Cyber Security of Industrial Control Systems

March 2015

Eric Luiijf and Bert Jan te Paske


GCCS 2015
The Netherlands

Preface

Our society and its citizens depend on the undisturbed functioning of (critical) infrastructures and their services. Crucial processes in most critical infrastructures, and in many other organisations, rely on the correct and undisturbed functioning of Industrial Control Systems (ICS). A failure of ICS may both cause critical services to fail and may result in safety risk to people and or the environment. Therefore, the cyber security and resilience of ICS is of utmost importance to society as a whole, to utilities and other critical infrastructure operators, and to organisations which use ICS.
This document first and foremost, provides private and public sector executives with an Executive Summary outlining the ICS risk and challenges. We appeal to the executive leadership of organisations to address the clear and present cyber security danger to their organisations and our societies as a whole.

Underpinning the Executive Summary, this document provides governmental policy-makers, technical managers, ICS suppliers and others involved in the ICS domain with background and security awareness information about the cyber security challenges for ICS. Moreover, this document provides you with a perspective for action and pointers to relevant resources.

On behalf of the authors,

Eric Luiijf


GCCS 2015
The Netherlands

Executive Summary

Industrial Control Systems, or ICS, monitor and control physical processes. ICS control our critical infrastructures, safety-critical processes and most production processes. ICS are now everywhere around us, often hiding in everyday functionality, as illustrated by the insert "Good Morning with ICS" on page 10.

The term ICS[1] may evoke images of industrial plants with noisy machinery and a control room with operators checking gauges and reacting to alarm signals. While perhaps a romantic memory of twentieth-century industry, it has little to do with how ICS are applied today. Gradually, and without most of you really noticing it, ICS transformed from proprietary hardware and software solutions into commercial off-the-shelf (COTS) computers and operating systems. Moreover, ICS connect to public networks including the Internet. Hand in hand with those changes the ICS cyber security challenges insidiously sneaked into organisations whilst not being recognised and understood.

Organisations have gratefully accepted the business benefits of these technology shifts: centralised operations with less operators, 24 by 7 remote support and maintenance for complex production systems, increased flexibility and process adaptability, integration with corporate IT, and other cost reductions, for instance due to the use of COTS computers and software. What many organisations have failed to appreciate are the adverse effects of these advancements, in particular those related to the cyber security of ICS, which constitute the cost side of the business case. ICS that were designed for closed proprietary and benign environments have over time become open, networked and publicly connected. Both the ICS and the physical

[1] Neglecting minor terminological and technical differences, synonyms for ICS include SCADA, DCS, and IACS that are part of the Operational Technology (OT) or Process Automation (PA) domain.

processes they control, have thus become more susceptible to malware, hacking and deliberate network disruptions (see section 3.1 “Myths about ICS Cyber Security”). ICS-controlled critical infrastructure may be disrupted or physically damaged, resulting in an impact on people’s safety, the economy, the environment, and the social cohesion (e.g. in case of a long duration disrupted utility). Other types of business may suffer from interrupted or damaged ICS-controlled production capabilities, with serious impact on their business continuity. Those responsible for ICS need to properly address the cyber security risk of their ICS, as only then the merits of today’s technological advances can be safely exploited.

Whilst ICS are in many ways becoming standard IT, ICS do have some distinguishing features that, unfortunately, tend to impede the implementation of security controls:

1. First, ICS are typically used to control critical processes. Key priorities are the 24 by 7 continuity and the ability for operations to view and control the processes. ICS-triggered disruption of the production or critical functions, may affect the organisation’s profit and reputation. This causes a strong reluctance to apply any system changes that could harm the continuity of the production and its performance. Security controls common in regular IT, including regular patching and antivirus updates, therefore pose a risk to the monitored and controlled production processes. Executive management should enforce the implementation of suitable security controls based on risk assessments, and not tolerate cyber security being sacrificed to the ‘do not touch it’ attitude.
2. Secondly, ICS and (office) IT have historically been managed by separate organisational units. ICS people do not consider their ICS to be IT. ICS are just monitoring and control functions integrated into the process being operated. ICS people lack cyber security education. The IT department, on the other hand, is unfamiliar with the peculiarities and limitations of ICS technology. They do not regard the control of processes to have any relationship with IT. Only few people

have the knowledge and experience to bridge both domains and define an integrated security approach. Organisations that have brought the personnel from these two diverse domains together, have successfully bridged the gap and improved the mutual understanding of both their IT and ICS domains. Their security posture has risen considerably.

3. A final characteristic of ICS is their long lifespan. Whereas regular IT is renewed every few years, ICS tend to stay in place for decades. One reason is the high cost involved in migration, especially when ICS are deployed at many geographically dispersed field sites. As ICS components have asynchronous lifecycles, a coherent security approach can only be gradually implemented. Most ICS environments and their cyber security therefore have to cope with legacy. In practice, the opportunity for a coherent cyber security approach is often missed when decisions about security requirements for new ICS components are made autonomously in projects and constrained by project budgets. This is why executive management should request an ICS cyber security masterplan as a framework for security requirements when individual ICS components are replaced.

Executives need to understand and balance the cyber security risk related to the use of ICS with other business risk factors. The ICS cyber security risk is not theoretical. Although ICS security incidents are often kept under the radar, serious incidents do happen. Some examples can be found in section 3.5; executives of other organisations may inform you in confidence about the incidents they experienced.

The Board needs to understand that the cyber risk to ICS is not an IT-issue to be managed deep down in their organisation. It is a risk affecting the continuity and reputation of the business. Cyber security of ICS should be part of long-term strategy, human resources plans, business processes, procurement and many other domains. The potential risk impact to the business and/or society requires a systematic risk

approach integrated in the organisation's risk management framework and managed at Executive level. As a guiding principle, the residual risk should be kept at a minimum within realistic boundaries ('as low as reasonably practicable' or ALARP).
Therefore, this document provides you and your organisation with perspectives for action to manage the ICS risk. Section 1.4 provides, per type of responsibility, a quick access to the key topics. A first step to assess the maturity of one's organisation in controlling the cyber security risk to ICS, may be to consider the two sets of questions below: one set for the CEO and one set for the CISO.

However, fighting the cyber security risk of ICS on your own is a losing battle. Other board rooms currently face the same risks and challenges; these are often organisations involved in the same business chains. Joining forces as an organisation with peers and or government agencies, for instance by sharing cyber security-related information on ICS, is a way of showing leadership. In most industries, cyber resilience is considered a common interest and not part of the competitive arena. Moreover, executive management is well advised to benchmark the cyber security of their ICS against that of their peers, if only to learn where an extra effort could or should be made (e.g. see section 5.2).

As a CEO, you should ask the following questions[2] to your Board about the cyber security of your ICS:

- How are you informed about the cyber security risk and the potential business impact to the primary processes in your area of responsibility?
- Do you know the current cyber security risk level and potential business impact?

[2] These questions were partially derived from [27].

- Does your risk appetite follows the ALARP principle and do you meet current regulations, industry standards and good practices?
- Do you have a governance structure and incident response structure in place in which accountabilities and responsibilities for ICS security are clearly stated and accepted by each of you?
- Is your workforce well aware of the cyber threats to ICS and are they appropriately trained?

The following questions should be asked to the Chief Information Security Officer (CISO):

- What strategies have been put in place to identify and manage the cyber security risk of ICS?
- How do you measure your cyber security maturity and compliance levels?
- Have you selected an effective set of controls that will reduce the risk to ICS to ALARP?
- How comprehensive is your ICS incident response plan? How often is it tested?
- How many and what types of cyber security incidents in your ICS occur per reporting period? What is the threshold for notifying your executive leadership about a cyber security incident?
- How well do your IT and process automation/production departments communicate and collaborate on cyber security?

Good Morning with ICS

What ICS controlled functions did you use this morning before you arrived at your desk? None? Then, we ask you to re-trace your steps.

Your alarm clock awoke you. You turned on the bedside light. The required extra Watts were generated, transported and distributed under ICS control. While you took a shower, ICS adjusted the drinking water production process and maintained the pressure in the pipelines to your home. Heating of your home and cooking breakfast required the production, transport and distribution of gas. All these processes are controlled by ICS. The cup of milk you used required automatic milking, strict temperature control of the intermediate storage tanks, and processing and packaging at the milk factory, all under ICS control. You either took the train (ICS-controlled signalling, points, power and traction), or road transport (ICS-controlled traffic lights, safety systems in tunnels and traffic control of lanes). Arriving at the office, you passed the ICS-operated barrier to the parking lot and the ICS-controlled security barrier or doors to enter the premises. The air conditioning, fire protection and evacuation systems of your organisation are all operated by ICS 24/7, as well as the elevator you took to your office at the top floor. The (critical) large coffee/tea/chocolate/soup machine has embedded ICS and is connected to the Internet …

You may have noticed that we deliberately skipped at least twenty other ICS operated functions your organisation and you have encountered and used this morning. Can you name them? Surprised by how ICS embed and hide themselves in functionality that is taken for granted?

But who is taking care of the cyber security and resilience of such critical functions? Or are these ICS managed in an unconsciously insecure way?

Contents

1 Introduction

In these good practices we will use the term Industrial Control Systems (ICS)[3] to denote the class of Information and Communication Technology (ICT [4]) which measure, monitor and control physical processes. Our society and its citizens depend on the undisturbed functioning of ICS-controlled infrastructures and their services. Nations have identified infrastructures and services which are critical, which means that the failure of such an infrastructure or service may seriously impact the health and well-being of citizens, the economy, the environment, and the functioning of the government ([4], [49]).

