CESG

CPNI
Centre for the Protection
of National Infrastructure

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

FRAMEWORK OVERVIEW

A GOOD PRACTICE GUIDE

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favouring by CPNI, CESG or PA Consulting Group. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. The content of this document is based on information available as at the date of publication.

The case study although fictitious is based on the experiences of PA Consulting Group through their work with companies in ICS industries. Any similarities are strictly coincidental and are not based on any one specific company.

This is general guidance only and is not intended to cover all scenarios or to be tailored to particular organisations or individuals. It is not a substitute for seeking appropriate specialist advice.

To the fullest extent permitted by law, CPNI, CESG and PA Consulting Group and their employees and advisers accept no responsibility for any errors or omissions contained within this document. In particular, to the fullest extent permitted by law, CPNI, CESG and PA Consulting Group and their employees and advisers shall not be liable for any loss or damage whatsoever, arising from any error or omission in this document, or from any person or organisation acting or refraining from acting upon or otherwise using the information contained in this document.

Copyright

Corporate Headquarters:

PA Consulting Group
123 Buckingham Palace Road
London SW1W 9SR
United Kingdom
Tel: +44 20 7730 9000
Fax: +44 20 7333 5050
www.paconsulting.com

Version no: Final v1.0

Prepared by: PA Consulting Group

Document reference:

CONTENTS

1 INTRODUCTION

1.1 Aims and objectives

The aim of this document is to provide good practice guidance for Industrial Control Systems (ICS) security. Specifically this document:

- Provides an overview of the necessity for ICS security
- Highlights the differences between ICS security and IT security
- Describes the key principles used to develop this framework
- Identifies eight core elements for addressing ICS security and for each, presents good practice principles
- Describes the Security for Industrial Control Systems (SICS) Framework which includes this document, the eight core elements and the supporting elements.

1.2 Terminology

1.2.1 Industrial Control System (ICS)

Throughout this framework the term Industrial Control System (ICS) is used as generic term to cover all industrial control, process control, distributed control system (DCS), supervisory control and data acquisition (SCADA), industrial automation and related safety systems.

1.2.2 Good Practice

Good practice, in the context of this document, is defined as:

> *The best of industry practices such as strategies, activities, or approaches, which have been shown to be effective through research, evaluation and implementation.*

The good practice summarised in this document is intended only as guidance. For some environments and ICS, it may not be possible to implement all of these principles. For example:

Good practice statement:
Protect ICS with anti-malware software on workstations and servers

Complication:
It is not always possible to implement anti-malware software on ICS workstations or servers (e.g. owing to lack of vendor accreditation)

Good practice statement:
Obtain vendor accreditation and configuration guidance from ICS vendors prior to deployment of such software

Complication:
Some vendors will not accredit anti-malware software and other ICS are incompatible with such software.

Where this is the case, other protection measures should be investigated.

2 SECURING INDUSTRIAL CONTROL SYSTEMS

2.1 Overview

ICS are making use of, and becoming progressively more reliant on, standard IT technologies. These technologies, such as Operating Systems, common protocols e.g. TCP/IP, web applications, and increasingly wireless technologies, are replacing conventional proprietary technologies and further enabling bespoke ICS to be replaced with off the shelf hardware and software.

Although there are positive business benefits to be gained from this development, this transformation brings two main concerns:

Firstly, ICS were traditionally only designed for the purpose of local control and to be reliable and safe rather than secure. Due to the need for connectivity to enable corporate users to access real time information, once isolated systems are now being connected to other systems or larger open networks. This exposes them to external threats, such as malware and hackers, that they were never expected to encounter and against which they have no robust defence.

Secondly, commercial off the shelf software and general-purpose hardware are being used to replace proprietary ICS. This means vulnerabilities affecting those technologies can now be exploited in those environments without specific knowledge of ICS. The systems are then made even more insecure because many of the standard IT security protection measures normally used with these technologies have not been adopted in the ICS environment. Security through obscurity is no longer a suitable kind of defence.

There are potentially serious consequences should these vulnerabilities be exploited. The impacts of an electronic attack on ICS can include, for example: denial of service, unauthorised control of the process, loss of integrity, loss of confidentiality, loss of reputation and health, safety and environmental impacts.

2.2 ICS security framework

Although ICS are now frequently based on standard IT technologies, their operational environments differ significantly from the corporate IT environment. There are a great number of lessons that can be learned from the experiences gained by IT security experts leading to the use of (after tailoring) some standard security tools and techniques to protect ICS. However, other standard security measures may be completely inappropriate or not available for use in a control system environment.

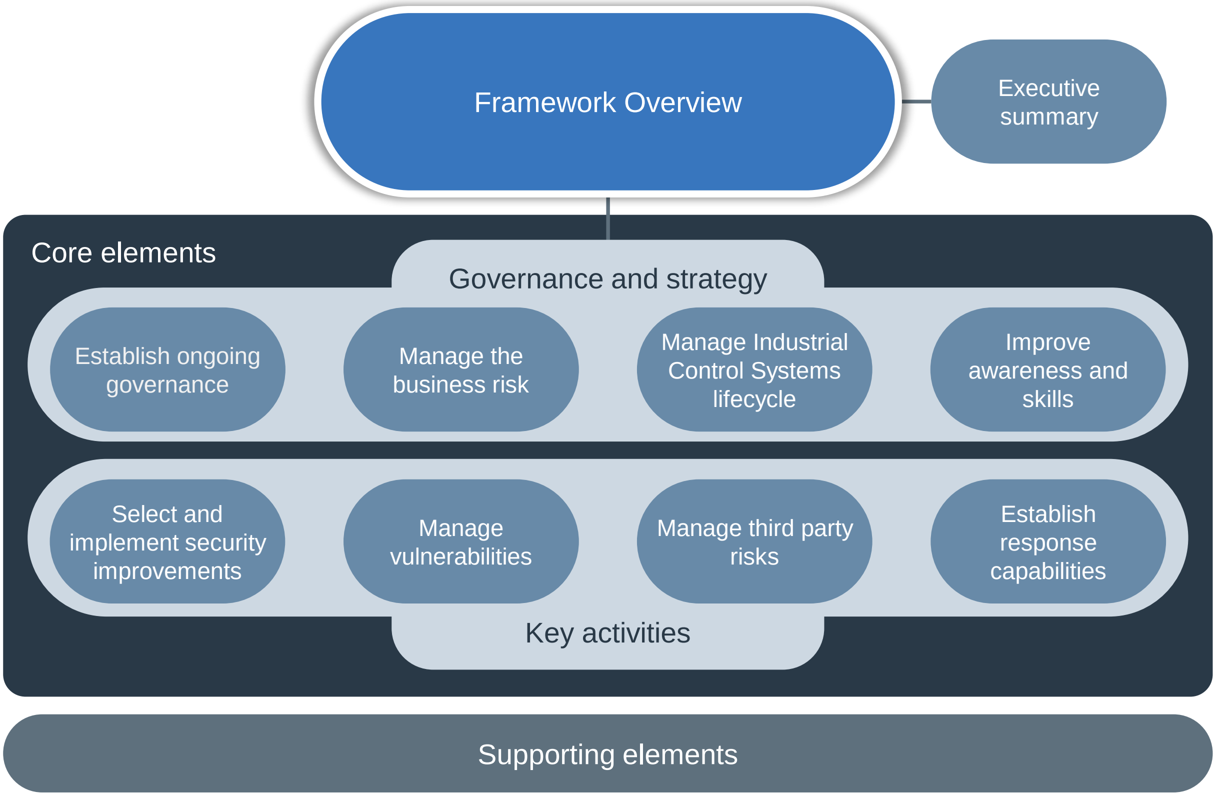
For example, it may not always be possible to install anti-malware protection on ICS, owing to the lack of processor power on legacy systems, the age of operating systems or the lack of vendor certification. In addition, security testing on ICS must also be approached with extreme caution as vulnerability scanning can seriously affect the operation of many control devices. Dedicated test environments are rarely available and there are few opportunities to take the systems off-line for routine testing, patching and maintenance.

