Deloitte.

Securing Industrial Control Systems

Secure. Vigilant. Resilient.

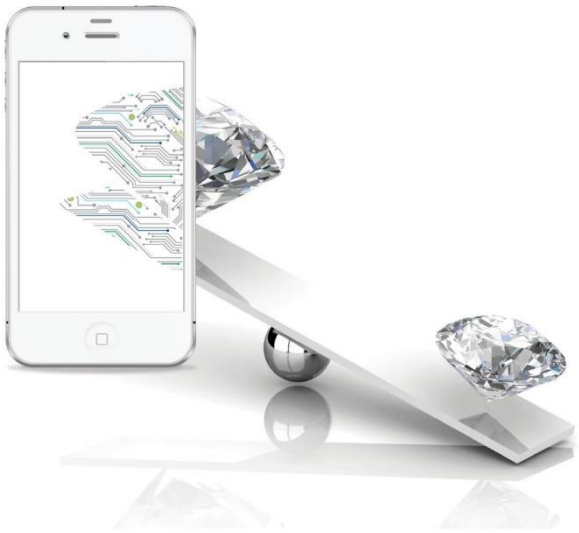
May 2015

Cyber Security

Securing industrial control systems: Don’t be a victim of cyber-attacks

Cyber security

Just as the workplace is becoming distributed across traditional business, social and domestic locations, so too are automation systems. There is an increasing trend in building automation and remote supervision and control of traditional machinery and the home and equipment contained therein, as well as in the medical field. Much of this equipment tends to be connected to the internet to enable convenient and possibly highly efficient access and use. However, this high degree of connectivity, together with the lack of security measures, is where the exposure originates from.



The vision of Securing Industrial Control Systems is portable to securing “Connected Devices/Technology” also referred to as the “Internet of Things”. The International Telecommunications Union predicts that the number of connected devices will reach 25 billion by 2020, up from 10 billion in 2011.

Security trends

Security-related controversies in society increase in parallel with the increase of the use and abuse of hacker tools.

Trends in information security

The world is becoming increasingly connected. New technologies are constantly introduced; devices and people are becoming more connected; networking technology has become more standardised, converged and pervasive; and organisations have come to depend increasingly on IT solutions. With the rising use of new technology and connectivity, cybercrime also increases significantly. Cybercrime ranges from agents who attack systems for espionage purposes, to teenagers who attack systems for fun. The increase of security-related controversies in society grows in parallel with the use and abuse of hacker tools.

Trends in industrial control systems

Industrial control systems (ICSs) were designed to control industrial automation processes (i.e. operational technology) and were initially deployed in isolated networks, running on proprietary protocols with custom software. The exposure of these control systems to cyber threats was therefore limited to connected corporate IT solutions and direct physical access. Over the years, we witnessed new business needs which triggered office information technology and operational technology (OT) interaction, integration and use of internet-enabled communication.

In addition, the use of off-the-shelf software and hardware has become a standard practice for ICS owners, increasing the exposure surface. The coexistence of legacy and new equipment (accompanied by the *OT/IT technology convergence and integration and the use of off-the-shelf software) creates vulnerable setups that can be abused by attackers.

*** The multitude of commodity and proprietary computers and software, their sensors, actuators, controllers, distributed wired and wireless networks, human-machine interfaces, IT interfaces and development systems that communicate with and control the automated production processes and machinery in production, manufacturing and processing plants, in pipelines, logistics, warehousing, transportation, ships, motorised vehicles and aeroplanes and increasingly buildings and cities**

Challenges in securing ICS

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

ICS security is a challenge.

The security vulnerability and compromise trends in industrial systems imply the necessity to include security into operations. Embedding security in operational technology is often a challenging task. Systems and networks used in industrial automation have requirements different from the systems and networks used in office automation. These systems are designed to remain in production for much longer than office systems and are sometimes still not designed with security in mind.

