CESG

CPNI
Centre for the Protection of National Infrastructure

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

MANAGE INDUSTRIAL CONTROL SYSTEMS LIFECYCLE

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:

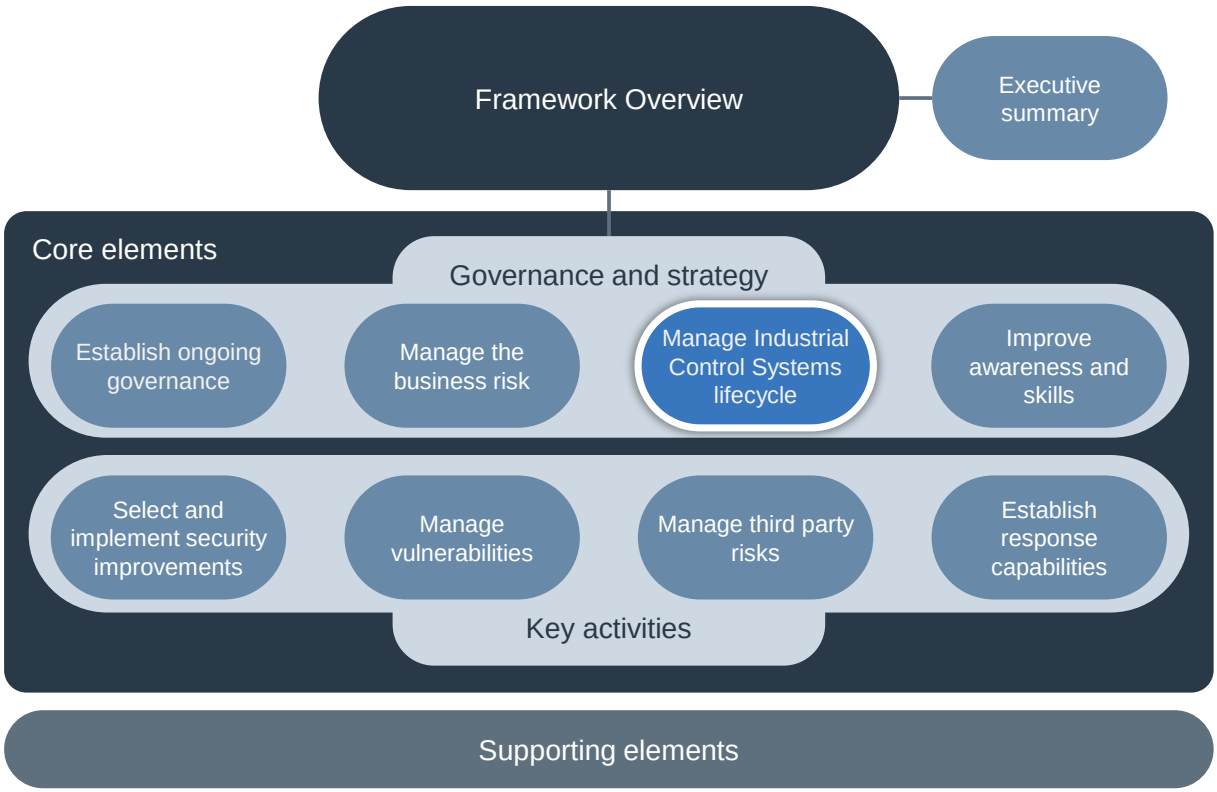
CONTENTS

1 INTRODUCTION

1.1 Framework context

The Security for Industrial Control Systems (SICS) Framework provides organisations with good practice guidance for securing Industrial Control Systems (ICS). This framework consists of a good practice guide Framework Overview, which describes eight core elements at a high level. This is supported by eight good practice guides, one for each core element and which provide more detailed guidance on implementation. Additional supporting elements of the framework provide guidance on specific topics. The framework, core elements and supporting elements are shown in Figure 1.

