Deloitte.

Secure Vigilant Resilient

Cyber Security and Resilience Services

Secure. Vigilant. Resilient

Cyber Security

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

Internet of things

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

The use and abuse of hacker tools grows in parallel with the increase of security related controversies in society.

Trends in information security

The world is becoming increasingly connected. New technologies are constantly introduced, devices and people are getting more connected, networking technology has become more intense 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 that attack systems for espionage purposes, to teenagers that attack systems for fun. The use and abuse of hacker tools grows in parallel with the increase of security related controversies in society.

Trends in industrial control systems

Industrial control systems (ICS) 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 coexistence of legacy and new equipment, accompanied by the IT/OT integration and the use of off-the-shelf software, create vulnerable setups that can be abused by attackers.

Challenges in security ICS

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 the 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. Segregating a network often requires downtime of operations and providing remote access to third parties exposes the plant to new risks. History proves that even airgaped systems, isolated from the outside world, can fall victim to cyber attacks due to use of USB or portable media.

Sooner or later an intentional or unintentional attack will occur. Does your organisation have preventive measures in place? Will it impact the control systems? Will your organisation be able to identify it in an early stage?

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.

Firewalls separate the IT and OT networks
Firewall configurations are often too permissive, because flexibility and access to external parties are critical business requirements.

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 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.

Understanding the threats and gaining insight into the security capabilities of your organisation ensures an effective and cost-efficient way of securing your organisation.

Deloitte's point of view

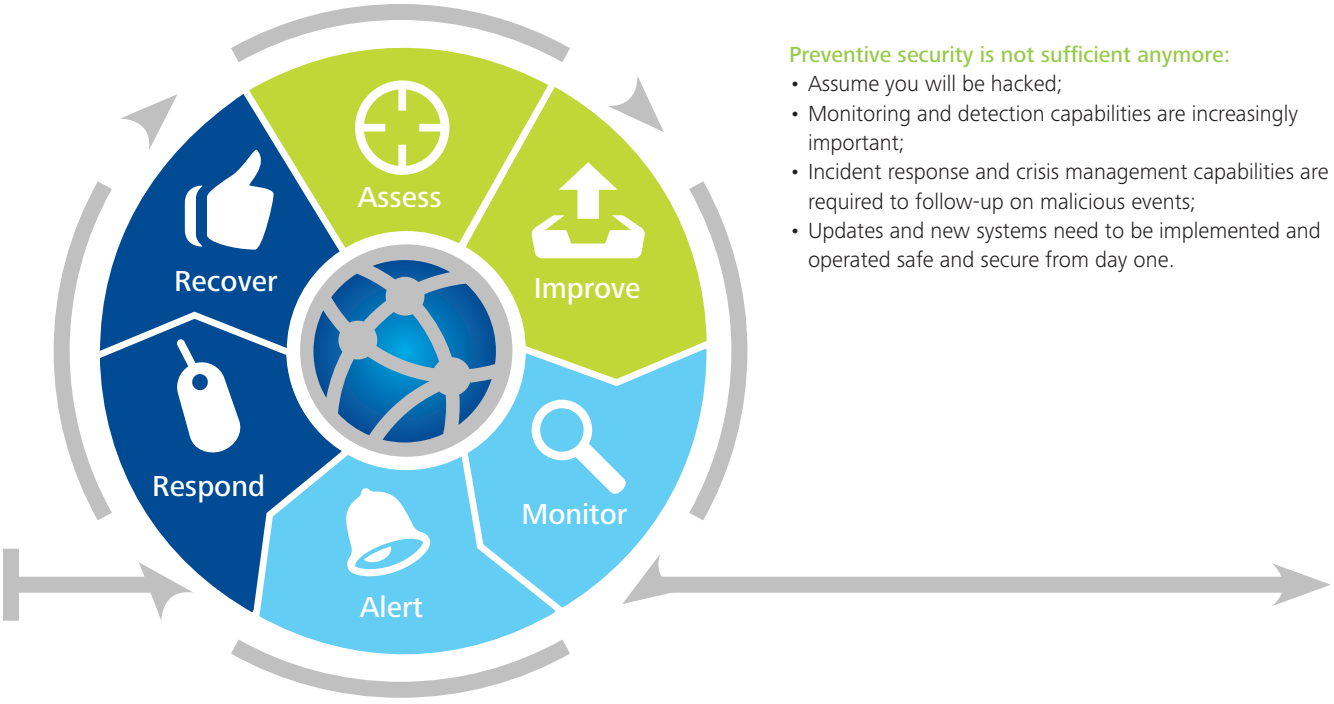
Safety, availability, reliability ... and security

In extreme cases, security impacts safety. More often, lack of security impacts the operations of the site, leading to financial or reputational loss.

Industrial systems are expensive and are – from an IT perspective – inherently insecure. Should you be worried about security and 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 facility has a 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 ensures an effective and cost-efficient way of securing your organisation.

Deloitte notices that industrial asset owners do not focus on security, 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 making the likelihood of a cyber incident lower.



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 one.