1.1 Examples of critical ICS

Examples of critical infrastructures are energy, transport, and drinking water. Crucial processes of most critical infrastructures and of many organisations rely on the correct and undisturbed functioning of ICS. For example, ICS form the heart of production processes in refineries, the chemical industry, the food and drug industries, and baggage processing at airports.

A failure of ICS may cause service disruptions and/or a safety risk to people and the environment. For example, environmental catastrophes may occur due to failing or cyberattacked ICS losing control over hazardous materials, causing leakage or toxic emissions. At the same time, the set of threats to ICS has widened and hostile actors look for ways to attack ICS, as section 0 outlines. Therefore, the cyber security and resilience of ICS is of utmost importance to society as a whole, to utilities and other critical infrastructure operators, and to organisations and industries using ICS.

[3] Other frequently used terms for ICS, apart from slight differences in connotation, are Distributed Control Systems (DCS), Industrial Automation Control Systems (IACS), Process Control Systems (PCS), and Supervisory Control and Data Acquisition (SCADA).

[4] In the remainder of this document we will use the more commonly used abbreviation IT instead of ICT; both notions are interchangeable in the context of this document.

1.2 The Audience

The intended audience of these Cyber Security Good Practices for ICS includes private and public sector executives and governmental policy-makers responsible for critical (and other) infrastructures and their services. In addition, this document aims at the broad spectrum of ICS manufacturers, suppliers, system integrators, cyber resilience researchers, and last but not least, at the middle management of organisations who apply and use ICS in their crucial business processes.

1.3 Purposes of this Guide

This guide aims to answer the following questions:

1. Which are the ICS cyber security-related challenges?
   The Executive Summary provides an executive level insight in the cyber security risk of ICS and the (business) need for action.
2. What is my responsibility?
   Chapter 2 discusses the need for Executive and Tactical Leadership to address the cyber security challenges of ICS.
3. What should I do?
   The remaining chapters and the set of references and resources include a more detailed discussion of the risk (chapter 3) and provide you with good practices for dealing with aspects of ICS cyber security (chapters 5 and 6) while identifying organisational challenges and common pitfalls (chapter 4).

1.4 How to use this Guide?

You can read this guide from start to end. Another way is to use the table on the next page, which provides pointers to the chapters considered of particular interest to each stakeholder.

	CEO	Board Members	CISO	IT manager	ICS manager	HR department	Procurement dpt	Policy maker	Manufacturer / Supplier / System integrator	Research
Executive summary	X	X	X	o	o	o	o	o	o	o
Introduction			X	X	X	o	o	o	o	o
Start in the Board Room		X	X	X	X	o	o	o	o	
What is your risk challenge			X	X	X		o	X		
Organisational challenges			X	X	X			o		
Moving forward towards cyber resilience			X	o	o	X			o	o
Be strong together			o	o	o		X	o	X	o
The next steps			o	o	o			o	o	

X= required reading; o = suggested reading

2 Start in the Board Room

Cyber security in general, and cyber security of ICS in particular, is not an IT-problem but a board room issue, as the executive summary explains. The executive level manages the risk to the business objectives of the organisation and protects the public and private shareholder interests ([7], [8], [31], [35]). The undisturbed functioning of critical processes supported by ICS forms a crucial element for the business: cyber threats to ICS may have grave impact on society, the business and reputation of the organisation, and the safety of people and the environment. Therefore, organisations need to address the cyber security of ICS with full support by the executive level. Increasingly, stakeholders and shareholders request that organisations be transparent with regard to the number of serious cyber incidents, data protection breaches, and the overall cyber risk [52].

2.1 Governance challenges

ICS and their related cyber security challenges may hide themselves in everyday functionality, as illustrated by the insert “Good Morning with ICS” on page 10. Such functionality is often managed at the tactical and operational levels by Operational Technology (OT) groups or process-specific department(s). Most of the time, that department has no or only limited understanding of cyber security [50]. The responsibility for cyber security often lies with the IT department, which fails to understand the embedded IT in ICS. At the OT working level there is a certain amount of push-back due to the concern about how cyber security measures may impact on operations safety and efficiency, when not implementing those measures may have a greater potential for impacting safety. As result, the organisation may fail to manage the cyber security risk to ICS properly.

Stimulated by the World Economic Forum (WEF; [7], [8]), the issue of cyber security and resilience is gaining weight in board rooms. ICS is part of that discussion; its proper governance may be even more crucial as ICS monitor and control critical continuity, security, and safety related processes of organisations. Using the motto ‘leading by doing’, the WEF recognises four cyber security principles: recognition of dependencies, role of leadership, integrated risk management, and promotion of uptake. We address those four principles below.

2.2 Recognition of Dependencies

Critical infrastructure services are increasingly intertwined and dependent upon each other. Many of their critical processes rely on the undisturbed functioning of ICS. Services to citizens, small and medium enterprises, organisations and society as a whole are most often provided through a chain of cooperating organisations. Leadership recognises its own business dependency on other organisations. Moreover, cyber security weaknesses, and therefore system instabilities, often occur at the interfaces between organisations, for instance, due to the lack of sharing cyber security-related information. At the operational/technological level, organisations use the same ICS technologies with the same vulnerabilities and face the same threats and threat actors as other organisations in their own sector and other sectors. Do not forget that the strength of one's own ICS security is only as strong as the weakest link in the ICS ecosystem.

2.3 Leadership

2.3.1 Organisational leadership

The Executive Summary discussed the need to manage the ICS risk at board level and to show leadership. This requirement is replicated at the CISO, IT, ICS and human resources management levels. Be aware that the gap between executive and operational/technical levels is huge. Moreover, the technical understanding and jargon of the ICS domain do not easily translate into the key performance indicators and the risk to the business. Cyber security related terminology makes communication between board level and middle management layers even more challenging. Here is an example: "The production had to be shut down as RTU-25 controlling motor 2 in unit 19-52 has been infected by the HAML-virus which entered the ICS via a USB drive". The expected reporting sought to be: "The production has been shut down due to a cyberattack. Restarting the production will take 12 hours. Twenty main clients are affected. Estimated production loss will be 15,000 units. A smoke cloud was visible due to the shut down; expect questions from the financial press." Proactive operating leadership will recognise this gap and initiate actions to reduce this gap, for instance through the coaching of the 'linking pins' between the technical/operational and business (risk) level, and through regular exercises.

Fighting the cyber risk of ICS on your own is a losing battle. Joining forces as an organisation with peers and or government agencies, for instance sharing cyber security-related information on ICS, is a way of showing leadership. The 'Good Practices on Information Sharing' may help organisations to overcome barriers and start sharing cyber security-related information with peers [45].

2.3.2 National leadership and policy-makers

Nations recognise the importance of national critical infrastructures [49]. As explained above, most critical infrastructures rely on ICS for monitoring and controlling their critical processes. Understanding the risk of cyber security and ICS, a number of nations have started to pay attention to this topic in various ways:

- Creating a national cyber security strategy (NCSS) that shows that the cyber security of ICS is high on the national agenda. Moreover, the NCSS should include ICS-security specific actions. For example, the state of Qatar pledges preferential treatment for security certified CII equipment in national projects. The certified equipment (see section 6.5) reflects an improved assurance level by demonstrating that security has been an element of the design [33]. The USA has created a policy framework for improving the cyber security of its critical infrastructure; ICS security is an element of this framework [19].
- Providing free management workshops for executives and ICS security training for plant operators (e.g. Qatar).
- Providing good practice information on the cyber security of ICS, e.g. [2], [18], [21], [22], [24], [26], [34], [36], [37], [38] and [51].
- Providing a self-assessment tool, e.g. [28] and [36], or free on-site security assessments for critical infrastructures.
- Support for Information Sharing and Analysis Centres and other forms of Information Exchanges, e.g. [42], [39], and [30] (Meridian membership only).
- Creating awareness by performing (inter)national exercises which include cyberattacks against critical infrastructure ICS.
- Providing a guide for cyber security training in ICS environments [22].
- Providing guidance to manufacturers and system integrators [25].
- Providing Common Criteria protection profiles for ICS [23].
- Initiating research and development programs addressing the security of ICS.

Moreover, some countries have either issued, or are planning, critical information infrastructure related legislation that mandates baseline security and resilience obligations for critical infrastructure operators and/or obligatory reporting of security breaches. Note that [45] discusses some pros and cons of mandatory reporting.

2.3.3 Leadership by manufacturers, system integrators and maintenance organisations

Manufacturers, system integrators and maintenance organisations can shoulder their responsibility and show leadership by providing secure ICS and ICS services:

- Create secure ICS products.
- Provide security-related documentation for the specific end-user groups.

- By default, include a security chapter (or option) in each ICS-related proposal, even when the requestor has forgotten to insert the topic in its request for quotation. In other words: educate the customer.
- When providing ICS to an end-user organisation, educate the end-user about all security aspects of the delivered ICS, e.g. make sure standard passwords are replaced by proper passwords before handing over the responsibility for the system.
- Educate all your installation and maintenance personnel about ICS cyber security; even better, have certified engineers on board (see section 5.3).

2.4 Risk Management

The WEF recognises that effective management of the cyber risk requires a structural effort by organisations, starting at the board room or C-level. Organisations should embed practices to assess, monitor and mitigate the cyber risk to ICS in their corporate risk management structure. This approach should be organised around the identification of information assets in general, and ICS in particular, that are of value to the organisation and its business processes. The responsibility for each of these assets, and the cyber risk pertaining to them, must be allocated to an undisputed asset or business process owner. The responsible asset owners and business managers can then be involved in periodic risk assessments and efforts to mitigate the risk to an accepted level.