Figure 1 - Where this element fits in the SICS Framework



1.2 Manage Industrial Control Systems lifecycle - summary

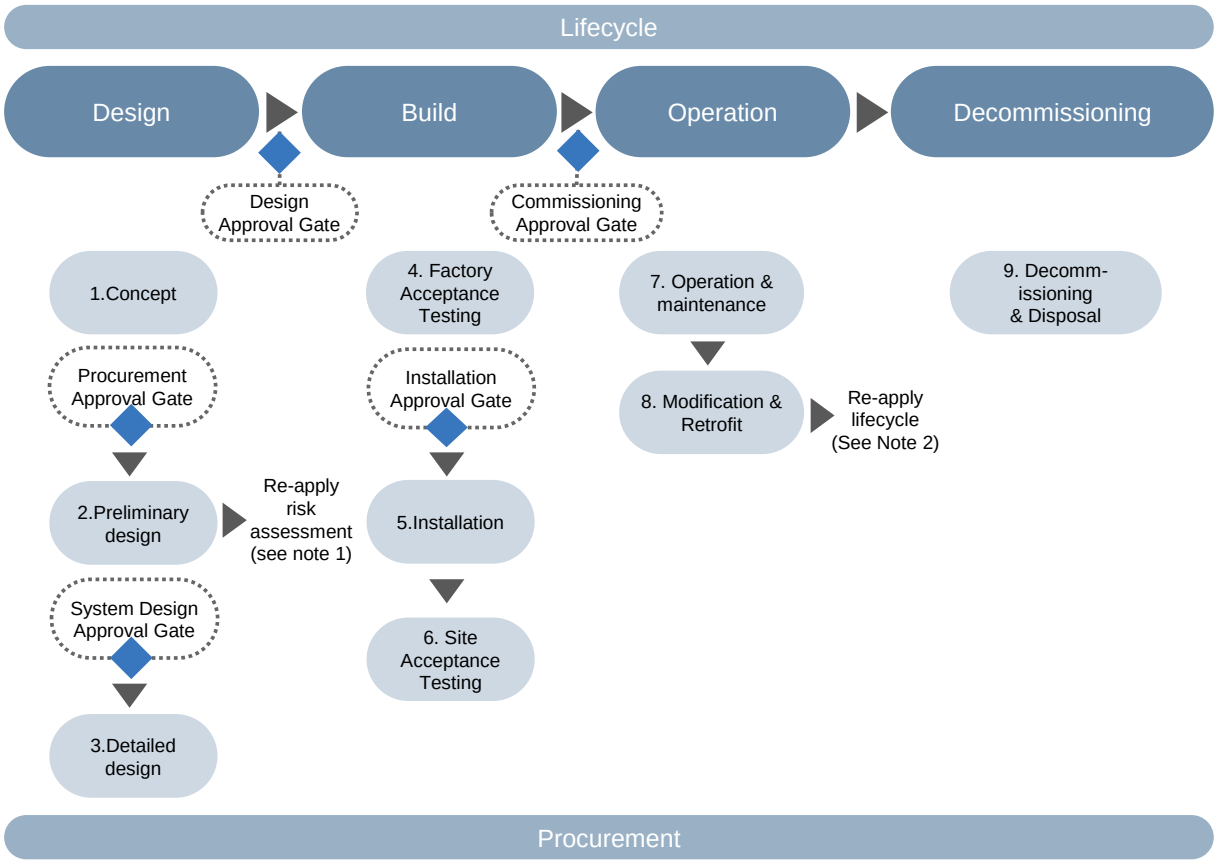
The objective of this guide is:

- 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.

ICS are usually installed with an expectation of a long service life. However, major renewals, modifications, and business integration needs mean that both during development and operation there are often a number of ICS related projects, any of which could have security implications. Consequently it is necessary to manage security through the entire ICS lifecycle, which consists of four key phases - design, build, operation and decommissioning (as shown in Figure 2).

Following risk assessment, any projects or operations that may affect ICS security should adopt an approach that builds-in and maintains security from an early stage. The assurance of these requirements should be assessed regularly throughout the ICS lifecycle. Any new system on a 'green field' site should build security requirements into the procurement, design, and build process from the outset. Subsequent operation of the ICS should maintain the effectiveness of this built-in security during the remaining service life of the system.

Figure 2 - The ICS Lifecycle



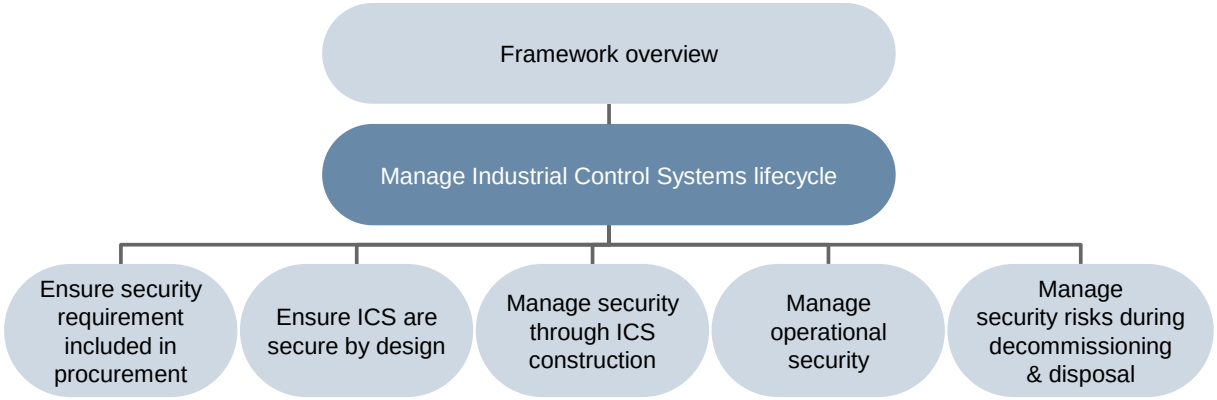
Note 1: Risk assessments may have to be repeated at several stages of the lifecycle.

Note 2: The phase at which a modification enters the lifecycle will be dependent upon both the system being modified and the specific modification under consideration

Implementing security protection measures into ICS can be more difficult and costly once systems have been built and deployed. Even more important bolting on security measures to an existing, live ICS, or late in its development, is often less effective than building them in at the beginning. Dealing with security risks by integrating protection measures into the ICS early in its lifecycle is more effective, avoids overruns, is usually less costly and can often be a business enabler.

To manage the ICS lifecycle within the organisation there are five good practice principles, these are shown in Figure 3.