This ICS security framework is based on industry good practice from the fields of ICS and IT security and aims to help organisations address the challenges of increased use of standard IT technologies in the ICS environment. The SICS Framework consisting of its core and supporting elements is intended to be a point of reference for an organisation to begin to develop and tailor the ICS security that is appropriate to its needs. The eight core elements of the framework are:

- Establish ongoing governance
- Manage the business risk
- Manage Industrial Control Systems lifecycle
- Improve awareness and skills
- Select and implement security improvements
- Manage vulnerabilities
- Manage third party risks
- Establish response capabilities.

The SICS Framework consisting of eight core elements and the supporting elements is shown below in Figure 1.

Figure 1- Where the Framework Overview fits in the SICS Framework



This document provides an overview of all the elements in the SICS Framework, with more detail on each provided in separate guidance documents. All the guides in the framework can be found on the CPNI website at http://www.cpni.gov.uk/advice/cyber/scada/.

A mapping of the SICS Framework to the NIST Framework – Improving Critical Infrastructure Cybersecurity v1.0 is available in Appendix B. This mapping shows where the NIST Framework elements are covered within the SICS Framework.

2.3 Guiding principles

Throughout the development of this framework, three guiding principles have been used. These principles are:

1. Protect, Detect and Respond

Constructing a security framework for any system is not just a matter of deploying protection measures. It is important to be able to detect possible incidents or attacks and respond in an appropriate manner in order to minimise the impact.

- **Protect** - Deploy specific protection measures to prevent and discourage cyber attack against ICS
- **Detect** - Establish mechanisms for rapidly identifying actual or suspected electronic attacks
- **Respond** - Undertake appropriate action in response to confirmed security incidents against the ICS.

2. Defence in Depth

Where a system uses only a single protection measure, any weakness in that measure could leave it exposed to attack. This means that organisations need to recognise that no single security measure is foolproof as vulnerabilities and weaknesses could be identified at any point. In order to reduce these risks, multiple protection measures in series should be implemented.

For example, in order to safeguard the ICS from electronic attacks (e.g. hackers, malware), it may be insufficient to rely on a single firewall, designed to protect the corporate IT network. A much more effective security model is to build on the benefits of the corporate firewall by adding a dedicated ICS firewall and deploy other protection measures such as anti-malware software and intrusion detection/prevention. Such a multi-layer security model is referred to as defence in depth.

3. Technical, procedural and managerial protection measures

When developing an ICS security plan there is a natural tendency to focus the majority of effort on the technology. Although important, technology is insufficient on its own to provide robust protection.

For example, when implementing a firewall it is not just a matter of installation and configuration. Consideration must also be given to associated procedural and managerial requirements:

- Procedural requirements may include change control and firewall monitoring
- Managerial requirements may include firewall assurance, standards, assurance and training.

3 ESTABLISH ONGOING GOVERNANCE

Formal governance for the management of ICS security will ensure that a consistent and appropriate strategy is followed throughout the organisation. Without such governance the protection of ICS can be ad-hoc or insufficient, and expose the organisation to additional risk. An effective governance framework provides clear roles and responsibilities, an up-to-date strategy for managing ICS security risk, and assurance that the supporting policies and standards are relevant and are being followed.

Organisations need to put in place ongoing governance for managing their ICS security risks, ensuring that current risks are appropriately addressed and that continuous review and improvement of the security posture takes place to reflect changes in the organisation and in its environment.

3.1 Objective

- To formally establish a governance framework to ensure that ICS security risks are managed consistently and appropriately on an ongoing basis.

3.2 Good practice principles

3.2.1 Establish governance and supporting organisation

- Obtain senior management support for ICS security management
- Identify any impacts of legal and regulatory requirements on ICS security
- Define roles and responsibilities for all elements of ICS security throughout the organisation
- Appoint a single point of accountability for ICS security risk. Depending on the size of the organisation this may be one person or it could be a number of regional points of accountability reporting into a single point.

3.2.2 Develop and implement the security strategy

- Define a strategy that aligns with the business and operational needs and that sets the objectives for ICS security and the actions to reach those
- Build the business case to support the ICS security programme
- Define, document, disseminate and manage, under change control, formal policy and standards for ICS security
- Ensure that the policy and standards accurately reflect the organisational requirements and support

business requirements
- Ensure policy and standards are agreed by all relevant parties.

3.2.3 Monitor the risks and ensure compliance

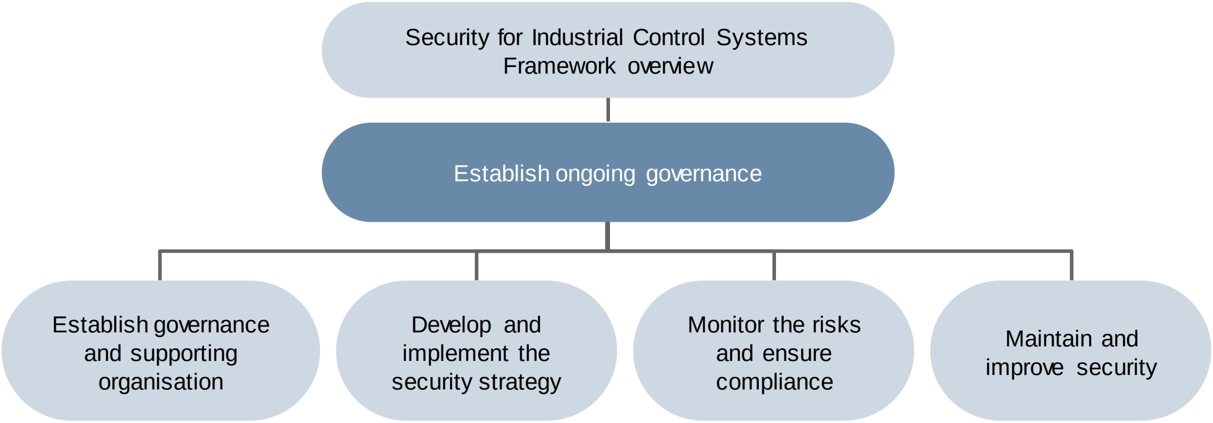
- Ensure the security strategy remains appropriate through monitoring the risks
- Implement an assurance programme to ensure that the ICS security policy and standards are complied with on a continuous basis.

3.2.4 Maintain and improve security

- Establish an ongoing programme to ensure that ICS security is maintained regularly and improved continually. This could take the form of annual reviews or a review prompted by changes in circumstances, such as changes in the threats or legal requirements.

Figure 2 shows the structure of this element as outlined in the detailed good practice guide, which can be found at http://www.cpni.gov.uk/advice/cyber/scada/.

Figure 2 - Structure of SICS Framework element ‘Establish ongoing governance’



Security for Industrial Control Systems Framework overview
Establish ongoing governance
Establish governance and supporting organisation
Develop and implement the security strategy
Monitor the risks and ensure compliance
Maintain and improve security

4 MANAGE THE BUSINESS RISK

A preliminary step in improving the security of ICS is to gain a thorough understanding of the relevant business risk. Business risk is a function of threats, impacts and vulnerabilities. Only with a good knowledge of the business risk can an organisation make informed decisions on the appropriate levels of security protection.

