by employees but also contractors, IS vendors and ICS maintenance support organizations. Meaning that all individuals with access to the network may also have, or could gain, access to the process networks.

Interconnected networks are cause for concern as individuals responsible for ICS components may have a false sense of security attributed to the safety of their processing facility. This is a throwback from the days when the only security to be concerned with was physical; as the process environment survived in an isolated environment. This obviously translates into potential lax digital security management and increases the chances of a higher impact to the facility should a cyber-attack occur.



The Approach

Through a series of meetings and interviews (workshops), a large number of details are collected about current computer settings and practices from the Process OT team. The risk assessment is conducted on the principle of the ISO 27001 family of standard for information security management, the ISA99/IEC62443 Industrial Automation and Control Systems Security, as well as other relevant security standards for industrial controls systems. The details are then consolidated into the five categories to facilitate a structured approach to identifying and measuring security risks.

1. ***Digital systems inventory***
   This is the important first stage that identifies all critical systems and their components. This does not only include ICS applications (such as SCADA) but network components, safety systems, security systems and critical information sources. Collecting relevant cyber security elements are an important factor in inventory information collection.

2. ***System criticality Definition***
   This category covers the criticality of the system by identifying related attributes to the functionality of the system (financial loss, penalties, equipment damage, environmental damage or human casualties). This should be closely linked to risk measurements from the risk department.

3. ***Recoverability of critical computing systems***
   This category investigates the ability to maintain business continuity in case of computing incidents and disruptions. We look at the tested (proof) ability to recover from system failures, how regularly back-ups are taken, how backup software is stored and managed and whether obsolete systems components are kept in inventory for critical systems.

4. ***Accessibility to critical computing devices***
   This category reviews the current physical and logical (via networks and wireless means) accessibility given to computing devices. The concept here is clear, the less accessible a system the better its inherent strength from attacks.

5. ***Vulnerabilities of critical computing device software***
   This category identifies the types of software vulnerabilities (such as lack of virus protection or weak passwords) of computers and network devices in the process environment. This category generally requires that components be patched, hardened, upgraded, and scanned for viruses but that they also pose no threat from external devices connected to them or remote connections.

Following the initial meetings and the first risk assessment measures have been structured, we then begin to focus on clearly identified vulnerabilities. This will include interviews and sample testing to discover vulnerabilities of individual components. These additional technical reviews and tests will provide a control procedure to verify against the collected information from the interviews.

The Practical side

The method follows a typical risk assessment approach (based on industry norms ISA/IEC 63442 and ISO 27001) and delivers a security maturity level (based on COBIT maturity levels) in 5 measurable categories:

1. ***System criticality***: Defining critical digital systems and components

2. ***System Security management***: Applying best procedural practices to security

3. ***System Recoverability***: Ensuring the ability to recover systems or components from failures and/or incidents

4. ***System Accessibility***: Limiting general access, both logical and physical, to digital systems

5. ***System/component hardware and software vulnerabilities:*** Mitigating known software and hardware vulnerabilities within the allowance of contractual agreements and limitations of systems

Figure I – Rapid digital risk assessment approach

Document review

This is a task that should be performed first. Depending on the documentation handed over, and its quality, this is strong indication of their OT security stance.

Workshops

The workshop approach consists of a 4 hour session involving key responsible persons who determine the criticality of their systems, security approach to maintenance and support, recovery capability in case of an incident. We also delve into network connectivity, physical security and vulnerabilities.

Technical Investigations

The technical security check consists of different steps, either performed individually or simultaneously. This will include anything from penetration testing, devices scanning or location walkthrough; needless to say that the approach utilized is depended on the industrial activities, the risk involved and customer comfort. However, a sample of digital components are investigated on their security vulnerabilities.

Examples of industrial control systems risk measurements

***Chart* 1 – System Cyber Security maturity**

This chart links system criticality level to cyber maturity. This demonstrates potential cyber readiness weaknesses and allows of focused compensations measures based on "what-if" scenarios.