Electronic and physical access to critical cyber assets is not managed. Updating anti-virus software or solutions, 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 or to spend the money on cyber security. Similarly, network segregation and remote access are a challenge.

Networks should be segregated based on, for example:

- The business purpose
- Business intelligence requirements
- End-to-end supply and demand process management
- Integration with ERP systems
- Integration to 3rd Party systems through various inter-communication protocols
- Internet access requirements

This often requires downtime of operations, and providing remote access to third parties exposes the production plant to new risks. History proves that even air-gapped systems (isolated from the outside world) can fall victim to cyber-attacks due to the use of USB or portable storage media.

Eventually, an intentional or unintentional violation of cyber security will occur. Does your organisation have preventative measures in place? Will your organisation anticipate the violation or even detect it. Will you be able to analyse the incident and respond? Will it affect the industrial control systems? Will your organisation be able to identify it in an early stage and respond in good time?

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 for legitimate purposes. However, there are many examples where these devices were infected and caused damage or operational loss.

Firewalls separate the IT and OT networks.

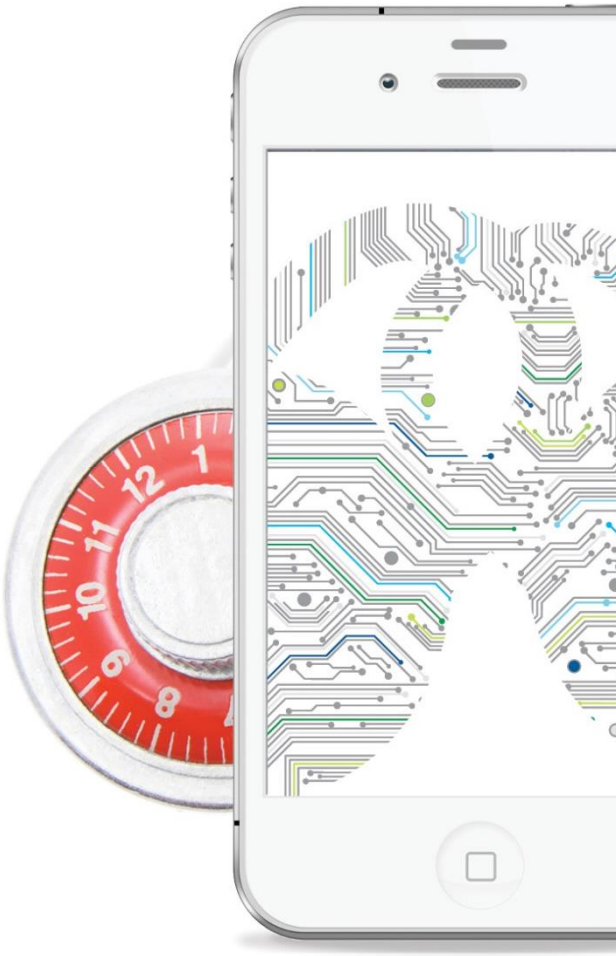
Firewall configurations are often too permissive, because flexibility and access to external parties are deemed critical business requirements. For example, support of the OT environment by Original Equipment Manufacturers (OEM's) and System Integrators (SI's).

Security is seen as the responsibility of the integrator.

Often, ICS security is not covered in the SLAs and contracts with the system integrators and various OEM vendors. Even when covered, these contracts rarely include statements for keeping security mechanisms up to date.

Our organisation 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.