Managing the business risk is not a one off exercise – it is an ongoing process which is part of a wider risk management approach. Once a risk assessment has been conducted, the risk appetite defined and relevant security measures implemented for an organisation, it is important to maintain ongoing management of the business risk as this can change over time due to further identification of vulnerabilities and changes to the threat.

4.1 Objective

- To gain a thorough understanding of the risk that the organisation is facing in order to identify and drive the appropriate level of security protection required.

4.2 Good practice principles

4.2.1 Assess business risk

- **Understand the systems** - conduct a formal inventory audit and evaluation of the ICS.
- **Understand the threats** - identify and evaluate the threats facing the ICS. Possible threats may include: denial of service, targeted attacks, accidental incidents, unauthorised control, malicious code installed on machines, malware infections, phishing or social engineering.
- **Understand the impacts** - identify potential impacts and consequences to the ICS should a threat be realised. Examples of such consequences may include: loss of reputation, violation of regulatory requirements (e.g. health and safety, environmental), inability to meet business commitments or financial losses.
- **Understand the vulnerabilities -** undertake a vulnerability assessment of the ICS. Such a review should include: evaluation of the infrastructure, operating systems, applications, component software, network connections, remote access connectivity, physical security, personnel security and processes and procedures.

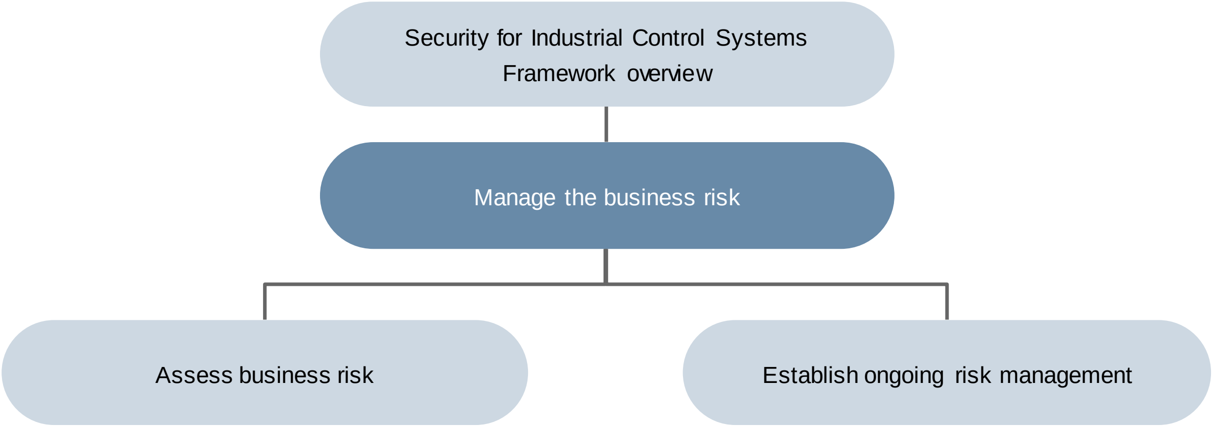
4.2.2 Establish ongoing risk management

- Business risk is a function of threats, vulnerabilities and impacts. Any changes to parameters (e.g. installing a new system) could change the business risk. Consequently, an ongoing risk management process is required to identify any of these changes re- evaluate the business risk and initiate appropriate security improvements.

Additional supporting guidance on risk management can be obtained in CESG - Risk management of cyber security in technology projects (see Appendix A).

Figure 3 shows the structure of this element as outlined in the detailed good practice guide, which can be found at http://www.cpni.gov.uk/advice/cyber/scada/.

Figure 3 - Structure of SICS Framework element 'Manage the business risk'


Security for Industrial Control Systems Framework overview
Manage the business risk
Assess business risk
Establish ongoing risk management

5 MANAGE INDUSTRIAL CONTROL SYSTEMS LIFECYCLE

Implementing security protection measures into systems is notoriously more difficult and costly to do once the systems have been built and deployed. The security provided by bolting on security measures to existing live systems may also be less effective than if it were included in the original design. Dealing with security risks early in the ICS lifecycle during the project development process and maintaining them during ICS operations can be more effective, avoids overruns, and usually reduces costs.

5.1 Objective

- To ensure all projects and operations that either directly or indirectly impact ICS assets follow a security engineering process throughout the ICS lifecycle, and incorporate appropriate security measures in their design, specification, and operation.

5.2 Good practice principles

5.2.1 Ensure security requirement included in procurement

- Ensure that prior to initiating any ICS related procurement, strategic efforts are made to align vendors in the supply chain to security expectations, including the security engineering process to be followed, and the expected security requirements of the ICS.
- Ensure standard security clauses, specifications, and selected risk reduction measures are incorporated in all procurement contracts.

5.2.2 Ensure ICS are secure by design

- Ensure that an ICS Security Subject Matter Expert is appointed to the project as a single point of accountability for security risk management and reporting, security engineering process management, and security design authorisation for the design phase of the ICS lifecycle.
- Ensure that all staff involved in the design phase of the ICS lifecycle have the appropriate level of security training and awareness, this includes sub-contractors and third parties involved in the supply chain.
- Include security requirements in the design and specification of projects and ensure that all appropriate security polices and standards are adhered to.
- Ensure the security engineering process contains sufficient security assurance gates to permit the review and authorisation of the security design at key points, and prior to the start of the next

lifecycle phase.

- Ensure all projects and operations that either directly or indirectly impact ICS assets follow a security engineering process throughout the ICS lifecycle.

5.2.3 Manage security through ICS construction

- Undertake security reviews throughout the build phase of the ICS lifecycle, for example, at the same time as health and safety checks.
- Ensure that all staff involved in the build phase of the ICS lifecycle have the appropriate level of security training and awareness, this includes sub-contractor staff and third party staff involved in the supply chain.
- Ensure that an ICS Security Subject Matter Expert is appointed to the project as a single point of accountability for security risk management and reporting, security engineering process management, and security design authorisation for the build phase of the ICS lifecycle.

5.2.4 Manage operational security

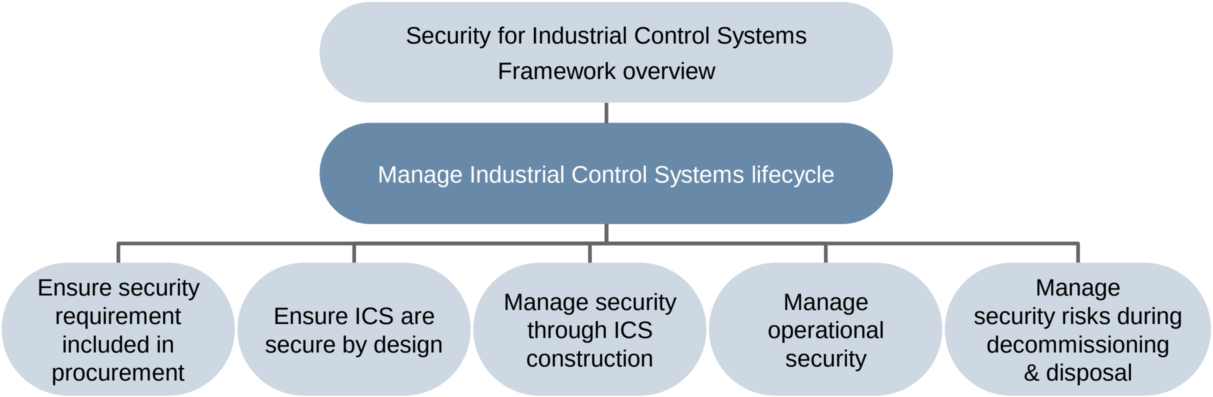
- Ensure that the management and operational elements of the ICS security controls are embedded into business as usual operations.
- Ensure that all staff managing or operating critical assets have successfully completed appropriate background checks and vetting which are maintained throughout the period they have access to the asset.
- Undertake security reviews throughout the operational phase of the ICS lifecycle, for example, at the same time as health and safety checks.
- Ensure all projects and operations that either directly or indirectly impact ICS assets follow a security engineering process throughout the ICS lifecycle.