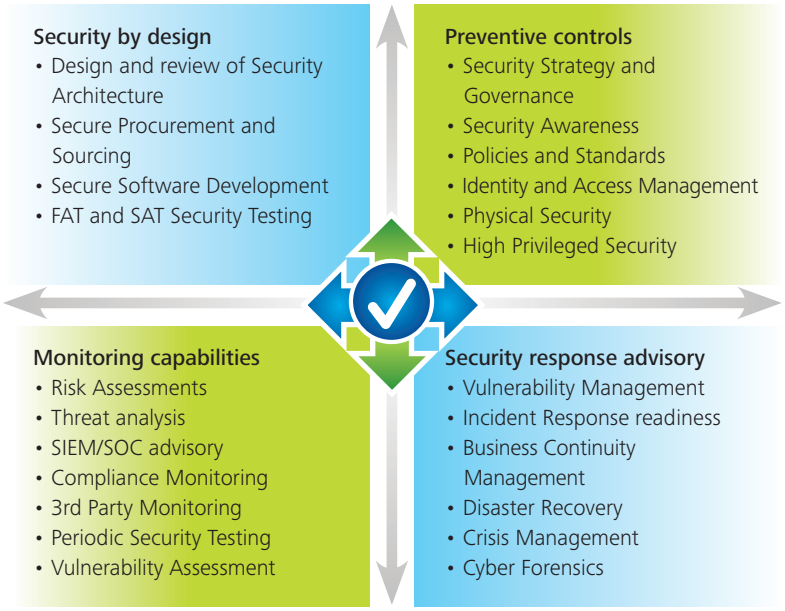
Security portfolio: the basic to-do's

Reactive and proactive security

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

The organisation should focus on increasing the readiness and resilience of the IT equipment. Preventive controls offer the organisation a solid security basis and are the first step an asset owner should take. Multi-layer security, or defense in depth, best states 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.



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 requirements and need to be usable for the people onsite.

Portable media

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

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 HMIs and engineering stations via a central server in the operational domain.

Security training

We host an intensive hands-on 3-day ICS (SCADA) Security Training covering ICS architecture, ICS vulnerabilities, Securing ICS and hands-on hacking of an ICS environment.

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 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 needs to be approved by the vendor before installation in the production environment. There are ICS specific solutions able to push metadata on approved patches and updates. When combined with remote access, operators can remotely make these changes.

ICS Security Assessment

A multi-day engagement in which we test and review the security of the ICS environment, covering network segementation, rogue devices and governance.

The future of ICS security

The industrial control systems are becoming more intelligent and more autonomous.

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, 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 would like to optimise the processes in their plant at any time from any location. In the future we should expect the profiliation of HMIs on tablets and smartphones.

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 and standards development;
- Increasing budget for security;
- Embedding security by design in new industrial assets

Contact

Dave Kennedy
Managing Director, Risk Advisory
Deloitte Africa
Tel: +27 11 806 5340
Email: dkennedy@deloitte.co.za

South Africa

Cathy Gibson
Leader: Cyber Risk & Resilience, Risk Advisory
(Johannesburg)
Tel: +27 11 806 5386
Email: cgibson@deloitte.co.za

Danita de Swardt
Director: Cyber Risk & Resilience, Risk Advisory
(Johannesburg)
Tel: +27 11 806 5208
Email: ddeswardt@deloitte.co.za

Karthi Pillay
Director, Risk Advisory
(Johannesburg)
Deloitte South Africa
Tel: +27 11 806 5173
Email: kpillay@deloitte.co.za

Michele Townsend
Director, Risk Advisory
(Johannesburg)
Deloitte South Africa
Tel: +2711 806 5992
Email: mntownsend@deloitte.co.za

Braam Pretorius
Associate Director: Cyber Risk & Resilience,
Risk Advisory
(Johannesburg)
Tel: +27 11 806 5429
Email: brpretorius@deloitte.co.za

Henry Peens
Senior Manager: Cyber Risk & Resilience,
Risk Advisory
Tel: +27 11 806 5625
Email: hpeens@deloitte.co.za

Paul Orffer
Senior Manager: Cyber Risk & Resilience,
Risk Advisory
(Johannesburg)
Tel: +27 11 806 5567
Email: porffer@deloitte.co.za

Tiaan van Schalkwyk
Senior Manager, Cyber Risk & Resilience,
Risk Advisory
(Johannesburg)
Deloitte South Africa
Tel: +27 11 806 5167
Email: tvanschalkwyk@deloitte.co.za

Reyaaz Jacobs
Director: Risk Advisory
(KwaZulu-Natal)
Tel: +27 31 560 7165
Email: rejacobs@deloitte.co.za

Etienne Ward
Director, Risk Advisory
(Cape Town)
Deloitte South Africa
Tel: +27 21 427 5683
Email: etward@deloitte.co.za

Africa

Jens Kock
Partner, Risk Advisory
(Namibia)
Deloitte Namibia
Tel: +264 61 285 5003
Email: jkock@deloitte.co.za

Julie Akinyi Nyangaya
Partner, Risk Advisory,
(East Africa)
Deloitte Kenya
Tel: +254 20 423 0234
Email: jnyangaye@deloitte.co.ke

Tricha Simon
Partner, Risk Advisory,
(Central Africa)
Deloitte Zimbabwe
Tel: +263 4 74 6248
Email: tsimon@deloitte.co.zw

Anthony Olukoju
Partner, Risk Advisory,
(West Africa)
Deloitte Nigeria
Tel: +234 805 209 0501
Email: aolukoju@deloitte.com

Joe Ohemeng
Partner, Risk Advisory
(Ghana)
Deloitte Ghana
Tel: +23 33 0277 4169
Email: johemeng@deloitte.com

Graham Dawes
Director: RA leader:
Rest of Africa
Tel: +254(0)719892209
Email: gdawes@deloitte.co.za

Designed and produced by Creative Services at Deloitte, Johannesburg. 808163/REV/jo)