The Deloitte point of view

Safety, availability, reliability... and security

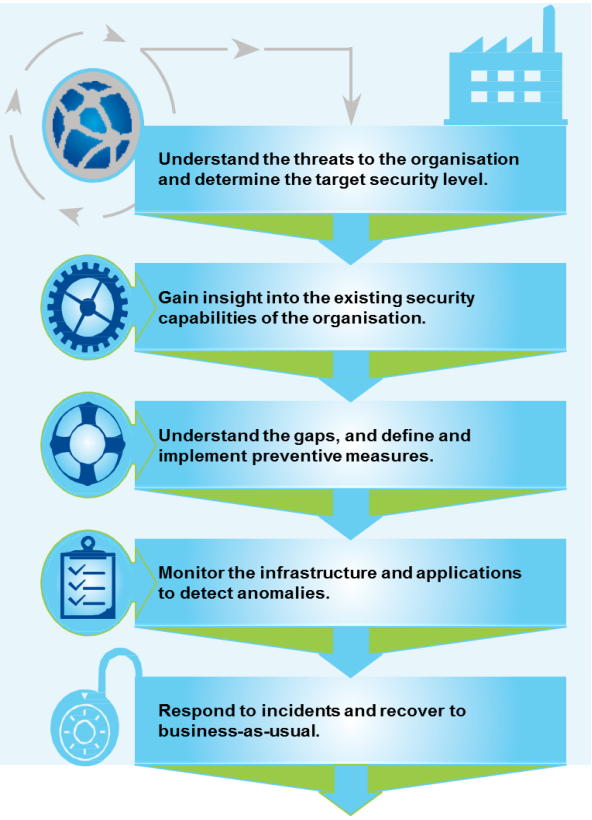
In extreme cases, cyber security affects safety. More often, lack of security affects the operations of the site, leading to financial or reputational loss, injuries, loss of life, environmental contamination and/or regulatory sanctions (or fines).

Industrial systems are expensive and are – from an IT security relative perspective – often inherently insecure. Should you be worried about security? Moreover, which measures should your organisation implement?

Organisations are aware of cyber threats but are confident that their organisation will not be a target of an attack. Depending on the industrial sector, in combination with the products produced, specific threats are applicable. The applicable threats influence the required level of security for the organisation. For example, a nuclear power facility has a more complex threat landscape and requires a higher security level than a water purification plant. Understanding the threats and gaining insight into the security capabilities of your organisation ensure an effective and cost-efficient way of securing your organisation.

Deloitte notices that industrial asset owners do not focus on security of their OT equipment, which often implies that there is room for improvement in basic security measures. Implementation of several common security measures makes industrial assets significantly more secure, thus reducing the likelihood of a cyber-incident.

Adequate security must be a process of continual improvement and not a once-off exercise. There is no so-called "silver bullet" for protection of critical cyber assets.



Preventative 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 and tie in with IT cyber security capabilities.
- Updates and new systems need to be implemented and operated safely and securely from day one.

Security portfolio: The basic to-do's

Reactive and proactive security

The increasing integration of computers in society means an increasing demand for security services. Both proactive and reactive security measures are needed. The four boxes on the right enumerate the range of security services offered by Deloitte.

The organisation should focus on increasing the security readiness and resilience of the IT type equipment in the OT environment. Preventative controls offer the organisation a solid security basis and are the first step an asset owner should take. Multi-layer security, or defence in depth, best embodies how security should be addressed.

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

Organisations cannot protect what they do not know about. It is vital for an organisation to establish and maintain a comprehensive inventory of its OT cyber assets.

Common threats in ICS

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

Technical solutions in the operational domain need to work in harsh environmental conditions. Processes need to be adjusted so they match the facility's requirements and need to be usable for the people onsite.

Portable media, such as a USB storage device, need to be scanned for malicious code before it enters the facility. There are ICS specific solutions that provide whitelisting of data on portable media. These solutions require an engineer to scan the USB storage device on a mounted scanner station

before entering the facility. The best recommended practise is for all USB ports or storage devices to be disabled, especially on all data critical Servers.

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 Human-machine Interfaces (HMIs) and engineering workstations via a central server in the operational domain.