5.2.5 Manage security risks during decommissioning & disposal

- Ensure that an ICS Security Subject Matter Expert is appointed to the project as a single point of accountability for security risk management and reporting, security engineering process management, and security design authorisation for the decommissioning and disposal phase of the ICS lifecycle.
- Ensure ICS and related material are disposed of securely, which should include erasing configuration profiles and secure destruction if appropriate.

Figure 4 shows the structure of this element as outlined in the detailed good practice guide, which can be found at http://www.cpni.gov.uk/advice/cyber/scada/.

Figure 4 - Structure of SICS Framework element 'Manage Industrial Control Systems lifecycle'


Security for Industrial Control Systems Framework overview
Manage Industrial Control Systems lifecycle
Ensure security requirement included in procurement
Ensure ICS are secure by design
Manage security through ICS construction
Manage operational security
Manage security risks during decommissioning & disposal

6 IMPROVE AWARENESS AND SKILLS

A holistic approach to security includes technical, procedural and social aspects and should recognise that the success of any of these security protection measures is ultimately dependent upon the human component. Employees are both the most important resource and the biggest threat to security. Yet ICS personnel are often unfamiliar with IT security and IT security personnel often lack knowledge of ICS and their operating environment. This situation can be improved by increasing understanding through general awareness programmes, education and by developing skills through training.

6.1 Objective

- To increase ICS security awareness throughout the organisation and to ensure that all personnel have the appropriate knowledge and skills required to fulfil their role.

6.2 Good practice principles

6.2.1 Increase ongoing awareness

- Engage with senior management to ensure that the business implications of ICS security risks are understood and therefore help achieve buy-in for management of these risks.
- Establish awareness programmes to increase general security understanding. These programmes should highlight security responsibilities, draw attention to current threats and increase vigilance.
- Communicate the business case to explain the need for the ICS security programme.

6.2.2 Establish training frameworks

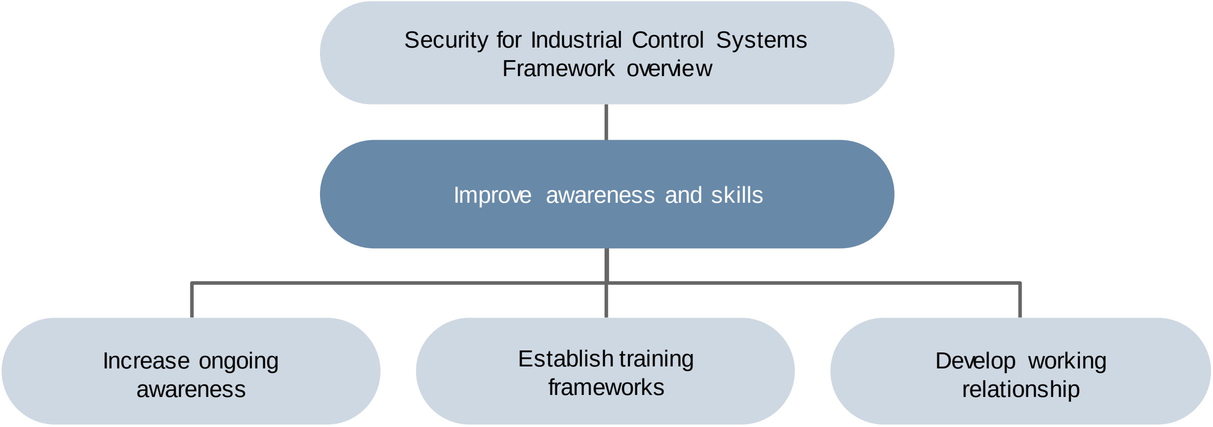
- Coach IT personnel to develop an appreciation and understanding of the ICS and their operating environments, highlighting the differences and similarities between the security of ICS and enterprise IT systems
- Develop IT security skills within ICS teams and provide appropriate IT support services to these teams.

6.2.3 Develop working relationship

- To establish links between IT security and ICS teams in order to build working relationships, share skills, and facilitate knowledge transfer.

Figure 5 shows the structure of this element as outlined in the detailed good practice guide, which can be found at http://www.cpni.gov.uk/advice/cyber/scada/.

Figure 5 - Structure of SICS Framework element 'Improve awareness and skills'


Security for Industrial Control Systems Framework overview
Improve awareness and skills
Increase ongoing awareness
Establish training frameworks
Develop working relationship

7 SELECT AND IMPLEMENT SECURITY IMPROVEMENTS

Based on the assessment of the business risk, organisations should select and implement technical, procedural and management protection measures to increase the security of ICS.

7.1 Objective

- To secure ICS by selecting and implementing technical, procedural and management protection measures commensurate with the business risk.

7.2 Good practice principles

7.2.1 Review risks and assess existing controls

- Form a cross discipline risk reduction team
- Review the business risks
- Assess the effectiveness of the current controls against the risks identified.

7.2.2 Define target state

- Agree the target risk profile for the organisation
- Develop a risk reduction strategy
- Map security measures to the risks.

7.2.3 Develop a risk reduction plan

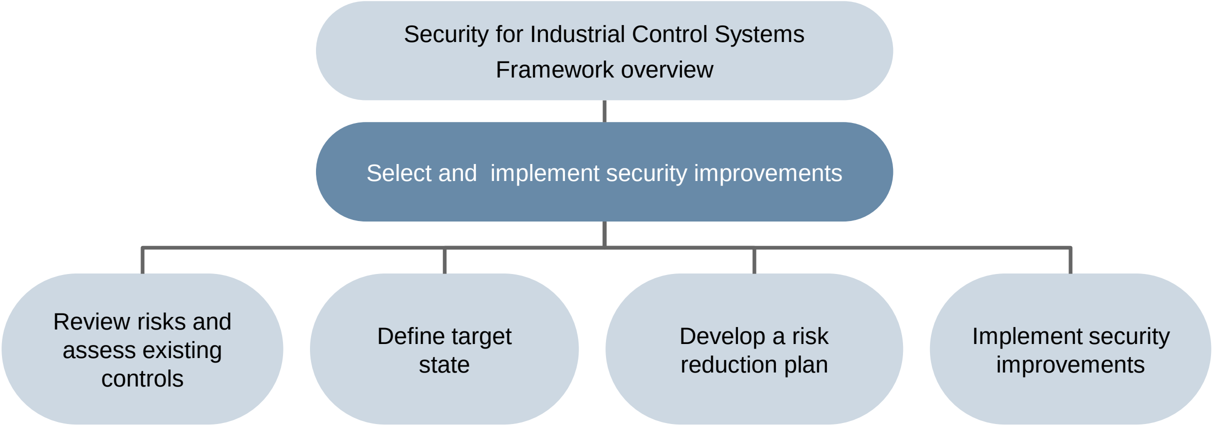
- Hold a risk reduction workshop to identify quick wins and long-term solutions
- Identify quick wins
- Form a risk reduction plan.

7.2.4 Implement security improvements

- Agree the implementation plan
- Implement security improvements.