Figure 3 – Good practice principles to manage the Industrial Control Systems lifecycle



By following the principles outlined in this guide, organisations should be able to manage their ICS security risks throughout the ICS lifecycle, ensuring that the security is maintained during any changes in the organisation and in its environment.

2 ENSURE SECURITY REQUIREMENT INCLUDED IN PROCUREMENT

Many organisations feel that vendors are not supplying them with secure ICS and vendors often respond by stating that security was never included in the contract requirements. Organisations need to work closely with vendors to ensure that both parties are aligned in their approach to security throughout the ICS lifecycle. Security requirements should be included in procurement contracts to ensure that both parties have clearly defined responsibilities, supported by contractual arrangements. These contractual arrangements should be included throughout the ICS lifecycle (as shown in Figure 2).

The relevant good practice in the overarching document 'Security for Industrial Control Systems – Framework Overview' is:

- 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.

2.1 Strategic alignment of vendors and the supply chain

In many industry sectors vendors continue to offer ICS solutions with little or no security function included, either because they feel the market does not yet require it, or because they lack the skills to do so. In the absence of regulation, organisations themselves must prepare the ground with vendors and the supply chain prior to procurement through effective dialogue about their security needs.

They can help vendors prepare to meet requirements in future procurements, for example, by adopting secure development processes, including security functions in systems and products and where appropriate teaming with existing security product vendors.

Prior to undertaking an ICS procurement, organisations should give serious consideration to implementing strategic initiatives to inform major vendors of their current and future security posture and how this will affect their ICS procurements. This may be done by individual organisations, or jointly via sector or cross-sector user or industry groups.

2.2 Build security requirements into contracts

Defining ICS security requirements that are informed by initial risk assessments and standards at the concept phase ensures that appropriate clauses are included within procurement contracts. This will ensure that vendors consider security as one of the fundamental requirements for the system and its delivery. This should include security aspects relating to the handling of data, drawings and information and not just the technology.

Security requirements provided during procurement should be used to assess the effectiveness of a vendor's security solution during the tender evaluation process. This ensures that vendors compete not only on the functional content but also security. It is not uncommon for major ICS vendors to omit the services of their own engineering security division in bids unless the client has specifically requested them during procurement. Including significant security measures in proposals when they have not been requested in the design requirements can mean a vendor's proposal is treated unfairly when assessing costs. Conversely requesting the security engineering service after the award of the contract will result in a significant increase in costs. By clearly stating security requirements in procurement contracts users can communicate their security expectations and can ensure a level playing field for competing vendors.

It is for this reason that single supplier procurements should be avoided, with preference given to tenders from multiple vendors to ensure supply chain resilience, and leverage the most economic security solution for the asset. Additionally the concept of trusted vendors can be used to build security into procurement contracts, inviting tenders only from vendors with an assessed and approved approach to security.

This approach to building security into procurement contracts should be reflected down the supply chain to the supplier's suppliers, and should cover not only the primary ICS being acquired but all associated equipment and all security activities such as:

- Security requirements for test and development tools and facilities
- Ensuring a supplier follows a secure development life cycle
- Ensuring a supplier carries out security testing and assurance
- Ensuring security integrity through secure custody of equipment and systems through delivery, installation, and commissioning
- Owner operator security testing and assurance during factory accepting testing and site acceptance testing (SAT), and commissioning validation and verification
- Future proofing by ensuring that contracts are outcome based and account for improvements in best practice and new standards.

Software coding errors can also create vulnerabilities. This is the case with control systems as well as IT software. Including coding for security as a clause within a procurement contract is necessary to ensure that the code is developed securely and has been tested.

Procurement contracts should refer to any policies or standards (internal or industry) to be followed in the system design and implementation.

Contracts should also contain sufficient detail about the security requirements that will be expected in the delivered system. However, it is important to do this to an appropriate level so that the contractual requirements are not too prescriptive. The contract should clearly state what requirements are mandatory and which are optional. For further guidance on what security clauses should be considered in contracts, see SICS Framework element 'Managing third party risk'.

In addition to stating the security requirements, procurement contracts should also clearly state the expectations for security assurance throughout the life cycle. Examples of these expectations are:

- Security design reviews or health checks
- Secure coding reviews
- Security testing
- Secure replacement and destruction of defective parts containing data (e.g. hard disks).

The decision to procure ICS should be a key assurance gate in the security engineering lifecycle. It should require the approval of the ICS Security subject matter expert to ensure the security risk, and security engineering process can be effectively managed during the project, and the concept security design is acceptable.

For details on typical concept phase security engineering activities refer to Table 1 in Appendix A.

Further guidance on security requirements can be found in the DHS Cyber Security Procurement Language for Control Systems[1] document and also in the Catalogue of Control System Security Requirements document produced by the DHS, and in the Cyber Security Procurement Methodology for Power Delivery Systems[2] from EPRI.

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

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

3 ENSURE ICS ARE SECURE BY DESIGN

Adding security to a system after it has been built is notoriously more expensive and difficult than incorporating security into the design of ICS. Security for ICS should be considered a core requirement in the design phase of the ICS lifecycle (see Figure 2) and not an optional extra. Embedding effective security requirements into the design stage should reduce the effort required to maintain security throughout the life of the ICS.