Special attention should be paid to suppliers, system integrators, contractors and other third parties involved in ICS during all of the life-cycle phases. Management must appreciate that ICS, like most other IT, are increasingly heterogeneous, complex infrastructures often crossing organisational boundaries both on the technical, the process and business levels. Clear understanding of these interfaces and the dependencies and obligations towards external parties is a key prerequisite for effective management of the cyber risk. Section 0 provides good practices for managing these interfaces and dependencies.

2.5 Promote Uptake

As discussed above, the ICS monitored and controlled production or services are part of a dependency chain. The fourth WEF principle states that organisations should encourage their suppliers and other organisations which are part of their ICS eco-system, to adopt the same WEF principles. This means that the executive level needs to take a lead in the collaborative protection of the (ICS-controlled) service chain(s) by engaging the executive level of suppliers and other organisations one depends on. Highlighting one's expectations of the

other organisation and recognising that cyber security of (ICS-controlled) services is a collaborative task, is a first stage of the dialogue. Empower middle management to work out the operational details.

Nations may promote uptake by launching national stimulus programs for the cyber security of ICS by:

- pledging government funding and investments in critical information infrastructure protection (CIIP) related industries,
- taking the initiative to start Information Exchanges (see sections 6.1 and 6.2 as well as [45]) and keep the information sharing fly-wheel in motion,
- offering incentives to CII operators in the form of government subsidised technical and executive training,
- offering free cyber security evaluation services.

3 The Cyber Risk Profile of ICS

To effectively manage cyber security risk in ICS, one needs a good understanding of what ICS are and of the environment in which they are operated. In both respects, a lot has changed over the past decades. However, those responsible for corporate risk management of organisations are often not aware of these changes, and of how they affect the cyber risk profile of ICS. As important as it is to appreciate new trends and developments, ICS also have inherent characteristics that set them apart from regular IT. Practice has shown that cyber risk to ICS is not a theoretical matter. Incidents do happen and one should learn the lessons identified by others.

3.1 Myths about ICS Cyber Security

ICS were traditionally designed around reliability and safety. Until recently, cyber security was not a design consideration for ICS because:

- ICS were based on proprietary code and standards.
- Knowledge about ICS was limited to a small set of experts; nobody else was interested.
- ICS operated in a completely disconnected environment.
- ICS operated in a benign environment. Protocols and protocol implementations were therefore simple and not hardened against attacks.
- Hackers were not interested in ICS.

All these design assumptions have subsequently been proved to have been flawed:

- ICS applications increasingly operate on top of commercial off-the-shelf (COTS) hardware, operating systems and internet protocol stacks.
- ICS applications move to open source environments.
- The knowledge about ICS is widely distributed; descriptions and manuals on most ICS applications and protocols can be found openly on the internet.
- ICS networks are directly and indirectly connected to public networks such as the internet. ICS may even be controlled on a tablet from a home location.
- ICS have fallen victim to disgruntled insiders (see paragraph 3.5 on incidents).

- Hackers are very interested in breaking ICS. In the last years, many presentations at Hacker Conventions such as Black Hat have been about ICS insecurity. Hacker and test toolsets incorporate vulnerability scans for ICS, e.g. MetaSploit.

The next paragraphs explore how ICS differ from common IT, and how the aforementioned developments may be addressed from a cyber security perspective.

3.2 ICS versus (office) IT: Different Concerns

There are major differences between the normal (office) IT and the ICS domains when it comes to the cyber security requirements that the systems are expected to meet. 'Office' IT often prioritises confidentiality over availability and integrity. For ICS, the focus is usually on the availability, visibility, operability, and integrity of the ICS-controlled processes, the process efficiency, and safety. Cyber security, including the confidentiality aspect, is a lesser concern. This results in a different security focus where the sensible choice is not to implement security controls which could harm system availability and performance.

It is not unusual to take (office) IT services down for a restart to install security-related software mitigations and configuration changes during a maintenance window or even lunch break. The external threat dynamics force the (office) IT department to be vigilant. Within the ICS domain, the 24 by 7 process continuity requirements often preclude such 'ad hoc' security activities.

3.3 Trends and Threats in ICS Technology

3.3.1 ICS technology

One key difference between ICS and (office) IT is the technical and economic lifespan. The periods typically used for 'writing-off' ICS are very long when compared to the periods in which organisations 'write off' (office) IT. ICS components therefore remain in use for a long time, especially when compared to the fast technological development and replacement rate of regular IT. Typical ICS therefore have an installed base of aging technology, the so-called legacy ICS, which often includes supplier-specific applications and hardware, and decades-old communication protocols and hardware.

Old ICS protocols and applications may contain vulnerabilities, since they were designed for a benign environment without any security threat, as explained in paragraph 3.1. Meanwhile, newer ICS components based on COTS technology have their own vulnerabilities, knowledge of which is widespread. With today's

business pressure to connect ICS with the outside world, the risk of these vulnerabilities being exploited becomes more severe.

Whereas (office) IT uses strict policies for updates and patching, this is not at all common in ICS. Software updates may impact the system stability and availability. Often, ICS have no representative testing environment to determine the effects of an update or patch before implementing it.

Table 1: Comparison of characteristic differences between ICS and (office) IT

	ICS	(Office) IT
Security priority	Availability, Process visibility, Process operability, Integrity, Confidentiality	Confidentiality, Integrity, Availability
Availability of provided services	24 by 7 by 365 days/year	Restarted when needed
Latency	Real-time requirements	Varying response times are accepted
Software robustness	Expect benign environment; protocols fail when challenged	Implementations under continuous hacker scrutiny; weaknesses removed
Anti-malware	Uncommon; insufficient resources in legacy ICS	Standard
Patching	Requires OK from ICS manufacturers, testing; deployment hard in a 24/7 environment [6]	Almost immediate when available (e.g. 'Patch Tuesday')
Passwords	Hard wired in legacy ICS; never changed group passwords	Regularly changed
Default accounts	Often unchanged	Removed / changed
Physical security	Varying	High for server and network
Security awareness	Varying	Continuous attention
Depreciation	10 to 25 years	3 to 5 years

Summarising, it is becoming increasingly apparent that ICS protocols and implementations are lagging ten years or three 'generations' behind the security learning curve of 'office' IT. A risk to manage.

3.3.2 The ICS environment

The ICS environment is becoming increasingly open. Market developments sometimes require that data from ICS is provided to business departments within the organisation, or to third parties via public communication

networks. From an operational perspective, it is often convenient to implement remote access facilities. This allows system operators to react to ICS alarms from home, while system integrators and third party maintenance engineers may remotely access ICS for monitoring equipment status, implementing system changes and performing remote maintenance.
Organisations should be aware of the cyber threats and risk factors to ICS introduced by external employees and their activities. A good practice is to contractually oblige third parties providing ICS related services to adhere to the organisation's own cyber security policies.
ICS designers, ICS suppliers, and system integrators are more focused on the development of new features than on the development of systems that are inherently more secure. A lack of harmonised client demand and regulatory requirements for cyber security amplify the lack of focus on 'cyber securing' ICS products. Only recently, the need for cyber security of ICS has become more prominent.
The crux of the matter is that ICS security challenges can only be tackled jointly by the government (as user, first customer, legislator for critical sectors, and supervisor), ICS users, manufacturers, system integrators, suppliers, as well as by knowledge, educational and research institutes. The market drives new features in ICS equipment, and until the market begins demanding security features, they will continue to be low priority for manufacturers/vendors of ICS equipment.

3.4 Threat Actors

In terms of threats and threat actors, an increasing interest in, and knowledge about, ICS can be observed in hacker communities and during hacker conventions such as Black Hat and DEF CON®. At the same time, recently revealed cyber espionage and other hostile activities, probably by states and state-related actors, show a strong preference for gaining access to ICS of critical infrastructures. External links between ICS networks and the outside world, combined with the poor resistance of ICS protocols to incorrect communication packets, substantially increase the possibility of hostile activity achieving ICS failure. Moreover, ICS are susceptible to malware. This can be used in a targeted campaign but may also end up in the ICS unintentionally, through another infected system or device. In either case, the resulting damage and impact upon organisations and society due to failing ICS-controlled processes can be significant.

This threat is not theoretical. Cyber security incidents happen in ICS environments. For many reasons, such cyber security incidents are not often reported as ICS security incidents but as 'technical failure'. Public reporting of security breaches in ICS is only required in a limited number of nations, and mostly in specific sectors.

3.5 Cyber Security Incidents in ICS Environments do happen

Below, a selected set of examples of ICS failures show that cyber security incidents and malicious attacks against ICS do happen. Moreover, some examples show the potential impact of ICS disruptions. We have omitted the well-documented and well-known Maroochy Water Services [54] and Stuxnet [55] cases.

Malware

- Trend Micro identified 13 varieties of banking malware disguised as legitimate industrial control systems (ICS) software updates from Siemens, GE, and Advantech, and originating as spear phishing attempts or drive-by download attacks [56].
- Recently, a crew member on a ship at the North Sea checked his email and clicked on a malicious link. The imported malware spread via the ship's network, froze all ICS and locked down the entire ship.
- ICS-CERT alerted ICS users about a sophisticated malware campaign that has compromised numerous ICS environments using a variant of the BlackEnergy malware. Analysis indicates that this campaign has been ongoing since at least 2011. Multiple companies working with ICS-CERT have identified the malware on Internet-connected human-machine interfaces (HMIs) [57].
- An earlier 2014 ICS-CERT advisory discusses the Havex malware payload which enumerates Open Platform Communication (OPC) connectivity. Multiple common OPC platforms have crashed intermittently resulting in a denial of service of applications which interact with ICS and manufacturing automation [58].
- In April 2013, oil plants and an oil exporting terminal on Kharg Island, Iran, were affected by a virus in the ICS. The Kharg Island facilities process 80 percent of Iran's crude oil. Components were taken off-line [59].
- In 2010, a specialised Conficker version targeted the ICS systems of the Dutch milk processing company Royal Friesland Campina. This resulted in a nine hours production loss [60].
- In 2005, the ICS at a number of oil and gas platforms in the North Sea were affected by the Zotob.E worm. Cleaning took a very long time as personnel needed to hop from platform to platform to disinfect the systems.
- In 2003, the Slammer worm penetrated the ICS network of First Energy's Davis-Besse nuclear power plant in Ohio. It disabled a safety monitoring system for nearly five hours [61].