Figure 6 shows the structure of this element as outlined in the detailed good practice guide, which can be found at http://www.cpni.gov.uk/advice/cyber/scada/.

Figure 6 - Structure of SICS Framework element ‘Select and implement security improvements’


Security for Industrial Control Systems Framework overview
Select and implement security improvements
Review risks and assess existing controls
Define target state
Develop a risk reduction plan
Implement security improvements

`

8 MANAGE VULNERABILITIES

Implementing vulnerability management across ICS is not a one-off exercise. ICS vulnerabilities develop and evolve over time and organisations should therefore continuously assess them. This includes identifying, evaluating and reacting to newly published vulnerabilities, changes in security threats and cyber security incidents. Establishing formal vulnerability management processes ensures that any new vulnerability or change to the threat landscape is identified as early as possible and any required corrective action is taken promptly.

8.1 Objective

- To establish the procedures necessary to monitor, evaluate and take appropriate action in response to newly published vulnerabilities and changes to the threat landscape.

8.2 Good practice principles

8.2.1 Monitor vulnerabilities and threat activity

- Implement a vulnerability management process to ensure that vulnerabilities are kept to a minimum in the ICS environment.
- Ensure that new published vulnerabilities affecting the technologies used in the ICS are known about through continuous monitoring of subscriptions to specialised information sources (including CERTs, ICS vendors, and those providing underlying software used in the ICS – e.g. Microsoft).
- Regularly assess the current threats to ICS. Such an assessment should include: monitoring the reports of similar ICS infrastructure in related sectors being targeted, drawing on open source intelligence or participating in special interest groups to determine whether the risk profile is changing.

8.2.2 Analyse impacts and review response options

- On detection of new vulnerabilities or changes in the threat landscape, the potential impact for the ICS environment should be analysed. If there is an impact, potential response options like security patching should be explored. Where security patching is not possible or practical, compensating controls should be considered.

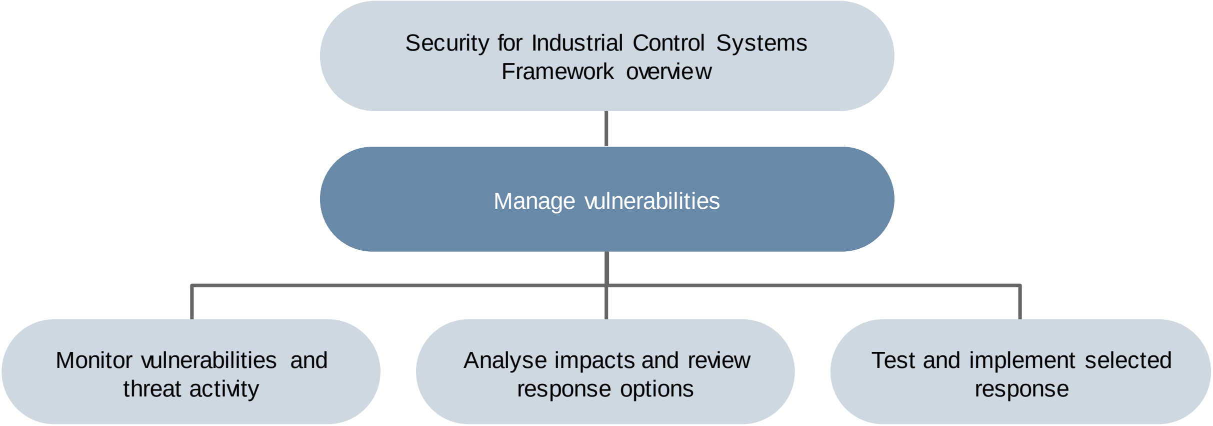
8.2.3 Test and implement selected response

- Implement processes for deployment of security patches to ICS. These processes should be supported by deployment and audit tools. The processes should make allowance for criticality assessment of patches, vendor certification of patches, testing of patches prior to deployment, and a staged deployment process to minimise the risk of disruption from the change. Ensure the security patching process can support patching in response to security alerts and incidents.

The ENISA document “Window of Exposure a real problem for SCADA systems” provides further details on this subject (see Appendix A).

Figure 7 shows the structure of this element as outlined in the detailed good practice guide, which can be found at http://www.cpni.gov.uk/advice/cyber/scada/.

Figure 7 - Structure of SICS Framework element ‘Manage vulnerabilities’



Security for Industrial Control Systems Framework overview

Manage vulnerabilities

Monitor vulnerabilities and threat activity

Analyse impacts and review response options

Test and implement selected response

9 MANAGE THIRD PARTY RISKS

The security of an organisation’s ICS can be put at significant risk by third parties, for example, vendors, support organisations and other links in the value chain. Technologies that allow greater interconnectivity, such as remote access or the internet, also bring new threats from outside the organisation. Managing these risks should receive significant attention, including engaging third parties to ensure they are taking steps to reduce these potential risks.

9.1 Objective

- To identify key third parties and effectively manage the associated risks that may have an impact on the security of an organisation's ICS.

9.2 Good practice principles

9.2.1 Identify third parties

- Identify all third parties, including vendors and service providers, and all other links in the value chain that are associated with the ICS.

9.2.2 Manage risk from vendors

- Ensure that security clauses are detailed in all procurement contracts prior to agreements and are cascaded down to sub-contractors.
- Engage with all vendors on an ongoing basis to ensure:
  - Current and future discoveries of vulnerabilities within the systems that they supply are identified and notified promptly to the user organisation
  - The organisation understands the security architecture of the ICS provided by vendors and how they may be supported remotely
  - Vendors understand the organisation's architecture in order to provide secure ICS.
- Request vendors to provide security guidance (including system hardening) for their current ICS and a roadmap for future system development utilising a secure development lifecycle (SDLC).
- Ensure that all vendors incorporate appropriate anti-malware protection within their ICS.
- Establish an effective software patching process with the vendor.
- Agree with the vendor system hardening procedures for the ICS in operation.
- Identify all component technologies (e.g. databases, open source software) used within the ICS to

ensure that all vulnerabilities are managed.

- Undertake regular security reviews and audits of all vendors according to risk based priorities.

9.2.3 Manage risk from support organisations

- Undertake regular risk assessments of support organisations and ensure any required countermeasures are implemented.
- Prevent access to the ICS by support organisations until appropriate measures to prevent or reduce potential security breaches have been implemented. Issue and agree a contract defining the terms of the connection.
- Engage with all support organisations on an ongoing basis to ensure all security incidents that may have a security impact on the organisation are reported.
- Increase awareness in all support organisations so they fully understand the ICS that they are supporting and agree to work in accordance with agreed security procedures.