The relevant good practice in the overarching document 'Security for Industrial Control Systems – Framework Overview' is:

- 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 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.

3.1 Appoint an ICS Security Subject Matter Expert (SME)

Projects with ICS security implications should appoint an ICS security SME who will be accountable and responsible for security issues throughout the delivery phase of the control system lifecycle. The ICS security SME should be appointed at the beginning of the concept phase (Figure 2). This SME may only work part time, or may be in charge of a larger team, depending on the size of the project. They should be accountable for security risk management, security engineering process management, and security design authorisation and change control for the project. Within a larger team the Single Point of Accountability (SPA) can discharge security responsibilities to the team members as required.

Having an expert who can translate security requirements from policies and standards into a form that can be incorporated into the project specification can be extremely cost-effective. Building quality and accountability for security issues into the design and project life cycle ensures that ICS security

requirements are not forgotten and that the projects remain aware of the security implications of decisions.

3.2 Implement project staff security training and awareness

Projects with ICS security implications should ensure that all relevant project staff are trained, including those in the supply chain or other third party organisations who will contribute to the security of the ICS or interact with it during its development. This training should include raising awareness and internal certification to prevent security flaws or risks being introduced during the design, manufacture, and testing of the ICS.

These activities should be identified and planned for during the concept phase (Figure 2) along with any accreditation needed for particular security roles. The need for security training and awareness should be cascaded down the supply chain to sub-contractors and third parties via the procurement contract (see SICS Framework element 'Improve awareness and skills').

3.3 Build security requirements into design specifications

Building ICS security into the design and build process at the project stage seems obvious but is often overlooked or not done. Security requirements should be considered in the same way as any other functional requirements. They should be clearly expressed and included in any functional design specifications, and be subject to the same change control process.

It is important that security requirements for any system should be based on the business risk. A low risk system may require less security protection than one which is a higher risk or critical. If the level of business risk is not assessed then there is a danger that a system might be over protected (which could be a waste of resources that could have been better deployed elsewhere), or not protected sufficiently.

It should be expected that several iterations of security design with supporting risk assessments will be required to move from the preliminary design phase to the detailed design phase (Figure 2).

System security requirements should be considered during development along with how they align to an organisation's policy and standards. More detail is set out in the SICS Framework element 'Select and implement security improvements', 'Process control Domain: security requirements for vendors[3]' from the Working-party on Instrument Behaviour (WIB) and ISA Secure[4].

Further guidance on requirements can be found in the DHS Cyber Security Procurement Language for Control Systems[5] document and also the Catalogue of Control System Security Requirements[6] produced by the DHS.

3.4 System design security reviews

Once a project has progressed to a stage where there is a high level design and agreed architecture, it should be reviewed against the security specifications and requirements. At this stage the system will not yet exist but this review can be carried out in a similar manner to that for live systems but will be a paper-based exercise. Further guidance can be found in SICS Framework element 'Understand the business risk'.

The review should seek to identify any gaps that exist between the proposed design and the security requirements, specifications, policy and standards.

---

[3] http://www.wib.nl/download.html

[4] http://www.isasecure.org

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

[6] https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf

A key output of this review should be assurance that the design is compliant with the policy, standards, security requirements and specifications. Another output should be a list of security gaps and risks, which should be reviewed and incorporated in the design while the development is still fairly early in the life cycle, or accepted as residual risk.

It may be that a number of reviews need to be carried out at various stages of the development cycle. This will depend on how large and complex the system is and whether the implementation is happening in stages. Where possible these reviews should be incorporated within, or at least fed into, other system reviews that might already be in the implementation plan e.g. health and safety reviews etc.

Both the preliminary design phase and the detailed design phase of the ICS represent key assurance gates in the security engineering lifecycle, requiring the approval of the ICS Security SME. This will ensure the security risk, and security engineering process continue to be effectively managed during the project and the ICS system security design is acceptable and contains all the necessary requirements.

For details on typical preliminary design and detailed design phase security engineering activities refer to Table 1 in Appendix A.

4 MANAGE SECURITY THROUGH ICS CONSTRUCTION

Processes should be established to highlight, at an early stage, any projects that might have ICS security considerations. A register or inventory of projects involving ICS elements should be maintained. This is to ensure that the project development processes include a security engineering lifecycle so that all projects incorporate security into the development process.

The relevant good practice in the overarching document 'Security for Industrial Control Systems – Framework Overview' is:

- 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.

4.1 Test the system

There are a number of security aspects that should be considered as part of the overall testing plan. In ICS projects security testing is often not considered until the very late stages of implementation or not included at all. However, security testing very often finds unexpected vulnerabilities and it is important to identify these at an early stage of the life cycle.

Examples of project types which might have ICS security implications include:

- Firewall updates within the business
- Infrastructure upgrade or changes
- Connecting the office network to the internet
- Connecting the office network to the process control network
- Control systems upgrades or replacements
- New control systems
- Changes to operational procedures
- Information systems / historian updates
- Implementation of management information systems (MIS), manufacturing execution system (MES), production reporting systems or process historians

- Connecting third parties, e.g. for support services
- Changing embedded code (firmware).