Malicious Acts

- On an undisclosed date in 2014, a cyberattack took place on the ICS of a German iron producing plant. The ICS breakdown caused substantial physical damage to the production plant [62].
- In October 2014, a disgruntled employee sabotaged the ICS of a waste water processing facility in the USA causing a spill of untreated waste water [63].

- In April 2009, Jesse William McGraw (also known with his hacker names 'GhostExodus' and 'PhantomExodizzmo') committed computer intrusions into several computers in the W.B. Carrell Memorial Clinic hospital building, including ICS controlling the heating, ventilation and air conditioning (HVAC) system [64]. He was sentenced by the federal court to 110 months in jail and had to pay $31,881.75 in restitution to the hospital groups affected by his attacks.
- From 2006 to 2008, the leak detections systems on three Pacific Energy Resources oil derricks offshore from Huntington Beach, South California, were remotely turned off by Mario Azar, a disgruntled employee. He had two unauthorised backdoor accesses to the ICS [65].
- Early January 2008, a 14 year old youth used a remote control device based on a TV remote control to manipulate tramway switches in Lodz, Poland. As a result, four tram vehicles were derailed and twelve people were injured [66].
- In October 2006, a hacker penetrated the ICS of a water filtering plant near Harrisburg Pennsylvania using a backdoor in a laptop of an employee [67].

Technical Risk

- Careless 'ping' sweeps' performed for security testing or network inventory purposes, frequently cause erratic ICS behaviour. In one case, a robotic arm inadvertently became active, and on another occasion a gas utility's ICS was locked up, stopping gas flowing for several hours [68].
- A software error in a station which pumps drinking water to Hekelgem, Belgium caused a disruption in the delivery of drinking water to 30,085 people for several hours on 23 November 2014 [69].
- ICS connections to the Internet. The German IRAM project by the Technische Universität Berlin produced a global inventory of various types of ICS directly accessible from the internet. They provide surprising maps and YouTube movies [70].

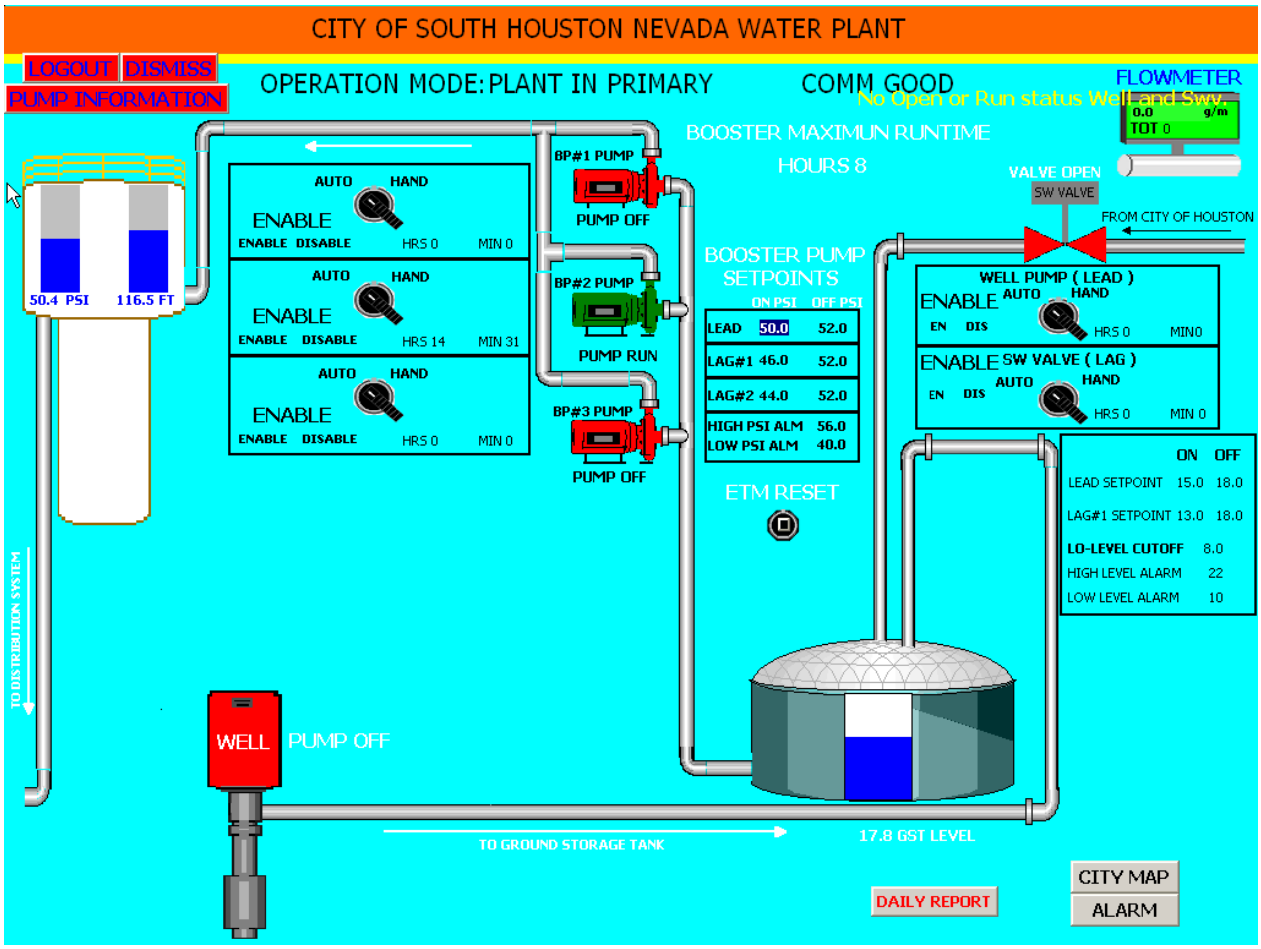

Figure 1: Bad things happen: screenshot of the HMI view of a US water plant 'donated' by a hacker to the pastebin repository.

4 Organisational Challenges

You are now aware of the cyber risk your ICS is facing. Are you determined to take appropriate action? This chapter explains why even after an organisation recognises the cyber security issues of ICS, the governance of implementing risk mitigating controls often proves difficult. Challenges include bridging the knowledge of the ICS, IT and cyber security domains within the organisation, building a business case for cyber security of ICS, and streamlining cyber security efforts over time.

4.1 ICS Hide-and-Seek in Functionality

Functionality, often under the responsibility of a non-IT department, controlled and monitored by ICS has gradually become IT. The operators still think in terms of on/off switches or a knob to crank up the flow or speed of the controlled process. The fact that there is an ICS in between the display with the switch or knob, and the actuator, motor, valve, etc. - and that therefore there is some IT with cyber security risk - is not recognised. The responsible department for, e.g. the management of a building, allows the connection to the outside world of HVAC, access control systems, and elevator control systems, for remote maintenance. The cyber security of the building may be jeopardised as they open cyber back doors to their organisation (for example, see [32]). Similarly, many remotely operated processes in our daily lives have control systems embedded. These systems are increasingly connected to (private) networks that in turn are connected to the global grid.

4.2 IT and ICS: Opposing Forces

4.2.1 Different cultures

Apart from their differences in functionality and technology, ICS and (office) IT historically have been managed by separate organisational units. IT people tend not to talk with the process-oriented people of the process department, as that is about grease, pumps, motors, valves, and certainly not IT. The process department on the other hand optimises the processes and keep them running; ICS is not considered IT by them. The number of people understanding and bridging both domains is limited. The number of people

understanding cyber security for both IT and ICS, and how to adopt an integrated security approach, is even more limited.

As ICS technology moves slowly towards regular IT, closer cooperation between the ICS and IT domains is desirable. Organisations that have brought the people of these different domains together have successfully bridged the gap, improved the mutual understanding, and increased the security posture of their IT and ICS domains.

4.2.2 A gap in cyber security awareness, education and interests

The ICS workforce traditionally consists of middle-aged employees with vast knowledge and experience with ICS technology but less knowledge of current developments in IT. Conventionally, process automation engineers have not been trained in information security. They themselves, as well as their organisation, are largely unaware that a task has been added to their job profile. Even when process automation managers are aware of cyber security issues, they seldom find a listening ear at the top, because implementing cyber security for ICS often costs a lot of money (notwithstanding the potential business impact risk).
The IT workforce is populated by younger employees with typically more cyber security knowledge. However, they do not put in an effort to secure the ICS as they do not recognise the IT in process automation. Even if they do, they are generally unfamiliar with the peculiarities and limitations of ICS technology.
Whenever process automation engineers and IT people try to work together, a huge cultural difference becomes evident between the process control approach ('twenty-four hours a day, seven days a week') on the one hand, and the approach of the office automation management ('just re-boot during the lunch break') on the other hand.