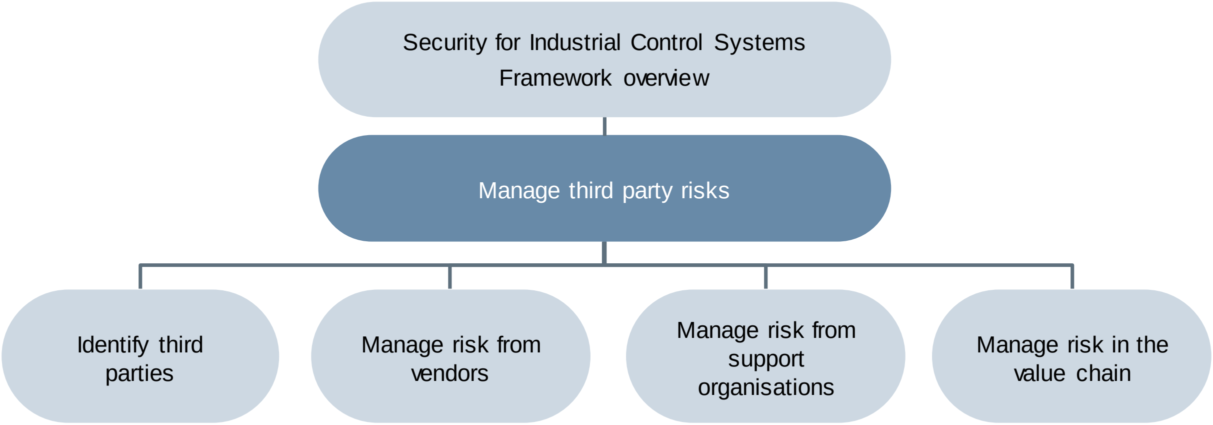
9.2.4 Manage risks in the value chain

- Ensure connections to any organisation in the value chain are secured on both sides and that the third party organisation provides assurance that their security risks are managed. Examples of such organisations include: suppliers, distributors, manufacturers, customers or joint ventures.

The DHS publication “Cyber security procurement language for control systems” provides further details on this subject (see Appendix A).

Figure 8 shows the structure of this element as outlined in the detailed good practice guide, which can be found at http://www.cpni.gov.uk/advice/cyber/scada/.

Figure 8 - Structure of SICS Framework element ‘Manage third party risks’


Security for Industrial Control Systems Framework overview
Manage third party risks
Identify third parties
Manage risk from vendors
Manage risk from support organisations
Manage risk in the value chain

10 ESTABLISH RESPONSE CAPABILITIES

Threats to the security and operation of ICS develop and evolve over time and organisations should therefore undertake continuous assessment of ICS security. This includes identifying, evaluating and reacting to new vulnerabilities, changes in security threats and cyber security incidents (e.g. malware or hacker attacks).

Establishing formal response management processes ensures that any changes to risks are identified as early as possible and any required corrective action is taken promptly.

10.1 Objective

- To establish procedures necessary to monitor, evaluate and take appropriate action in response to a variety of cyber security events.

10.2 Good practice principles

10.2.1 Form an ICS Security Response Team

- Form an ICS Security Response Team (ICS SRT) to respond to suspected security incidents. Representation should be drawn from a number of business areas including competent engineering staff familiar with ICS. A CNI company wishing to establish an ICS SRT can approach CERT-UK or CPNI for advice and support.

10.2.2 Integrate security response with other business response plans

- Ensure that appropriate cyber security response, business continuity, disaster recovery, and emergency plans are in operation for all ICS.
- Ensure that the cyber security response is integrated with other, business continuity, disaster recovery, and emergency responses.

10.2.3 Test and rehearse response capabilities

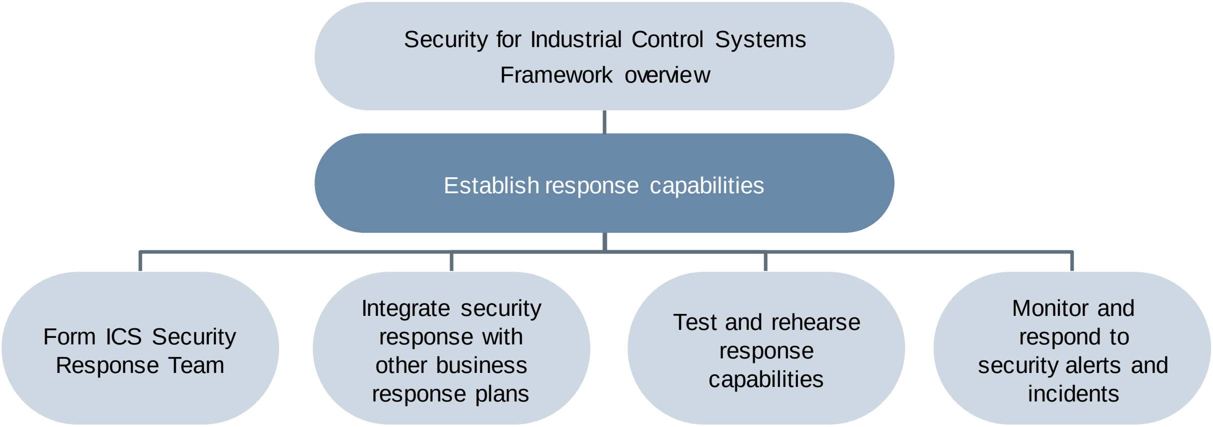
- Ensure that all cyber security plans are regularly maintained, rehearsed and tested.

10.2.4 Monitor and respond to security alerts and incidents

- Establish an early warning system that notifies appropriate personnel of security alerts and incidents.
- Establish processes and procedures to monitor, assess and initiate responses to security alerts and incidents. Possible responses may include: increase vigilance, isolate system, apply patches, or mobilise the ICS SRT.
- Ensure all ICS security incidents are formally reported and reviewed and that lessons learnt are captured and fed back in to the incident response process.

Figure 9 shows the structure of this element as outlined in the detailed good practice guide, which can be found at http://www.cpni.gov.uk/advice/cyber/scada/.

Figure 9 - Structure of SICS Framework element 'Establish response capabilities'


Security for Industrial Control Systems Framework overview
Establish response capabilities
Form ICS Security Response Team
Integrate security response with other business response plans
Test and rehearse response capabilities
Monitor and respond to security alerts and incidents

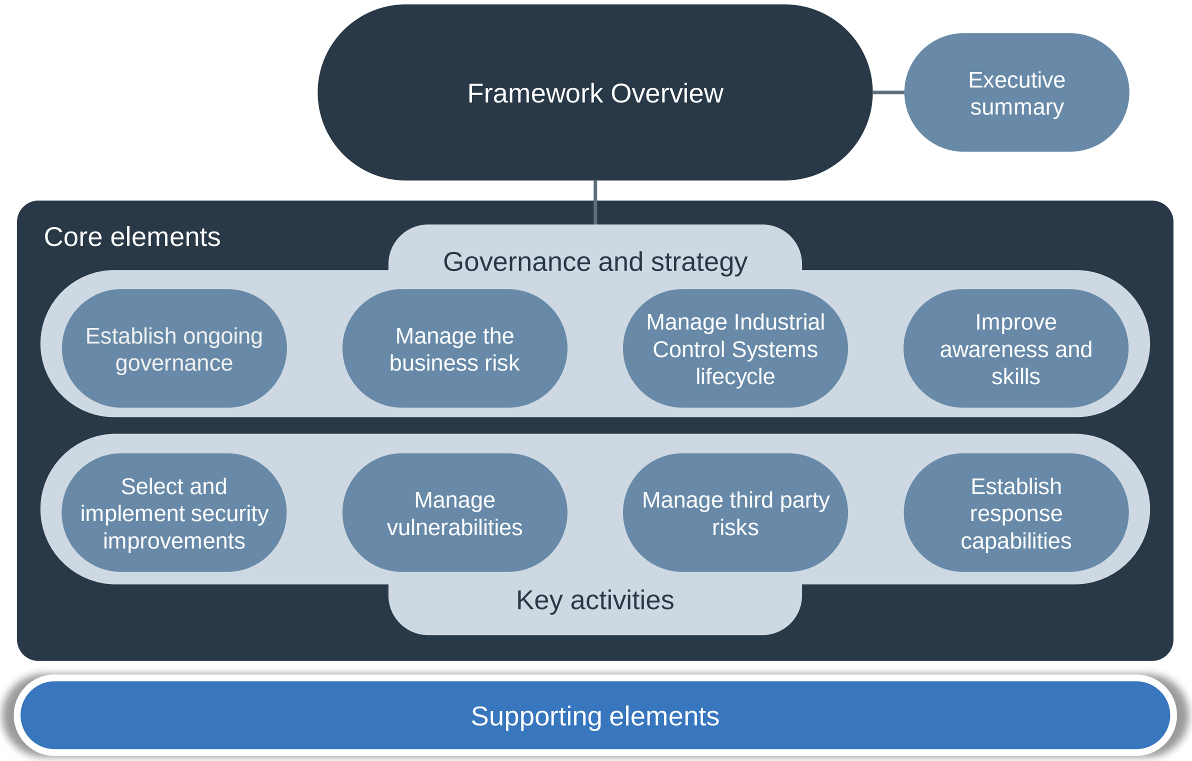
11 SUPPORTING ELEMENTS

The Security for Industrial Control System (SICS) Framework is made up of the eight core elements that are described in the previous sections of this document. To support the implementation of the SICS Framework, CPNI has also developed several supporting elements that provide:

- Additional targeted specialist guidance
- Supporting tools
- Training and communication materials.