Once an ICS is live it is very difficult to carry out security testing or vulnerability testing. There have been many documented incidents of security testing that has itself caused significant security incidents. Consequently there is great value in carrying out as much security testing as possible before a system goes live. The output of this testing can feed into a vulnerability management process for the system once it is in operation.

Consequently planning of security testing should start early on in the project and should consider a number of different areas which are described in the following sections.

During the various stages of system testing a baseline should be developed which will help confirm the security of the system as it was actually deployed and will aid in managing vulnerabilities in the future. This baseline should at least include:

- IP addresses (live should be treated as sensitive or consider using a test set)
- Network loading
- Ports, protocols and services
- Applications / Process running on hosts
- Typical operating parameters (e.g. CPU utilisation, network bandwidth etc.).

Unit testing: elements of security testing should be included throughout the ICS development cycle. Where systems are developed in sections or units it is likely that some functional testing of these units will take place. Some security testing should be planned into these unit tests to identify any issues at an early stage so they can be addressed early on in the life cycle before the issues are likely to cause significant impact.

Embedded systems testing: Over recent years, there have been investigations indicating widespread vulnerabilities in embedded systems such as low level controllers, Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). A widely quoted example is of a manufacturing firm that experienced significant disruption to its operations because an authorised security scan crashed many of the PLCs in its plant.

Many identified vulnerabilities are minor, but some are more serious and could have safety implications depending on how the devices are implemented. Consequently it is good practice to gain assurance about these devices prior to deployment into operations. There are a number of companies who provide security testing of PLCs and similar lower level devices.

At the time of writing there is no industry standard to perform this assurance against (although the International Society for Automation[7] (ISA) Working Group 4 are working on this) and there are no formal accredited bodies to perform this testing. However test tools are emerging which are dedicated to controller level testing. It is recommended that devices are tested using one of the available tools prior to being deployed. Where vulnerabilities exist that cannot be mitigated, compensating controls should be explored.

Factory acceptance testing: this provides an opportunity to test the full system before it goes into normal operations (when further testing becomes difficult) and should be carried out on the system as it will be installed. This stage is usually carried out at the vendor's premises and typically includes a variety of acceptance tests that would be carried out by the vendor / supplier, customer or by authorised third parties (on behalf of the customer). In instances where multiple systems' and vendors are involved, an integrated factory acceptance testing may be suitable. These tests are normally based on the functional requirements and specifications defined early in the project. Incorporating security into these tests is important because once a system has passed its acceptance tests it becomes very difficult to make changes to the system to correct any security issues.

[7] http://www.isasecure.org

Key topics that should be considered for inclusion in acceptance tests include:

- Security configuration (e.g. testing of firewalls, whitelisting and anti-malware)
- Software review
- Vulnerability scanning of the whole system
- Failover/ disaster recovery testing
- Backup testing
- Patch and update testing
- User accounts
- Remote access testing
- System hardening assurance (e.g. penetration testing)
- Ability to monitor the system (e.g. store and retrieve system logs).

The factory acceptance test represents a key assurance gate in the security engineering lifecycle, requiring the approval of the ICS Security SME prior to installation.

Commissioning / Site acceptance testing: following acceptance tests, the system is implemented into the live environment and typically a number of commissioning tests are carried out to verify that the system has been installed and configured correctly. Security tests should be included within these commissioning tests to confirm that the security elements have also been configured correctly. Integration testing should also be included where the system is part of a wider system.

The site acceptance test represents a key assurance gate in the security engineering lifecycle.

Further guidance on testing requirements can be found in the Cyber security assessment of ICS document by CPNI and US DHS[8].

4.2 Handover the system

Typically a large system development project is managed by a dedicated project team which is often separate from the operations team who will manage and maintain the system once it is in operation. As part of the process of handing over the systems to the operations teams all the associated process and procedures that are needed to support the security framework of the system need to be finalised and embedded into business as usual activities. Examples of these include:

- Account management and authentication
- Monitoring system logs
- Maintenance routines
- Firewalls management and monitoring
- Anti-virus deployment and assurance
- Response and continuity plans
- Change control procedures
- Fail-over testing
- Patching processes
- System isolation
- Loss of view procedures
- Ongoing assurance (see SICS Framework element ‘Understand the business risk’)
- Confirmation of all software on hard disks and firmware
- Up to date system documentation (network diagrams including links to ICS)

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

- Results of factory acceptance tests and commissioning tests.

Further discussion of this topic can be found in CPNI document 'Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments'[9].

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

5 MANAGE OPERATIONAL SECURITY

Once ICS are built and handed over, the effective management of the ICS security risk must be continued through the operational phase of the lifecycle. These security management activities and their respective processes and procedures must be defined and delivered as part of the project documentation, alongside any required operator training and support needed to implement them.

The relevant good practice in the overarching document 'Security for Industrial Control Systems – Framework Overview' is:

- 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.

5.1 Appoint a security manager

Operational areas with ICS security implications should appoint a manager who will be accountable for security issues throughout the operational phase of the control system lifecycle. This security manager may be responsible for one or more control systems and ensures that the delivered technical and managerial security controls for each system are monitored and maintained, to provide continuing assurance that the delivered system remains appropriately secured.