4.3 Justifying Cost

The business case for investing money into IT and ICS security has traditionally been a difficult one. The reason is that the benefits of better security cannot be expressed in terms of direct profit, but rather in terms of loss prevention [3]. Even with hindsight, it is difficult to determine the return on security investment: which incidents would have taken place had the security measures been neglected?
As budget claims nowadays must be justified by substantiating their cost-effectiveness, attempts have been made to develop supportive models. The Return on Security Investment (ROSI) model was proposed by Gordon and Loeb [53] to quantify benefits by relating the expected loss resulting from security incidents to the costs associated with mitigating security controls. Although there has been discussion about the model's practical value, the model does provide insight in how security may be valued. Keep in mind that the decision to implement security controls need not always be motivated by just balancing potential business impact and

cost. Other drivers may be: legally enforced security regulation (e.g. a 'licence to operate') or Corporate Social Responsibility (CSR) policies to reduce specific societal or environmental risk to a minimum.
On the cost side of the business case, ICS cyber security controls can be relatively expensive especially when they need to be implemented on a large number of sites or when they address older, proprietary ICS components. Unfortunately, the main budget holders are often at a significant organisational distance from the department which is responsible for installing, operating and maintaining ICS. Most often, the costs for cyber security are allocated to the IT and ICS-related departments, while the business profits are generated by totally different departments. This makes it even more challenging to put across the business case and convince decision makers of the necessity for security expenditures in the ICS domain.
A good practice for substantiating investments in ICS security is performing a self-assessment to benchmark an organisation's ICS cyber security maturity level. Available self-assessment tools include the CSET tool made available by the US Department of Homeland Security [28]. A different way is performing a self-assessment benchmark across a sector or other set of peers, similar to what has been done in the Dutch energy, drinking water, and the surface water management sectors [51].

4.4 Legacy systems

Due to the long economic life of ICS components, most ICS systems are built up from a large installed base of aging hardware and software that can only slowly be replaced. While this fact must be accepted by system owners and other stakeholders, it should alert them to the importance of making sensible choices related to securing their ICS when migration opportunities arise. Replacing legacy ICS by new ICS without cyber security functionality may create serious risks to the organisation for many years to come.
For organisations operating ICS, a key good practice is to keep an accurate inventory of assets, including hardware, software and firmware versions, as well as communication interfaces. Asset management is a prerequisite for effective cyber security risk management. Mitigating actions may include system hardening (disabling all functions that are not required for ICS operation) or applying layers of protection that provide a more secure external interface while using the legacy component's functionality internally.
Another good practice is to apply corporate security policies to newly acquired and legacy ICS components and network interfaces equally. Even when it is impossible for legacy systems to adhere to a policy, it is valuable to evoke an explicit "comply or explain" statement and identify any associated security risk.
Finally, management is well advised to establish a migration strategy and roadmap. This allows for a coherent phased approach and timely allocation of budgets. Replacement of ICS components should not just be based on isolated decisions constrained by local or ad hoc budget considerations.

On the super-organisational level, a joint effort can be made to accelerate the development and adaptation of more secure ICS technology. Such efforts are made within sectors through the definition of cyber security requirements for vendors or other interest group initiatives to influence vendors. An example of such an effort is the WIB standard, see paragraph 6.4.5.

While these sector specific and standardisation efforts are of great value, one should keep in mind that the legacy challenge is not primarily a lack of secure technology, but the organisational and technical difficulties involved in applying technology that is already available.

More information on the ICS and legacy topic can be found in the whitepaper [46].

5 Moving Towards Cyber Resilience

Cyber resilience for ICS requires a balanced, forward looking approach to the trio of: people, processes and technology. Key elements of a 'culture of security' identified in this chapter include the use of maturity models for assessing your cyber security posture, growing a work force with adequate skills and expertise, and ensuring that cyber-security requirements are a key consideration when procuring or replacing ICS components.

5.1 Culture of Security: Think Secure

The culture of ICS security, or Think Secure concept, is based on the following elements:

- Requirements: specify secure ICS and a secured ICS environment;
- Procurement: buy secure ICS;
- Engineering, development and system integration: develop secure ICS while properly assessing and understanding its impact on delivery, safety and cost;
- Projects: deploy secure ICS;
- Operations: run and maintain ICS securely;
- End-of-life: secure decommissioning and disposal of ICS.

During all these phases of the cyber security life-cycle, informed and trained personnel are needed (see paragraph 5.3) who are empowered to act responsibly.

5.2 Maturity Models

Maturity models are commonly used to review and benchmark an organisation's IT capabilities and processes. A key element in a maturity model is a reference framework defining a set of maturity levels. This may be accompanied by self-assessment checklists or tools. A cyber security maturity model serves two purposes. Firstly, organisations can use it to obtain an objective metric for their actual cyber security level. Secondly, maturity models can be used to define milestones in an organisation's roadmap towards improved cyber security capabilities.

The WEF proposed a model defining five levels of cyber security maturity [7]. In Figure 2, these levels graphically represent the 'hyper connection readiness curve', or the extent to which organisations are ready to address cyber security challenges in a hyper connected world. To what extent are ICSs part of this hyper connected world? Chapter 0 has made it clear that most ICS are no longer isolated systems and they have various external interfaces at a technical level. The term hyper connectivity not only pertains to technical interfaces, but also reflects the need to cooperate and exchange information with peers, external suppliers and operators of other dependent infrastructures [45]. The 'hyper connection readiness curve' can therefore be used in the ICS domain to assess whether an organisation makes conscious decisions about the desired level of connectedness, and what the maturity level of the organisation is, in terms of identifying and managing the related risk.

Figure 2: Five maturity levels of cyber security (source: WEF [7]).

Few cyber security maturity models exist that specifically address ICS. One example is the *Cyber security Capability Maturity Model (C2M2)* [20]. C2M2 has been developed by the US Department of Energy and the US Department of Homeland Security. C2M2 specifically targets the energy critical infrastructure sector and

its ICS: the model and toolkit have specific 'flavours' for the electricity, and the oil and natural gas subsectors. Other sectors could benefit from the development of similar maturity models tailored to their specifics.

5.3 Work Force Development

To address the wide range of risk factors to ICS, a Work Force Development Framework helps to standardise skills, knowledge and abilities for ICS security across the wide set of industries applying ICS within the core business. Such a 'Workforce Development Framework' has been developed within the Thematic Area 'ICS and Smart grids' of the European ERNCIP (European Reference Network for Critical Infrastructure Protection). It is carried forward as an international standard which also allows the certification of people.
The framework embeds a 'Workforce Development Model' which describes ICS security roles and responsibilities to maximise the resilience of critical infrastructures. For each of the identified roles, a competence framework exists which describes the cyber security knowledge and skill elements that should be mastered by following specific training blocks or gathered by experience. In certain cases, industry may require proof of the acquired knowledge and skills by means of certification. The framework joins elements from ICS security, IT, cyber security, and industrial, company and professional standards which are required as hybrid knowledge and skills by ICS Security professionals. It stimulates the market to provide cyber security for ICS training and certification. A first worldwide certification is the Global Industrial Cyber Security Professional (GICSP) that is supplied by the Global Information Assurance Certification (GIAC) organisation [44]. The certification has to be renewed every four years. Note that the framework also helps to cover the risk of unprofessional behaviour by third party installation, maintenance and support personnel.

In the ENISA report 'Certification of Cyber Security Skills of ICS/SCADA professionals' [5], a few other certifications/certificates are mentioned as well, such as Certified SCADA Security Architect (CSSA) and the ISA99/IEC 62443 Cyber Security Certificate Program.

5.4 Procurement of ICS Products and Services

ICS manufacturers, system integrators, and the suppliers of ICS services (from design and application development to turnkey project development and maintenance) play a major role in ICS security. They design, develop, implement and maintain ICS environments in (critical) infrastructures. They are the organisations that should ensure that the ICS software provides integrated security options. But they can also lead by example and raise their clients' ICS security posture to a higher level through the advice they provide and their professional way of working. For example, they can offer 'hardening' of the underlying operating system

in their quotations and proposals. Alternatively they can make proactive agreements from the supply side about secure ways of working by their maintenance personnel.
ICS operators, from their side, must be aware of dependencies and manage the cyber risk across interfaces with third parties. The following good practices can be adopted:

- When acquiring ICS components, include cyber security requirements in the system requirements presented to suppliers. These cyber security requirements should be derived from cyber security risk assessments and analysis of possible mitigating controls.
- When possible, contractually demand that suppliers and their subcontractors comply with your cyber security approach and policies.
- Suppliers must be requested to demonstrate that their employees bring the cyber security qualifications required for their tasks and responsibilities. Where useful, awareness training on relevant security policies may be provided.
- By joining forces with peers you may put pressure on suppliers to include cyber security in their product roadmaps. An example is compliance with (parts of) the cyber security standards discussed below.

5.5 Replacing ICS: Be Aware of Trapdoors

When replacing ICS, one has to consider:

- That it is likely that for a certain period of time, the new ICS has to coexist with legacy systems [46]. That may mean that not all security options of the ICS will be configured. When finally replacing legacy systems, one should consider introducing the full set of security options.
- Unfortunately, ICS vendors may deliver products which are not secure out of the box. When replacing old ICS functionality by new ICS products, one may unwittingly introduce new functions in the ICS network which are not configured, as they are not used operationally. This could be a lever that the hacker and his tools are looking for.
- Finally, receiving new ICS excites the system engineers. The old ICS is put into a corner and moves out of the organisation without much attention. However, not cleaning memories, destroying or securely wiping computer media may cause critical process parameters and network configuration data to fall into the hands of cyber attackers.
- ICS vendor product roadmaps show that in the next few years they will focus on mobility, virtualisation, remotely managed Security Operating Centres (SOC) and cloud based components. All are new concepts in the ICS domains and all may bring new and much-needed features, but may also introduce new risk factors.