The extended SICS Framework complemented with the additional supporting elements is represented in Figure 10.

Figure 10 – The core elements and their supporting elements



At the time of writing, the following documents constitute the additional available supporting elements that are dedicated to ICS security.

- **Firewall deployment for SCADA and Process Control Networks – A Good Practice Guide -** This guide sets out the current leading practices in ICS firewall deployment, including firewall architectures, deployment and management used to protect ICS.
- **Configuring and managing remote access to ICS** - This document provides guidance for developing secure remote access strategies for organisations that use industrial control systems. This document is for use in developing or updating strategies related to managing remote connectivity between operational assets, peers, vendors, operators and other elements that require access to critical information, devices or process data.
- **Cyber security assessment of ICS** - The guide provides an overview of the assessment process so users understand how to execute an ICS cyber security assessment. In addition to explaining actual security testing, it sets out the pros and cons of a number of alternate vulnerability testing methods so tests can be tailored to the specific ICS and the needs of the organisation.
- **Securing the move to IP** – This paper provides examples illustrating the challenges linked to the move to IP based networks. This document then describes the functional areas of ICS which typically used in the past analogue serial telecommunications technologies, those components which are impacted with the move to Ethernet TCP/IP communications; the security risks to consider when migrating to IP-based communications, and practical tips for ensuring the reliability and security of SCADA systems when leveraging Ethernet TCP/IP protocols and communications links.
- **SSAT (SCADA Self Assessment Tool)** – This is a tool to evaluate compliance against the principles developed in the Good Practice Guide.
- **E-Learning** – This online training module is designed to provide an introduction to the importance of ICS security and show how the Good Practice Guides can help improve security posture and mitigate the risk to organisations.

All these guides are available through the dedicated ICS security page on the CPNI website:

https://www.cpni.gov.uk/advice/cyber/scada/.

Other non ICS specific guidance is also available on the CPNI website: http://www.cpni.gov.uk/.

A DOCUMENT AND WEBSITE REFERENCES USED IN THIS FRAMEWORK

Section 2 Securing Industrial Control Securing Industrial Control Systems

NIST SP800-82 Guide to Industrial Control Systems (ICS) Security

http://csrc.nist.gov/publications/PubsDrafts.html#800-82r2

NIST Cyber Security Framework

http://www.nist.gov/cyberframework/

NERC Critical Infrastructure Protection (CIP)

http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Section 3 Establish ongoing governance

NIST SP800-82 - Guide to Industrial Control Systems (ICS) Security

http://csrc.nist.gov/publications/PubsDrafts.html#800-82r2

Section 4 Manage the business risk

CESG - Risk management of cyber security in technology projects

https://www.gov.uk/government/publications/risk-management-of-cyber-security-in-technology-projects/risk-management-of-cyber-security-in-technology-projects

ISO 31000:2009 Risk management – Principles and guidelines

http://www.iso.org/iso/home/standards/iso31000.htm

NIST SP 800-30 Guide for Conducting Risk Assessments

http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

AIChE - Guidelines for analysing and managing the security vulnerabilities of fixed chemical sites

http://www.aiche.org/ccps/publications/books/guidelines-analyzing-and-managing-security-vulnerabilities-fixed-chemical

HM Treasury Orange Book on Management of risks – Principles and concepts

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

Section 5 Manage Industrial Control Systems lifecycle

DHS - Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Environments

https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Using%20OpSec_v1_Draft.pdf

DHS - Cyber Security Procurement Language for Control Systems

https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf

Electric Power Research Institute - Cyber security Procurement Methodology for Power Delivery Systems

http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001026562

WIB - Process control Domain: security requirements for vendors - Version 2.0, October-2010

http://www.wib.nl/download.html

ISA Secure

http://www.isasecure.org/

CPNI and US DHS Cyber Security Assessment of ICS

http://www.cpni.gov.uk/documents/publications/2011/2011008-infosec-cyber_security_assessment_of_ics_viewpoint.pdf?epslanguage=en-gb

BS EN 15713:2009 Secure destruction of confidential material.

http://shop.bsigroup.com/ProductDetail/?pid=000000000030166950

Section 6 Improve awareness and skills

Guide to Industrial Control (ICS) Systems, SP800-82

http://csrc.nist.gov/publications/PubsDrafts.html#800-82r2

CPNI - ICS Security Practitioner / Manager Course, Incident Response Course

http://www.cpni.gov.uk/Contact-us/

GIAC - Global Industrial Cyber Security Professional (GICSP)

http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

CESG - CESG Certified Professionals (CCP)

http://www.cesg.gov.uk/awarenesstraining/certified-professionals/Pages/index.aspx

DHS Idaho National Laboratory (INL) - Advanced SCADA Security Red/Blue Team

https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT#workshop

IACRB - Certified SCADA Security Architect (CSSA)

http://www.iacertification.org/cssa_certified_scada_security_architect.html

Section 7 Select and implement security improvements

NIST SP800-82 Guide to Industrial Control Systems (ICS) Security

http://csrc.nist.gov/publications/PubsDrafts.html#800-82r2

CPNI - GPG Outsourcing: Security Governance Framework for IT Managed Service Provision

http://www.cpni.gov.uk/documents/publications/2006/2006027-gpg_outsourcing_it.pdf

Council on Cyber Security Council – Critical Security Controls for cyber defence

http://www.counciloncybersecurity.org/critical-controls/

CPNI - Firewall deployment for SCADA and Process Control Networks

https://www.cpni.gov.uk/documents/publications/2005/2005022-gpg_scada_firewall.pdf?epslanguage=en-gb

CPNI/ DHS - Configuring and managing remote access to ICS

https://www.cpni.gov.uk/documents/publications/2011/2011022-remote_access_for_ics_gpg.pdf?epslanguage=en-gb

IEC 62443-3-3 ed1.0 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

http://webstore.iec.ch/webstore/webstore.nsf/artnum/048406!opendocument

Section 8 Manage vulnerabilities

CPNI – iDATA programme

https://www.cpni.gov.uk/advice/cyber/idata/

ENISA - Window of Exposure a real problem for SCADA systems

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

ICS- CERT

https://ics-cert.us-cert.gov/

CERT-UK

https://www.cert.gov.uk/

MITRE CVE

https://cve.mitre.org/

CERT UK CISP – Cyber Information Sharing Partnership

https://www.cert.gov.uk/cisp/

CPNI – Information Exchanges

http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/

CPNI – Cyber Security Assessments of Industrial Control Systems

http://www.cpni.gov.uk/documents/publications/2011/2011008-infosec-cyber_security_assessment_of_ics_viewpoint.pdf?epslanguage=en-gb