Having a security manager for the operational security risk who can monitor and maintain security controls provides clear accountability for the management of the ongoing business risk, and ensures the initial security investment is maintained in a cost-effective manner. Maintaining this accountability into the operational phase of the control system lifecycle ensures that ICS security remains effective.

The security manager should be appointed as early as possible, ideally at the beginning of the concept phase (Figure 2 - The ICS Lifecycle), and, in any case, no later than the preliminary design phase to ensure that the ICS security engineering solution is consistent with current and future operational capabilities.

See SICS Framework element 'Establish ongoing governance'.

5.2 Implement operations staff security training and awareness

Operational areas with ICS security implications should ensure that all operations staff, including third parties who will monitor and maintain the system or interact with it during operations, have the necessary training, awareness and internal certification to effectively maintain the security controls and implement the processes developed during the project phase.

The security training and awareness activities should be identified and planned for during the concept phase (Figure 2) along with any accreditation activities for particular security roles and completed prior to the operations and maintenance phase.

The need for security training and awareness should be cascaded down the operational support chain to sub-contractors and third parties via the procurement contract or operational support contracts.

More detail can be found in the SICS Framework element 'Improve awareness and skills'.

5.3 Operations and maintenance

The security manager should ensure that all security policies, procedures, plans and programs provided by the project team at handover are implemented during phases 7, 8 and 9 of the control system lifecycle. This should result in a number of significant security activities that will need to be maintained throughout the operations and maintenance phase of the ICS:

- Maintenance of access control plan
- Monitoring and assessment of security event logs
- Maintenance of security patch update programme (including endpoints and network infrastructure e.g. switches and routers)
- Maintenance of security signature update programme
- Maintenance of vulnerability management programme (see SICS Framework element 'Manage vulnerabilities')
- Maintenance of cyber incident management programme (see SICS Framework element 'Establish response capabilities')
- Maintenance of security and compliance assessments
- Maintenance of staff security and awareness training (see for SICS Framework element 'Improve awareness and skills)
- Maintenance of security risk assessments
- Maintenance of security during obsolescence programme (maintaining security functions while managing obsolescence introduces additional constraints)
- Maintenance and monitoring of adherence to the acceptable use policy
- Obsolescence management that would otherwise have security implications.

5.4 Modify systems securely

Prior to any modification including patching to a control system, the current security risks and those that may be introduced by the change should be carefully considered. It may be necessary to conduct a review of systems to capture undocumented modifications that may have been introduced to ensure a known baseline prior to any modification. Once the security risks are understood, the relevant design phases (Figure 2) are repeated to ensure that security requirements are once again embedded in the procurement process as part of the lifecycle.

The nature and magnitude of the changes will determine the starting point. For example, modifications to operational security policies and procedures may not involve redesign of the control system itself, but their potential impact on the overall security of the system means they should still be considered as a design change. All modifications should be made as part of a change management process.

6 MANAGE SECURITY RISKS DURING DECOMMISSIONING & DISPOSAL

When replacing equipment it is essential that the subject of decommissioning and disposal is adequately addressed. The decommissioning and disposal of ICS should be treated as a project by implementing a controlled configuration change in the same way as for modifications. Decommissioning ICS may introduce potential security risks which must be understood prior to the change being carried out. Decommissioning changes can often undermine the security controls of remaining assets where systems have been deployed with a high degree of integration and share security controls within zones or enclaves.

The relevant good practice in the overarching document 'Security for Industrial Control Systems – Framework Overview' is:

- 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.

6.1 Secure destruction

Many of these systems will contain sensitive information that could be of use to a wide variety of groups including business competitors, identity thieves, criminals and terrorists. The types of information include:

- Staff names and addresses
- Passwords
- User accounts
- Telephone numbers
- Product information
- Customer details
- Information falling under the Data Protection Act
- Technical specifications
- Chemical and biological data.

Terrorist groups are known to have shown interest in the last two areas.

Digital media needs to be overwritten with random data several times to make the original data irretrievable; this should include all addressable locations and not just the file allocation table.

Where overwriting cannot be used the media should be purged by degaussing with a strong magnetic field or destroyed.

Organisations can find more about disposal of assets containing sensitive information in BS8470[10].

[10] www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030127562

7 CASE STUDY: WATER CO.

7.1 WATER Co.: summary of previous developments

WATER Co. is a water company that operates in wholesale and retail on a regional scale. They have assessed their ICS security and selected and implemented security improvements using the SICS good practice guidance and are now looking to ensure they manage ICS security risks through the entire lifecycle. WATER Co. covers the whole water value chain from extraction of water through to treatment and distribution and retail to households and businesses. It does not undertake any waste water treatment.

The ICS environment supporting the operations is distributed across the region with facilities controlling abstraction from boreholes, several water treatment plants, reservoirs, booster stations and network control points across the transport and distribution network.

The technical infrastructure supporting those systems is quite mixed with a number of systems acquired over the years. An ambitious technology refresh project was going to start soon. This would address the need to renew some obsolete technologies and increase the real time analysis of operational asset parameters to optimise running costs and gain a more accurate view of demand across the region.

WATER Co. intended to manage their ICS security risk through ensuring security is built-in the design of new systems. This starts with the technology refresh project that is currently at concept stage and that should reach commissioning stage in about two to three years' time if funding is approved.