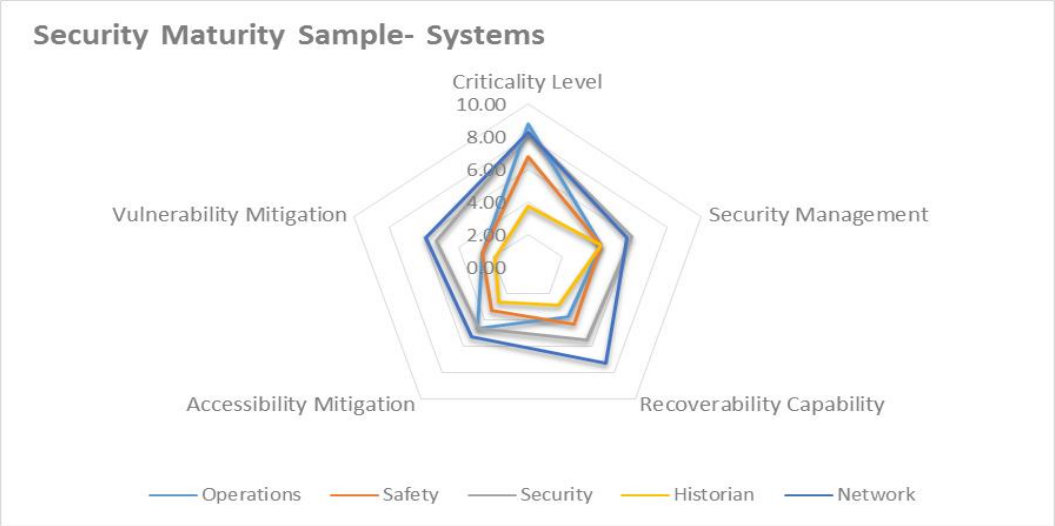


***Chart* 2 - Recoverability GAP**

This chart indicates the degree of separation between the ***expected*** recoverability of a system (usually by those responsible for operations) versus the ***estimated*** recoverability by those responsible for support and maintenance of the systems (usually system engineers).

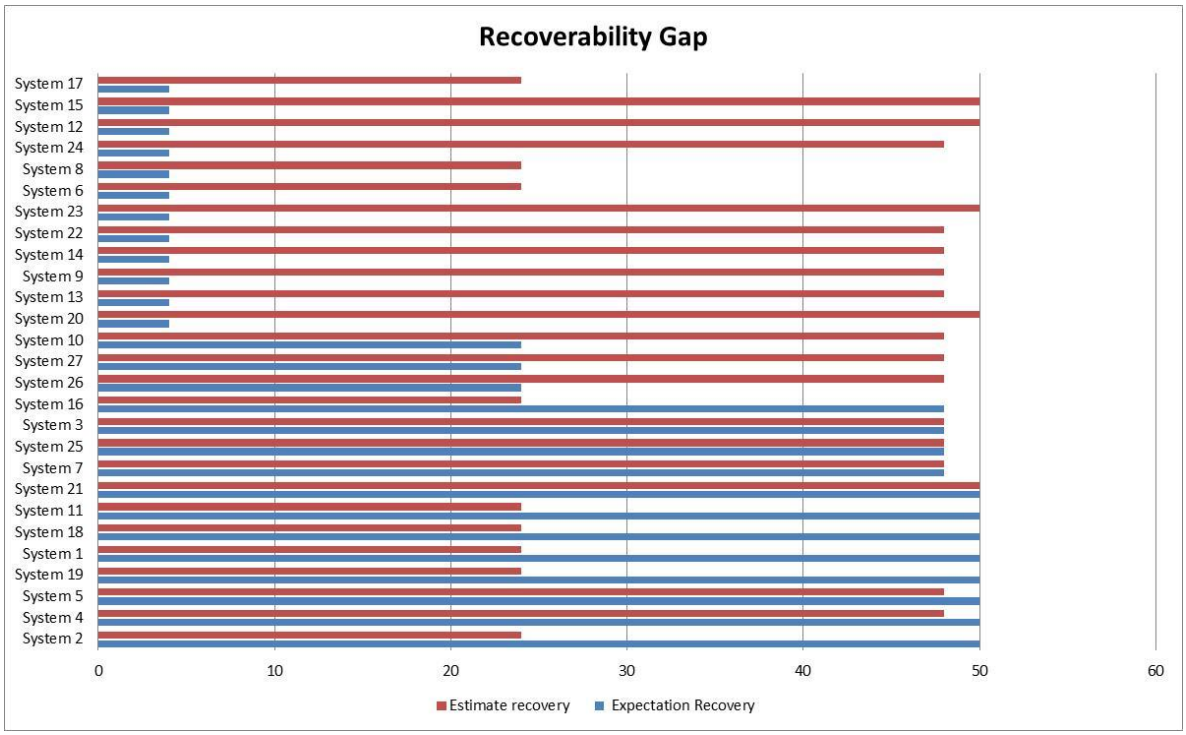


***Chart 3* - System Risk Quadrant**

This quadrant provides a view on high risk systems.