CPNI – Good Practice Guide to Patch Management

http://www.cpni.gov.uk/Documents/Publications/2006/2006029-GPG_Patch_management.pdf

Section 9 Manage third party risks

Cyber Essentials Scheme

https://www.cyberstreetwise.com/cyberessentials/

CPNI - A Good Practice Guide on Pre-Employment Screening

http://www.cpni.gov.uk/documents/publications/2015/pre-employment%20screening%20edition%205%20-%20final.pdf?epslanguage=en-gb

CPNI - Personnel Security Measures

http://www.cpni.gov.uk/advice/Personnel-security1/

BS 7858:2012: Security screening of individuals employed in a security environment. Code of practice

http://shop.bsigroup.com/ProductDetail/?pid=000000000030237324

DHS - Cyber Security Procurement Language for Control Systems

https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf

CPNI - Outsourcing: Security Governance Framework for IT Managed Service Provision

http://www.cpni.gov.uk/Documents/Publications/2006/2006027-GPG_Outsourcing_IT.pdf

CPNI and US DHS - Configuring & Managing Remote Access for ICS

https://www.cpni.gov.uk/documents/publications/2011/2011022-remote_access_for_ics_gpg.pdf?epslanguage=en-gb

CPNI - A Good Practice Guide on Pre-Employment Screening

http://www.cpni.gov.uk/documents/publications/2015/pre-employment%20screening%20edition%205%20-%20final.pdf?epslanguage=en-gb

CPNI – Personnel Security Measures

http://www.cpni.gov.uk/advice/Personnel-security1/

Section 10 Establish response capabilities

CPNI – First Responders Guide

http://www.cpni.gov.uk/Documents/Publications/2007/2007011-First_responders_guide.pdf

CPNI – An Introduction to Forensic Readiness Planning

http://www.cpni.gov.uk/Documents/Publications/2005/2005008-TN1005_Forensic_readiness_planning.pdf

CERT UK CISP – Cyber Information Sharing Partnership

https://www.cert.gov.uk/cisp/

B MAPPING OF THE SICS AND NIST FRAMEWORKS

This mapping illustrates where elements of the SICS Framework address the cybersecurity activities highlighted in the NIST Framework - Improving Critical Infrastructure Security v1.0 (12th February 2014).

	Establish ongoing governance	Manage the business risk	Industrial control systems lifecycle	Improve awareness and skills	Select and implement security controls	Vulnerability management	Manage third party risks	Establish response capabilities	Firewall deployment for SCADA and process control networks	Configuring and managing remote access for industrial control systems	Cyber security assessment of industrial control systems
Asset Management (ID.AM)	●	●	●		●		●				
Business Environment (ID.BE)		●			●		●				
Governance (ID.GV)	●	●			●		●				
Risk Assessment (ID.RA)		●			●	●		●			●
Risk Management Strategy (ID.RM)	●	●			●						
Access Control (PR.AC)	●				●		●		●	●	
Awareness and Training (PR.AT)	●			●	●		●				
Data Security (PR.DS)			●		●				●	●	●
Information Protection Processes and Procedures (PR.IP)	●	●	●	●	●	●	●	●			●
Maintenance (PR.MA)			●		●		●			●	

	Establish ongoing governance	Manage the business risk	Industrial control systems lifecycle	Improve awareness and skills	Select and implement security controls	Vulnerability management	Manage third party risks	Establish response capabilities	Firewall deployment for SCADA and process control networks	Configuring and managing remote access for industrial control systems	Cyber security assessment of industrial control systems
Protective Technology (PR.PT)			●		●	●	●		●	●	
Anomalies and Events (DE.AE)			●		●	●		●	●		
Security Continuous Monitoring (DE.CM)					●	●		●			
Detection Processes (DE.DP)	●				●			●			
Response Planning (RS.RP)					●			●			
Communications (RS.CO)					●	●		●			
Analysis (RS.AN)					●	●		●			
Mitigation (RS.MI)					●	●		●			
Improvements (RS.IM)								●			
Recovery Planning (RC.RP)					●			●			
Improvements (RC.IM)					●			●			
Communications (RC.CO)					●			●			

C GLOSSARY

Accountability	Assigned to someone who is required or expected to justify actions or decisions. Accountability cannot be shared
Availability	Availability is a property or characteristic. Something is available if it is accessible and usable when an authorised entity demands access
CERT	Computer Emergency Response Team
CESG	CESG is the Information Security arm of GCHQ, and the National Technical Authority for Information Assurance within the UK
CISO	Chief Information Security Officer
CISP	Cyber Information Sharing Partnership
Confidentiality	Is a characteristic that applies to information whereby the protection of it is to ensure that it is not made available or disclosed to unauthorised entities
CPNI	Centre for the Protection of National Infrastructure
FAT	Factory Acceptance Test
Governance	The structure and processes by which organisations are directed and controlled
HMI	Human Machine Interface
HSE	Health, Safety and Environment
ICS	Industrial Control Systems
IDS	Intrusion Detection System
Impact	The magnitude of harm that can be expected to result from the consequences of an event
IPS	Intrusion Prevention System
Integrity	The accuracy and completeness of information
Likelihood	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities

Malware	Malicious software
NDA	Non-disclosure Agreement
Policy	Defines a general commitment, direction, or intention
Procedures	A way of carrying out a process or activity
Programme	A set of related measures or activities with a particular long-term aim.
PLC	Programmable Logic Controller
RACI	Responsible, Accountable, Consulted and Informed
Responsibility	Having an obligation to do something as part of a role. Responsibility can be shared.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event
Risk appetite	The level of risk that is considered to be acceptable by the leadership of the entity taking into account the balance of risk with corresponding costs or loss of opportunity
RTU	Remote Terminal Unit
SAT	Site Acceptance Test
SDLC	Secure Development Lifecycle
SICS	Security for Industrial Control Systems
SIEM	Security Information and Event Management
SME	Subject Matter Expert
SPA	Single Point of Accountability
SRT	Security Response Team
SCADA	Supervisory Control And Data Acquisition
Standard	Provides a documented and consistent organisational interpretation of how to achieve the desired goals of the defined policy
Strategy	A plan of action designed to achieve a long-term or overall aim
Sub-contractor	Person or entity that enters into a contractual agreement with a prime contractor to perform a service or task
Support	The ‘provision of capabilities for’ or the ability ‘to interface to’ the ICS. e.g. monitoring systems, resetting passwords, problems, bug fixes, etc.
Threat	Any circumstance or event with the potential to harm an ICS through unauthorised access, destruction, disclosure, modification of data, and/or denial of service
Value-chain	Organisations involved in the process of activities inherent to the operation of a company e.g. for an oil pipeline the value chain could include an oil refinery operated by another organisation

Vendor	A person, organisation or integrator that provides software, hardware, firmware and/or documentation to the organisation for a fee or in exchange for services
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source

ACKNOWLEDGEMENTS

PA are grateful for the support and input from CPNI, CESG, the ICS community and those involved with CNI protection during the development of this good practice guidance framework. Contributions have been gratefully received and are too numerous to mention individually here.

About the authors

PA Consulting Group
123 Buckingham Palace Road
London
SW1W 9SR

Tel: +44 20 7730 9000
Fax: +44 20 7333 5050

Email: info@paconsulting.com
Web: www.paconsulting.com

For further information from PA Consulting Group on Industrial Control Systems security:

Email: IndustrialCyberSecurity@paconsulting.com

Web: http://www.paconsulting.com/industries/energy/energy-and-water-cyber-security/