7.2 Improving security of legacy systems in operation

The implementation of interim security controls needed to be planned and take place as a matter of priority.

The interim security improvement project described the design of the target solution and developed an implementation plan covering:

- The testing of the solution in a test lab, the phased implementation of the technologies on a pilot site first before roll-out to the entire estate and the post implementation testing
- The target schedule of implementation with identification of the required resources in operations, IT and ICS teams
- The number of service interruptions required to implement the changes.

The organisation runs a strict Change Management Process as they have learnt the hard way that some of the old technologies they operate have little tolerance for deviation from "normal" operation. The first submission to the CAB was rejected as the implementation plan did not consider:

- The potential risks of disruption of operations while the changes are being implemented
- The need for roll-back plans in case of unexpected issues
- The necessary update of operational procedures for field engineers and the associated training requirements.

The interim security improvement project then presented a new plan incorporating those aspects and the CAB gave its approval for the change. In this second presentation the project manager requested that the Change Management Process should be improved by adding a topic on security and resilience implications of any change and by making the ICS security officer a permanent member of the CAB.

After successful implementation and validation, the asset and configuration database was updated and new operational procedures implemented.

7.3 Managing security through the design cycle of the technology refresh project

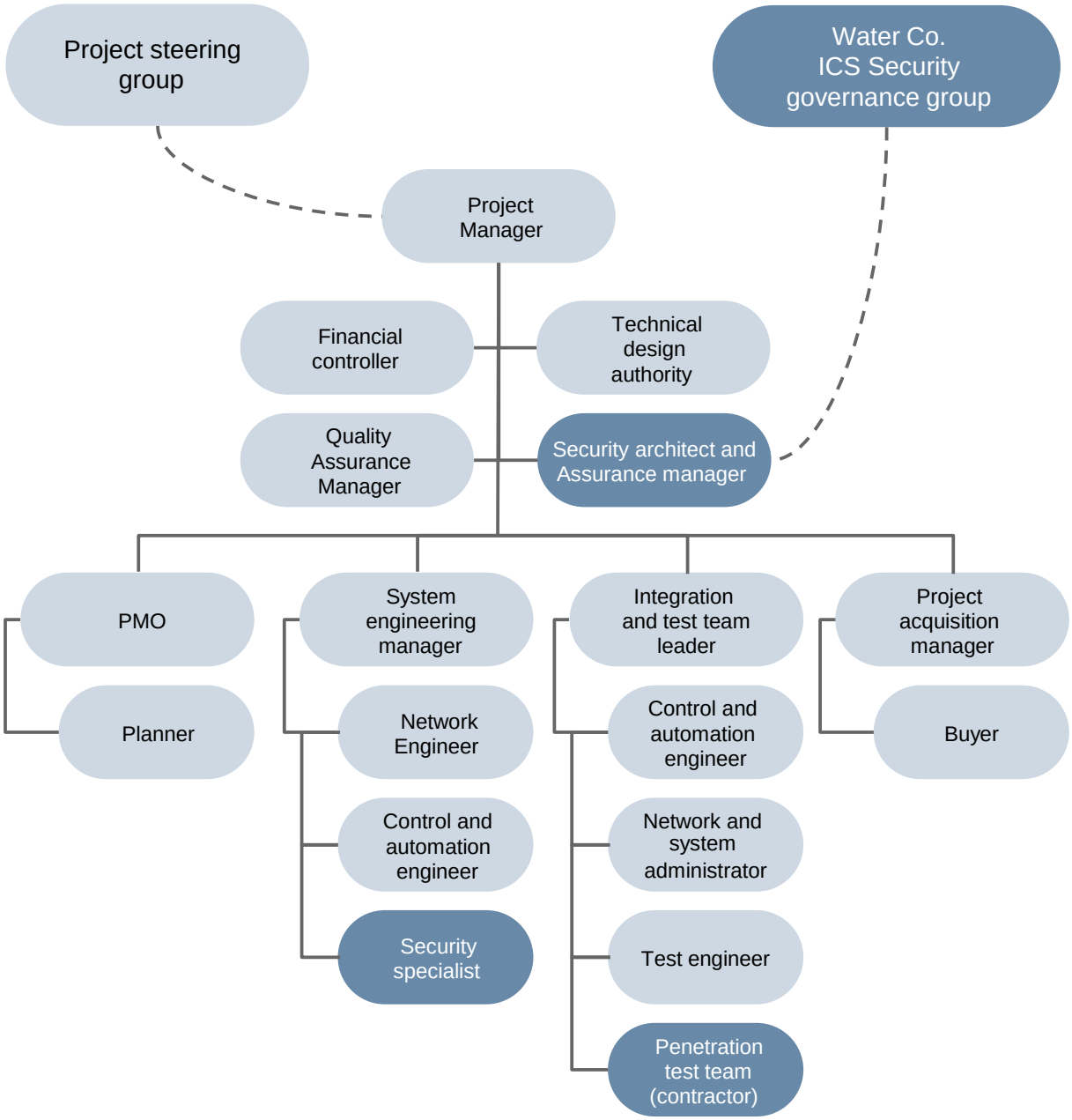
For this first major technology refresh project in more than ten years Water Co. decided to embed security from the outset of the project.