- Equipment integrity: your organisation may be faced with ICS and communication equipment that was either counterfeited or tampered with between the manufacturer and your place of installation. To address this risk, control your supply chain by only buying from Original Equipment Manufacturers (OEM) or their authorised resellers. In addition, the authenticity of equipment should be inspected, e.g. by comparing physical characteristics and software hashes.


GCCS 2015
The Netherlands

6 Be strong together

Fighting the cyber security risk of ICS on your own is a losing battle. As many organisations face similar challenges, one can benefit from joining forces with peers and with government agencies, e.g. by sharing cyber security-related information on ICS. In most industries, cyber resilience is considered a common interest and not part of the competitive arena. ICS operators and vendors have a shared responsibility to enhance the security level of ICS products; the establishment and implementation of standards is an important means to this end.

6.1 Join an ICS Security Community

To address cyber security threats and risk in a timely way, an organisation may team with its peers and or government agencies to share information on: for instance, threats, vulnerabilities, threat actors, incidents, and good practices. Such teaming may either be sector-specific or ICS (type) specific, and national or international. Sectoral Information Exchanges and Information Sharing and Analysis Centres (ISACs) have been established in various nations [45]. Examples of thematic Information Exchanges are the European SCADA and Control Systems Information Exchange (EuroSCSIE) [39] and the ICS-CERT [42] communities.

Good Practice documents, each addressing the ICS/SCADA security topics from a different angle, emerge from such communities:

- Checklist Security of ICS/SCADA systems [2],
- Guide to increased security in industrial information and control systems by the Swedish Civil Contingencies Agency with a focus on the organisational and tactical/operational management levels [34],
- The Qatar National ISC Security Standard stating both Policy Objectives and Policy & Baseline Controls [33],
- Various Good Practice documents by Centre for the Protection of National Infrastructure (CPNI) in the United Kingdom ([26], [31]),
- SCADA Good Practices for the Dutch drinking water sector written for the organisational and tactical/operational management levels, which are of use to other sectors as well [16],
- A NIST Guide to Industrial Control Systems (ICS) Security [18],
- DoE's 21 Steps to improve the security of SCADA networks [38],
- ICS-CERT advisories, fact sheets, and online training [42].

6.2 Information Sharing

Information Sharing of ICS cyber security related information with peers may help organisations to become less vulnerable and more resilient against cyber threats to their ICS. Public and private sector specific ISAC and Information Sharing and Analysis Organisations (ISAO), cover the cyber security of the OT domain. ICS-thematic, non-sector specific national and international computer emergency response teams, e.g. ICS-CERT [42], and information exchanges, e.g. EuroSCSIE [39]. Each covers another part of the cyber security incident cycle. For guidance on the topic *Information Sharing of cyber security-related information*, an accompanying Good Practice document has been published [45].

6.3 Incident Response Cycle

Incident Response for ICS should span all phases of the incident management cycle, which is outlined in the National Cyber Security Framework Manual (NCSFM) [29] on pages 112-114. The cycle comprises the phases pro-action, prevention, preparation, incident response, recovery, and aftercare / (legal) follow up.

Figure 3: The Incident Response Cycle

Each phase requires attention in one's ICS security plans and the set of related organisational, procedural and technical measures. For example, your organisation may decide to internally concentrate on pro-action and prevention activities and rely on sharing communities, e.g. a CERT, to provide support during the incident

response and recovery phases. Your national law enforcement agency may meanwhile gather and provide you with intelligence which allows you to disrupt or prevent an incident from occurring. They may offer help to derive specific evidence and situational information from an incident which can be used in the investigation and the prosecution of the culprit.

6.4 Requirements and Standards

Good practices invented by organisations may be implemented by their peers. Such practices evolve after some discussion into formal good practices, norms and standards. These are issued by industry and/or by national and international standards bodies. Below, we discuss some relevant standards and activities regarding the procurement phase of secure(d) ICS, and secured operations. Note that these standards may be used both for products and (third party) services related to the ICS domain.

6.4.1 ISO/IEC 27000 series

The ISO/IEC 27001 standard [13] is a widely established standard for information security management. The standard lays out how organisations may establish an Information Security Management System (ISMS) in which security is managed as a uniform controlled process, continuously updated based on reviews and audits. The ISO/IEC 27001 standard is accompanied by the ISO/IEC 27002 standard [14] which contains a set of information security controls, categorised into topics such as access control, communication security, physical security, human resource security etc. Whereas the security controls have a relatively high abstraction level, they are accompanied by implementation guidance with suggestions for how to put the controls into practice.

Organisations may choose to have their ISO/IEC 27001 implementations reviewed by an external certified auditing service provider, allowing them to carry a formal ISO/IEC 27001 certification. In 2013, the ISO/IEC 27001 standard has received an update to better align it with other standards like the ISO/IEC 9001 (quality) and ISO/IEC 22301 (business continuity management).

The scope of ISO/IEC 27001 covers any large organisation concerned with information security. This includes critical infrastructure providers aiming for a structured approach to addressing their cyber security risk. In particular, the standard can be uniformly applied to an organisation's ICS and other IT systems and infrastructures alike, thus supporting harmonisation of security across these domains both on the technical and process level.

Although the security controls of the ISO/IEC 27002 standard were designed to be generic and applicable to all types of information systems and application domains, it is not trivial to implement these controls in the

ICS domain, with its legacy systems and high availability requirements. This requires non-trivial expert knowledge of both ICS and cyber security.
A special concern relates to safety critical systems, as a mismatch exists between the safety critical system domain and the ISO/IEC 27002 controls, as was already outlined in 2003 by the European Workshop on Industrial Computer Systems Reliability, Safety and Security (EWICS) [40].
An attempt to close the gap between the ISO 27002 controls and the specifics of ICS has been made by ISO itself by releasing the technical report ISO/IEC 27019 [15]. The aim of ISO/IEC 27019 is to extend the ISO/IEC 27002 controls to the domain of digital process control systems and automation technology for the energy utility industry. ISO/IEC TR 27019 specifically covers digital process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat, in combination with the control of supporting processes.

6.4.2 International Society of Automation (ISA)

The International Society of Automation (ISA) has produced several sets of standards with particular relevance to the cyber security of ICS. Their ISA-99 standard was adopted by the International Electrotechnical Commission (IEC) and was renamed into ISA/IEC 62443 [17]. ISA/IEC 62443 comprises a series of standards, technical reports, and related information that define procedures for securely manufacturing, designing, implementing, or managing ICS. Standards are structured along four themes: general, policies and procedures, system, and components.

The ISA-95 standard was internationally adopted as IEC 62264 [9]. This standard for ICS addresses the important challenge of how to develop an automated interface between enterprise and control systems. ISA-95 defines five levels in industrial companies ranging from the physical production processes up to enterprise resource planning systems not directly related to production. Although it is by no means a security standard, its layered model has proven useful for defining security perimeters between the ICS and non-ICS domains.

6.4.3 OLF Recommended Guidelines #104

The Norwegian Oil and Gas industry Association (Norsk Olje og Gass) recommended guidelines for information security baseline requirements for process control, safety and support IT systems is a standard for the security of ICS. The mandatory use of this OLF 104 standard in the oil and gas industry has been codified in Norwegian law. Currently, a Norwegian technical committee works on updating the OLF standard [36]. The good practice is accompanied by a public self-assessment tool (Excel) [36].

6.4.4 CSPL

In 2009, ICS users and providers in America have jointly drawn up a Cyber Security Procurement Language for Control Systems (CSPL)[10]. This catalogue detailing security requirements for ICS is a step towards the development of a professional, joint approach to ICS (information) security.

6.4.5 WIB

Established in 1953, the WIB - Working-party on Instrument Behaviour [47] - is an association of process automation end-users for sharing knowledge and experience amongst the members. The WIB closely cooperates with its sister organisations NAMUR (User Association of Automation Technology in Process Industries) in Germany, EXERA in France, and EI (Evaluation International) in England.

With respect to the cyber security topic, today's end-users are faced with new challenges to keep their production facilities running while continuously taking into account the possibility of cyberattacks on their networks and systems. Therefore, the WIB Control Systems working group, which is concerned with plant security, took the initiative to draft the "Process control Domain: security requirements for vendors (M2784-X10 V2.0)" document [48]. This document is now a working product of the IEC TC65/WG10 committee which incorporated the WIB-document in the international standard IEC 62443 as IEC 62443-2-4 [11]. It has currently reached the IS (International Standard) status and is to be published by the IEC imminently as a standard. The standard focuses on the certification of ICS supplier security policies and practices. The proposed equivalent by ISA as part of ISA SP-99 will be a U.S. national publication of the IEC standard. This will open up the possibility of ICS certification with respect to information security.

The standard specifies requirements and provides recommendations for security measures to be implemented by manufacturers and vendors of ICS. This covers policy aspects related to the vendor's organisation, IT security processes, technological solutions, as well as the governance of their IT security. When a vendor's solution complies with this set of requirements, their solution is considered to be WIB Security Compatible. An end user or 'the Principal' shall comply with their own security policies, standards and specifications for their ICS domain. The common requirements of all the Principals are put into a WIB set of minimum requirements for vendors to comply with. Security Compatible solutions contribute in attaining this compliancy, but require additional security controls, e.g. adequate work procedures, skills & competencies of staff, etc.

The WIB Control Systems working group and the NAMUR security members strongly believe that awareness and actual implementation of the standard by the ICS suppliers and end-users is the next challenge. Therefore, the WIB and NAMUR are working together to create a roadmap / guideline on how to implement ICS security requirements in end-user organisations as well as in the organisations of their ICS suppliers. Coordination and cooperation with ICS vendor organisations like Federatie Technologiebranches (FHI) in The

Netherlands and the German Electrical and Electronic Manufacturers' Association (ZVEI) in Germany are already in progress.

