«Smart» SCADA Security

Analisi delle vulnerabilità

Antonio Conte
Manager
Deloitte ERS - Enterprise Risk Services

Deloitte.

Trends in information security

The world is becoming increasingly connected. **New technologies** are constantly introduced, devices and people are getting **more connected**, therefore the use of networking technology becomes more intense. organizations depend increasingly on IT solutions. With the rising use of new technology and connectivity, also cybercrime increases significantly.

Trends in industrial control systems (ICS)

Industrial control systems were designed and initially deployed in isolated networks, running on proprietary protocols with custom software. The exposure of these control systems to cyber threats was therefore limited. During the past years we witnessed new business needs which triggered office information technology and operational technology **integration** and use of **Internet enabled communication**. In addition, the use of **off-the-shelve** software and hardware became a standard practice for ICS owners, increasing the exposure surface.

The trends we observe imply that the risks to the availability of industrial systems grow significantly, while the security measures are often lacking.

ICS security is a challenge

The trends in industrial systems imply a necessity to include security into operations. Embedding security in operational technology is often a challenging task. Systems and networks used in industrial systems have different requirements than systems and networks from the office domain.

Updating **anti-virus, patching** or changing configuration files on systems in OT-environments is a challenge. Engineers need to guarantee safety, availability and reliability at all times and asset owners are reluctant to make changes to operational environments.
Similarly, **network segregation and remote access** are a challenge.

History proves that even air-gaped systems, isolated from the outside world, can fall victim to cyber attacks due to use of **USB or portable media**.

Reasons used to exclude security in ICS

The industrial control system is isolated
Often employees and external parties bring portable media and computers into facilities. There are many examples where these devices were infected and caused damage or operational loss.

Security is the responsibility of the integrator
Often ICS security is not covered in the SLAs with the system integrators. Even when covered, these contracts rarely include statements for keeping the security up-to-date.

Our organization is not a likely target
Besides intentional attacks, unintentional attacks pose a high risk factor. There are numerous examples where employees unintentionally introduce malware in ICS network.

Common Threats in ICS

Reducing the risk from a specific threat requires a combination of **technical solutions**, **formalized processes** and **people** with the right expertise.

Portable-Media

Portable media, such as a USB device, needs to be scanned for malicious code before it enters the facility.

Networks-Segmentation

Businesses require real-time information sharing between the operational and the office domain. There are ICS specific solutions that can enable secure connections between networks by using firewalls and enable specific connections to be established.

Remote-Access

Suppliers and integrators often require remote access to the operational network to monitor the performance of the equipment and remotely adjust operational parameters. There are ICS specific solutions that are agentless and enable remote access to engineering stations via a central server in the operational domain.

Patching

Before applying a security patch or an anti-virus update, the change needs to be approved by the vendor before installation in the production environment. There are ICS specific solutions allowing operators to remotely make these changes.

Security Trends | Challenges in securing ICS | ICS Security Needs | Future of ICS security

Preventive Security is not Sufficient anymore:

- Assume you will be hacked
- Monitoring and detection capabilities are increasingly important
- Incident response and crisis management capabilities are required to follow-up on malicious events
- Updates and new systems need to be implemented and operated safe and secure from day 1

Future of securing industrial systems

Going forward, automation will play an increasing important role in society. The industrial control systems are becoming more intelligent and more autonomous. These systems are now becoming part of the networked society.

Future developments will bring us more potential tools to guard ourselves against adversaries, at the same time the attack side will also develop and equip itself.

On the **Attack side** we will see

- Tools and knowledge are more widely available;
- More integration of open protocols and standard software and hardware;
- More internet facing industrial assets;
- Industrial systems are an increasing target of attack because of their direct physical connection (cyber warfare, terrorism);

On the **Defense** side we will see

- Education of professionals, combining knowledge of engineering and security;
- Industry initiatives and knowledge sharing;
- Best practices & standards development;
- Increasing budget for security;
- Embedding security by design in new industrial assets;

Security Trends | Challenges in securing ICS | ICS Security Needs | Future of ICS security

Reactive and Proactive Security

The four boxes on the right illustrate the minimum set of capabilities required to effective manage ICS security.

Preventive controls offer the organization a solid security basis and are the first step an asset owner should take.

Focus is on increasing the readiness and resilience of the IT equipment.

Developing monitoring and response capabilities enables the organization to address an essential aspect of security – **operational agility** - thereby being ready and resilient when an attack occurs.

1

Security by Design

- Design and review of Security Architecture
- Secure Procurement & Sourcing
- Secure Software Development
- Security Testing

2

Preventive Controls

- Security Strategy and Governance
- Security Awareness
- Policies & Standards
- Identity & Access Management
- Physical Security
- High Privileged Security

3

Monitoring Capabilities

- Risk Assessments
- Threat analysis
- SIEM/SOC advisory
- Compliance Monitoring
- 3rd Party Monitoring
- Periodic Security Testing
- Vulnerability Assessment

4

Security Response

- Incident Response readiness
- Continuity Management
- Disaster Recovery
- Crisis Management
- Cyber Forensics