At the time of the initial concern emerging from the risk assessment the project was at the point of passing its first gate for entering into further definition and procurement. However, in light of those new cyber security considerations, the board of directors asked the project team to rerun their concept taking into account cyber security aspects.

With the help of a specialised consulting firm with experience in embedding security in large infrastructure projects the project team came back with a concept stage integrating:

- A high level risk assessment showing the status of risks on the target infrastructure
- First concepts of security mechanisms to be integrated in the infrastructure, the experience of the interim security solution project was precious at this stage
- A first cost estimate associated to the security solution (Capex and Opex) based on the experience of the consulting firm in comparable projects
- A business case showing the impact of security in terms of risk reduction (less disruption, fewer penalties from the regulator, less reparation to customers, fewer costs linked to managing incidents) and in operational benefits by allowing safe and secured access to live operational data to drive improvements and efficiency gains. A draft project management plan containing an OBS (Organisation Breakdown Structure) to include security, Figure 4
- A WBS (Work Breakdown Structure) clearly highlighting the positioning of security during project execution, with the following roles:
  - Security assurance
  - Security design
  - Security testing
  - Security operations plan.
- A revised System Engineering Management Plan showing how security would be integrated in the system design cycle and how it would be validated at the different design approval stages.

Figure 4 - Project OBS



The board of directors was satisfied and reassured that security would be given the level of attention it required and authorised the extra funding for security. They had expected a higher cost as they already had the experience of an interim security solution which was very expensive in proportion to its relative limited scope. This demonstrated to them that tackling security at the right time was more cost effective than trying to secure a system late in the design or indeed after installation.

They also recognised the beneficial impact of the advice from the consulting firm and decided to retain their services during the project phase to fill the security roles while security skills are being developed in Water Co.

A TYPICAL SECURITY ENGINEERING ACTIVITIES

The following table provides a list of typical security engineering activities mapped to the ICS lifecycle phases. It is by no means exhaustive, but it should inform the reader of the range of security engineering activities, and a set of baseline security activities for inclusion in a security management plan. This takes account of the business strategy, the policies, standards and guidance in the ICS security framework in order to develop a specific plan for the system, site or asset.

Table 1 Typical security engineering activities

ICS Lifecycle Phases	Typical Security Engineering Activities
Concept	• Review previously achieved security performance • Consider security implications of project • Review security policy and security targets • Define system and identify critical assets • Define initial (template) architecture diagram • Define initial zones and conduits • Define baseline security controls • Evaluate past experience data for security • Perform preliminary threat and vulnerability assessment • Establish security plan (overall) • Define tolerability of security risk criteria • Identify influence on security of existing infrastructure constraints • Perform system threat and vulnerability and security risk analysis • Set-up threat and vulnerability log • Perform security risk assessment based upon risk analysis • Refine baseline security controls • Produce security procurement language to include: refined security controls; initial (template) architecture; initial zones and conduits The security procurement language shall contain additional clauses to ensure that a secure development environment (including tools and development facilities) is established and ensure that a secure development process is applied. Additionally the security procurement language shall be reflected in all of the supply chain contracts, sub-contracts, policies and procedures.

Preliminary Design	• Specify system security requirements (overall) • Define security acceptance criteria (overall) • Define security related functional requirements • Establish a security management plan • Apportion system security targets and requirements: – Specify subsystem and component security requirements – Define subsystem and component security acceptance criteria • Update system security plan • Identify zones and conduits • Perform a risk assessment of each zone and conduit • Apply security controls until zone and conduit risks are mitigated or tolerable • Analyse security risk for each zone and conduit. • Update subsystem and component security requirements • Assign a target security level to each zone and conduit
Detailed Design	Implement security management plan by review, analysis, testing, and data assessment addressing: • Threat and vulnerability log • Security risk analysis and security risk assessment • Justify security related design decisions • Undertake programme control, covering: – Security management – Control of sub-contractors and suppliers • Prepare generic security case • Prepare (if appropriate) generic application security case • Include security controls in the design • Verify the design (achieved security level)
Factory Acceptance Testing	• Implement security plan by: review, analysis, testing, and data assessment • Use threat and vulnerability logs • Build the system as per the design • Validation - Factory Acceptance Test (FAT)
Installation	• Establish installation programme • Implement installation programme
Site Acceptance Testing	• Establish commissioning programme • Implement commissioning programme • Validate the security controls within the commissioning programme • Monitor the performance of the security controls throughout operational trials • Prepare application specific security case • Validation - Site Acceptance Test (SAT) • Assess application specific security case
Operations and Maintenance	• Undertake ongoing security centred maintenance • Perform ongoing security performance monitoring • Threat and vulnerability log maintenance • Collect, analyse, evaluate, and use performance and security statistics • Update the existing Security Management Plan
Modification	• Consider security implications for modification and retrofit • Depending on the extent of modification recommence the lifecycle at the concept, preliminary design, or detailed design phase
Decommissioning & Disposal	• Establish security plan • Perform threat and vulnerability analysis and security risk assessment. • Implement security plan • If the decommissioning activity is complex, treat it as a modification

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/