6.5 Certification of ICS Components

Several schemes have been developed for ICS component certification, like schemes based on the Common Criteria or ISO/IEC 15408 [12], ISAsecure (isa.org) [43], and the Achilles communications certification Program:

1. The Common Criteria scheme started as an international effort to evaluate and certify the security features of IT systems, applications and products and encourage secure product development practices. It currently has more than twenty member countries formally accredited to conduct internationally recognised evaluations. These evaluations employ 'protection profiles' to define the functions being evaluated and the target outcomes. France has developed specific protection profiles for ICS [23].
2. The ISAsecure is an initiative of the Industrial Society for Automation. Their certification program [43] is based upon the IAC (Industrial Automation and Control) security lifecycle as defined in the ISA/IEC 62443 standard. As of now, the scope of the ISASecure certifications includes assessments of off-the-shelf ICS products and ICS product development security lifecycle practices.
3. The Achilles program was initiated by one of the industry prominent vendors as an attempt to reflect commitment to secure design. The Achilles program is based upon the IEC 62443-2-4 "Certification of IACS supplier security policies and practices" standard, and comprises two parts:
   - Achilles® Communication Certification.
     The Achilles Test Platform earned a formal recognition for Communication Robustness Testing for the ISASecure Certification program. It ensures the deployment of robust communications for industrial control systems and SCADA systems.
   - Achilles® Practices Certification.
     This certification provides independent verification that device manufacturers meet security best practices throughout the development lifecycle.

7 The Next Steps

Governments worldwide are adopting different approaches to promote and derive ICS security good practices. The approaches may include incentives to vendors and operators who demonstrate commitment towards security. Other nations have issued mandatory ICS security baselines that operators have to meet, e.g. the Qatari National ICS security standard [33]. The latter has been developed through an existing PPP model called (EN-IREC) that involves critical (information) infrastructure operators and government.

As critical infrastructures in many nations are monitored and controlled by ICS which are supplied by a limited set of suppliers, there is a need for global solutions, cyber security approaches, and harmonised workforce developments. Collaborative research and development on the cyber security of ICS, e.g. developing new robust and secure ICS protocols, needs international priority. A number of initiatives have already started. Policymakers and leadership can accelerate and push these developments towards resilient ICS based infrastructures.

Last but not least, you need to take your responsibility to protect your ICS and to engage other organisations to do the same.

References

Netherlands Government and Agencies

[1] Luiijf, H.A.M. (2010), "Process Control Security in the Cybercrime Information Exchange", NICC, The Hague, The Netherlands. On-line: http://www.cpni.nl/publications/PCS_brochure-UK.pdf

[2] NCSC (2012), "Checklist Security of ICS/SCADA systems", factsheet 2012-02, Ministry of Security and Justice, The Hague, The Netherlands. Online: https://www.ncsc.nl/binaries/content/documents/ncsc-en/services/expertise-advice/knowledge-sharing/factsheets/checklist-security-of-ics-scada-systems/1/Checklist security of ICS SCADA systems.pdf

Europe (European Commission, European Union, ENISA, World Economic Forum)

[3] ENISA (2012), "Introduction to Return on Security Investment", Heraklion, Greece. Online: https://enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

[4] European Council (2008), "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection", Brussels, Belgium. On-line: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[5] A. Pauna (2015), "Certification of Cyber Security skills of ICS/SCADA professionals", ENISA, Heraklion, Greece. Online: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals/at_download/fullReport

[6] A. Pauna, K. Moulinos (2013), "Window of Exposure… a real problem for SCADA Systems", ENISA, Heraklion, Greece. Online: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/window-of-exposure-a-real-problem-for-scada-systems/at_download/fullReport

[7] World Economic Forum (2014), "Risk and Responsibility in a Hyperconnected World (WEF principles)", Geneva, Switzerland. Online: http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience

[8] World Economic Forum (2012), "Partnering for Cyber Resilience. Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience", Geneva, Switzerland. Online: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

Standards (ISO, NIST, de facto)

[9] ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod), "Enterprise-Control System Integration - Part 1: Models and Terminology", International Society of Automation, North Carolina, USA.

[10] DHS (2009), “Cyber Security Procurement Language for Control Systems”, Department of Homeland Security, USA. Online: https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf

[11] IEC (expected 2015), “IEC 62443-2-4: Requirements for Security Programs for IACS Integration and Maintenance Service Providers“, International Society of Automation.

[12] ISO/IEC 15408:2008-2009, “Information technology -- Security techniques -- Evaluation criteria for IT security, ISO, Geneva, Switzerland.

[13] ISO/IEC 27001:2013, “Information technology -- Security techniques -- Information security management systems -- Requirements” including correction ISO/IEC 27001:2013COR1:2014, ISO, Geneva, Switzerland.

[14] ISO/IEC 27002:2013, “Information technology -- Security techniques -- Code of practice for information security controls” including correction ISO/IEC 27002:2013/COR1:2014, ISO, Geneva, Switzerland.

[15] ISO/IEC TR 27019:2013, ”Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry” , ISO, Geneva, Switzerland.

[16] H.A.M. Luiijf (2008), “SCADA Good Practices for the Dutch Drinking Water Sector”, TNO DV 2008 C096. Online: https://www.tno.nl/media/1538/tno-dv-2008-c096_web.pdf

[17] IEC/TS 62443-1-1 ed1.0, “Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models”, International Electrotechnical Commission, Geneva, Switzerland.

[18] K. Stouffer, J. Falco, K. Scarfone (2011), “Guide to Industrial Control Systems (ICS) Security”, NIST Special Publication SP 800-82, USA, 155 pages. Online: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[19] NIST (2014), “Framework for Improving Critical Infrastructure Cybersecurity“, NIST, USA. Online: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[20] USA Department of Energy and US Department of Homeland Security, “Cybersecurity Capability Maturity Model (C2M2)”, version 1.1, February 2014. Online: http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

Meridian and International Resources

[21] ANSSI (2014), “La cybersécurité des systèmes industriels” (Cyber Security for Industrial Systems), Agence nationale de la sécurité des systèmes d'information, Paris, France. Online: http://www.ssi.gouv.fr/entreprise/guide/la-cybersecurite-des-systemes-industriels/ (multiple documents)

[22] ANSSI (2015), “Guide pour une formation sur la cybersécurité des systèmes industriels” (Guide for Training on Cyber Security for Industrial Systems), Agence nationale de la sécurité des systèmes

d'information, Paris, France. Online: http://www.ssi.gouv.fr/entreprise/guide/guide-pour-une-formation-sur-la-cybersecurite-des-systemes-industriels/

[23] ANSSI (2015), "Protection Profiles for Industrial Systems" (in French), Agence nationale de la sécurité des systèmes d'information, Paris, France. Online: http://www.ssi.gouv.fr/entreprise/guide/profils-de-protection-pour-les-systemes-industriels/

[24] BSI (2013), "ICS-Security-Kompendium", Bonn, Germany. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile

[25] BSI (2014), "ICS-Security-Kompendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten", Bonn, Germany. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.pdf?__blob=publicationFile

[26] Centre for the Protection of National Infrastructure (CPNI), United Kingdom. Online: http://www.cpni.gov.uk/about/cni/
CPNI's website provides a collection of SCADA Good Practices, including a firewall guide.

[27] Department of Homeland Security, "Cyber Security Questions for CEOs", Washington DC, USA. Online: https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

[28] Department of Homeland Security, "Downloading and Installing CSET", Washington DC, USA. Online: https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

[29] E. Luiijf and J. Healey (2012), "Organisational Structures & Considerations", in: A. Klimburg, *National Cyber Security Framework Manual*, NATO CCD-COE Publications, Tallinn, Estonia. Online: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

[30] MERIDIAN home page. Online: http://meridianprocess.org/cms.aspx?e=21&id=6

[31] GOV.UK, "10 Steps: A Board Level Responsibility", CESG/CPNI, London, United Kingdom, 16 January 2015. Online: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-a-board-level-responsibility

[32] GAO (2015), "Federal Facility Security: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems", report GAO-15-6, Washington DC, USA. Online: http://www.gao.gov/products/GAO-15-6

[33] ictQatar (2014), "National ICS Security Standard v.3 March 2014", The National ICS security standard, , Ministry of Information and Communications Technology, Qatar. Online: http://www.ictqatar.qa/en/documents/document/controls-security-critical-industrial-automation-and-control-systems

[34] MSB (2014), "Guide to increased security in industrial information and control systems", Swedish Civil Contingencies Agency, Stockholm, Sweden. Online: https://www.msb.se/RibData/Filer/pdf/27473.pdf

[35] N.N. (2014), "Belgian Cyber Security Guide: Protect Your Information", Belgium. Online: https://www.b-ccentre.be/wp-content/uploads/2014/04/B-CCENTRE-BCSG-EN.pdf

[36] OLF, "Recommended guidelines for information security baseline requirements for process control, safety and support ICT systems", OLF104, Norway. Online: http://www.norskoljeoggass.no/en/Publica/Guidelines/Integrated-operations/104-Recommended-guidelines-for-information-security-baseline-requirements-for-process-control-safety-and-support-ICT-systems/

[37] Public Safety Canada (2012), "Industrial Control System (ICS) Cyber Security: Recommended Best Practices", Ottawa, Canada. Online: https://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-002-eng.aspx

ICS Communities

[38] DoE (2007), "21 steps to improve the security of SCADA networks", U.S. Dept. of Energy, USA. Online: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

[39] EuroSCSIE (European SCADA and Control Systems Information Exchange). Online: https://espace.cern.ch/EuroSCSIE/default.aspx