Networks segmentation

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

Patching

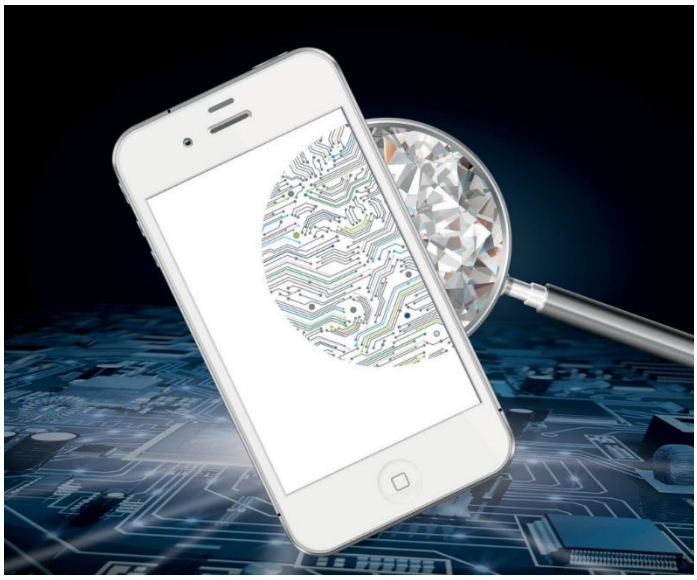
Before applying a security patch or an anti-virus update, the change must be approved by the vendor (OEM and/or SI) before installation in the production environment. There are ICS-specific solutions that are able to push metadata on approved patches and updates. When combined with remote access, operators can remotely make these changes.

The future of ICS security

Future of securing industrial systems

In the future, automation will play an increasingly important role in society.

The industrial control systems are becoming more intelligent and more autonomous. These systems, but also other control systems such as building automation, car systems and medical devices that were once disconnected from networks, 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.



For example

Engineers want to optimise the processes in their plant at any time from any location. Hence we currently have the proliferation of Human-machine Interfaces (HMIs) and Industrial PC's (iPC) on tablets and smartphones.

On the attack side, we will see:

- Tools and knowledge that are more widely available
- More integration of open protocols and standard software and hardware
- More internet-facing industrial assets
- Industrial systems are increasingly a target of attack because of their direct relationship to the economic and socio-political viability of geographic regions economy (cyber warfare, terrorism, *hacktivism, etc.)

On the defence side, we will see:

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

Industrial control systems are becoming more intelligent and more autonomous.

Contacts

South Africa	Africa
Dave Kennedy *Managing Director, Risk Advisory* *Deloitte Africa* Tel : +27 11 806 5340 Email: dkennedy@deloitte.co.za	**Graham Dawes** *Rest of Africa Leader: Risk Advisory* Tel: +254 71 989 2209 Email: gdawes@deloitte.co.za
Cathy Gibson *Africa Leader: Risk Advisory Cyber Risk & Resilience (Johannesburg)* Tel: +27 11 806 5386 Email: cgibson@deloitte.co.za	**Julie Akinyi Nyangaya** *Director: Risk Advisory (East Africa)* *Tel: +254 20 423 0234* Email: jnyangaye@deloitte.co.ke
Danita de Swardt *Director: Risk Advisory (Johannesburg)* Tel: +27 11 806 5208 Email: ddeswardt@deloitte.co.za	**Tricha Simon** *Director: Risk Advisory (Central Africa)* *Tel: +263 4 74 6248* Email: tsimon@deloitte.co.zw
Tiaan van Schalkwyk *Senior Manager: Risk Advisory (Johannesburg)* Tel: +27 11 806 5167 Email: tvanschalkwyk@deloitte.co.za	**Anthony Olukoju** *Director: Risk Advisory, (West Africa)* Tel: +234 805 209 0501 Email: aolukoju@deloitte.com
Reyaaz Jacobs *Director: Risk Advisory (KwaZulu-Natal)* Tel: +27 31 560 7165 Email: rejacobs@deloitte.co.za	**Joe Ohemeng** *Director: Risk Advisory (Ghana)* Tel: +23 33 0277 4169 Email: johemeng@deloitte.com