[40] EWICS: European Workshop on Industrial Computer Systems Reliability, Safety and Security. Online: http://www.ewics.org

[41] EWICS TC7 (2003), "A Study of the Applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the Needs of Safety Critical systems: Executive Summary", I.C. Smith (ed), EWICS TC7, EWICS. Online: http://www.ewics.org/attachments/roadmap-project/RdMapD31ExecSummary.pdf

[42] ICS-CERT, The Industrial Control Systems Cyber Emergency Response Team resources, alerts, advisories, reports, links, etcetera. Online: https://ics-cert.us-cert.gov/

[43] isaSecure. Online: http://www.isasecure.org/en-US/

[44] Global Industrial Cyber Security Professional (GICSP). Online: http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

[45] Eric Luiijf and Allard Kernkamp (2015), "Sharing Cyber Security Information: Good Practices Stemming from the Dutch Public-Private-Participation Approach", TNO, The Hague, The Netherlands. Online: http://www.tno.nl/infosharing

[46] M. Oosterink (2012), "Security of legacy process control systems: moving towards secure process control systems" (whitepaper), The Hague, The Netherlands. Online: http://www.cpni.nl/files/6313/3296/3223/CPNI.NL_WhitepaperUK-4.pdf

[47] WIB. Online: http://www.wib.nl/

[48] WIB (2010), "Process control Domain: security requirements for vendors. Version 2.0", The Hague, The Netherlands. Download form: http://www.wib.nl/download.html

Academic References and Research Organisations

[49] CIPedia. Online: http://www.cipedia.eu

[50] E. Luiijf (2013), "Discussion: Why are we so unconsciously insecure?", in: International Journal of Critical Infrastructure Protection 6(2013) pp. 179-181. DOI information: 10.1016/j.ijcip.2013.10.003.

[51] H.A.M. Luiijf, M. Ali, A. Zielstra (2011) "Assessing and Improving SCADA Security in the Dutch Drinking Water Sector" in: International Journal of Critical Infrastructure Protection 4(2011) pp. 124-134.

[52] P. Massart, A. Ghianda, S. Smith (2013), "Where Cyber Security is Heading", Security & Defence Agenda (SDA), Brussels, Belgium. Online: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=159402

[53] L.A. Gordon and M.P. Loeb (2002), "Return on Information Security Investments: Myths vs. Reality" Strategic Finance. Online: http://www.researchgate.net/publication/263808420_Return_on_information_security_investments_Myths_versus_realitieshttp://www.researchgate.net/publication/263808420_Return_on_information_security_investments_Myths_versus_realities

ICS Incidents Happen

[54] Marschall Abrams and Joe Weiss, "Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia", Boston, USA. Online: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

[55] Nicolas Falliere, Liam O Murchu, and Eric Chien (2011), "W32.Stuxnet Dossier", Cupertino CA, USA. Online: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[56] Kelly Jackson Higgins (2015), "Banking Trojans Disguised as ICS/SCADA Software Infecting Plants", DARKReading, USA. Online: http://www.darkreading.com/attacks-breaches/banking-trojans-disguised-as-ics-scada-software-infecting-plants/d/d-id/1318542

[57] ICS-CERT (2014), "Alert (ICS-ALERT-14-281-01B): Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)", DHS, USA. Online: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

[58] ICS-CERT (2014), "Advisory (ICS-ICSA-14-178-01): ISC Focused Malware", DHS, USA. Online: https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01

[59] Gregg Keizer (2012), "Virus attack on oil processing facilities in Iran", Computerworld. Online: http://www.computerworld.com/s/article/9226469/Iran_confirms_cyberattacks_against_oil_facilities

[60] Security.nl (2010), Conficker attack on Royal Friesland Campina, Netherlands. Online: http://www.security.nl/artikel/33906/1/Gerichte_hackeraanval_op_zuivelco%C3%B6peratie.html

[61] Kevin Poulson (2003), “Slammer worm crashed Ohio nuke plant network”, SecurityFocus. Online: http://www.securityfocus.com/news/6767

[62] BSI (2014), Cyberattack on a German iron plant, Bonn, Germany. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[63] Security.nl (2014), Disgruntled employee sabotages waste water processing facility, Netherlands. Online: https://www.security.nl/posting/404755/Werknemer+waterzuivering+VS+verdacht+van+sabotage

[64] U.S. Department of Justice Press Release “Arlington Security Guard Arrested on Federal Charges for Hacking into Hospital’s Computer System”, June 30, 2009. Online: http://www.justice.gov/usao/txn/PressRel09/mcgraw_cyber_compl_arrest_pr.html

[65] David Kretz (2009), “Feds: Hacker disabled offshore oil platform leak-detection system”, Wired, USA. Online: http://www.wired.com/2009/03/feds-hacker-dis/

[66] John Leyden (2008), “Polish teen derails tram after hacking train network: Turns city network into a Hornby set”, The Register, UK. Online: www.theregister.co.uk/2008/01/11/tram_hack

[67] Richard Esposito (2006), “Hackers Penetrate Water System Computers“, ABC News 30 October 2006. Online: http://abcnews.go.com/blogs/headlines/2006/10/hackers_penetra/

[68] David P. Duggan (2005), “Penetration Testing of Industrial Control Systems”, Sandia National Laboratories, USA. Online: http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdf

[69] Rudy De Saedeleir (2014), Drinkwaterproblemen in Ledekerke, Afflichem en Sint-Katherina-Lombeek (update), Goeiedag.be, Belgium. Online: http://www.goeiedag.be/affligem/2014/11/drinkwaterproblemen-in-liedekerke-affligem-en-sint-katherina-lombeek

[70] The Industrial Risk Assessment Map (IRAM) project on SCADA and other ICS systems connected to the Internet, Freie Universität Berlin, Germany. See for instance, http://www.scadacs.org and https://www.youtube.com/watch?v=yjPcftd2Ur4

List of Abbreviations

APT	Advanced Persistent Threat
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CSR	Corporate Social Responsibility
DCS	Distributed Control System
EC	European Commission
EGC	European Government CERTs
ENISA	European Union Agency for Network and Information Security
EuroSCSIE	European SCADA and Control Systems Information Exchange
GIAC	Global Information Assurance Certification
GICSP	Global Industrial Cyber Security Professional
HMI	Human-Machine Interface
HVAC	Heating, Ventilating, and Air Conditioning
IACS	Industrial Automation Control System
ICS	Industrial Control Systems
ICS-CERT	Industrial Control System CERT (USA)
ICT	Information and Communication Technology/Technologies
IEC	International Electrotechnical Commission
IP	Internet Protocol (suite)
ISAC	Information Sharing and Analysis Centre
ISAO	Information Sharing and Analysis Organisation

ISO	International Organization for Standardization [5]
IT	Information Technology/Technologies
NIS	Network and Information Security
OLF	Norwegian Oil and Gas Industry Association Guidelines
OT	Technology
PLC	Programmable Logic Controller
PPP	Public-Private Partnership
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SOC	Security Operating Centre
WEF	World Economic Forum

[5] note: ISO is not an abbreviation

Glossary

Critical infrastructure	An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. (EU definition [4]; other definitions at [49])
Cyber resilience	The ability of systems and organisations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery. (WEF definition [8]; other definitions at [49])
Cyber security	The analysis, warning, Information Sharing, vulnerability reduction, risk mitigation and recovery efforts for networked information systems. (WEF definition [8]; other definitions at [49])
Industrial Control Systems (ICS)	Industrial Control Systems is a general term that denotes various types of control systems such as Distributed Control Systems (DCS), Industrial Automation Control Systems (IACS), supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLC) which are used for measuring, monitoring and controlling physical processes.
Operational technology (OT)	Operational technology is defined by Gartner as an independent world of physical-equipment-oriented technology that is developed, implemented and supported separately from the IT department.
MERIDIAN	The Meridian Process aims to exchange ideas and initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP) issues globally. It explores the benefits and opportunities of cooperation between governments and provides an opportunity to share best practices from around the world. The Meridian Process seeks to create a community of senior government policymakers in CIIP by fostering ongoing collaboration.

	The Meridian Process recognises that it is only by working together that we can each advance our national CIIP goals and objectives. Participation in the Meridian Process is open to all countries/economies and is aimed at senior government policy-makers involved in CIIP-related issues. Every country/economy is invited to take part in the Meridian Process, and is encouraged to attend the annual Meridian Conference. [30]
SCADA	Centralised ICS that monitor and control entire sites, or groups of systems spread out at remote sites, for instance to control a national power transmission grid. Most SCADA control actions are performed automatically by Remote Terminal Units (RTU) and Programmable Logic Controllers (PLC).

Colophon

TNO

Oude Waalsdorperweg 63
2597 AK The Hague
Netherlands
http://www.tno.nl

Authors

Eric Luiijf — eric.luiijf@tno.nl
Bert Jan te Paske — bert_jan.tepaske@tno.nl

With contributions by

Auke Huistra

The MERIDIAN CIIP Community:

- ictQatar
- Public Safety Canada / Sécurité publique Canada
- Swedish Civil Contingencies Agency (MSB)
- U.S. Office of Cybersecurity and Communications (DHS)
- Meridian Coordinator – Peter Burnett

www.meridianprocess.org

The WIB

Commissioned by

Annemarie Zielstra, Director Cyber Security & Resilience, Defence, Safety and Security at TNO

Electronic version

Available at http://www.tno.nl/ICS-security

The preparation and publication of this document has been funded with the support of the Dutch Ministries of Economic Affairs, and Security and Justice as part of the National Roadmap to Secure Process Control Systems assignment. Moreover, the authors are grateful for the contributions and comments received from the MERIDIAN CIIP community.