CESG

CPNI
Centre for the Protection of National Infrastructure

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

SELECT AND IMPLEMENT SECURITY IMPROVEMENTS

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 v1.1

Prepared by: PA Consulting Group Document reference:

CONTENTS

1 INTRODUCTION 2

1.1 Framework context 2

1.2 Select and implement security improvements – summary 3

2 REVIEW RISKS AND ASSESS EXISTING CONTROLS 4

2.1 Form a cross discipline risk team 4

2.2 Review the business risks 5

2.3 Assess current ICS security posture 5

3 DEFINE TARGET STATE 6

3.1 Agree target risk profile 6

3.2 Develop a risk reduction strategy 6

3.3 Map security measures to risks 7

4 DEVELOP A RISK REDUCTION PLAN 8

4.1 Hold a risk reduction workshop 8

4.2 Identify quick wins 8

4.3 Form a risk reduction plan 9

4.3.1 Consider the cost 9

4.3.2 Assess the strength of protection 9

4.3.3 Construct a business case 9

4.3.4 Evaluate the impact on existing systems 10

4.3.5 Assess the ease of implementation 10

4.3.6 Plan for delivery 10

4.3.7 Select solutions 11

5 IMPLEMENT SECURITY IMPROVEMENTS 12

5.1 Agree implementation plan 12

5.2 Implement security improvements 13

6 CASE STUDY: WATER CO. 14

ACKNOWLEDGEMENTS 20

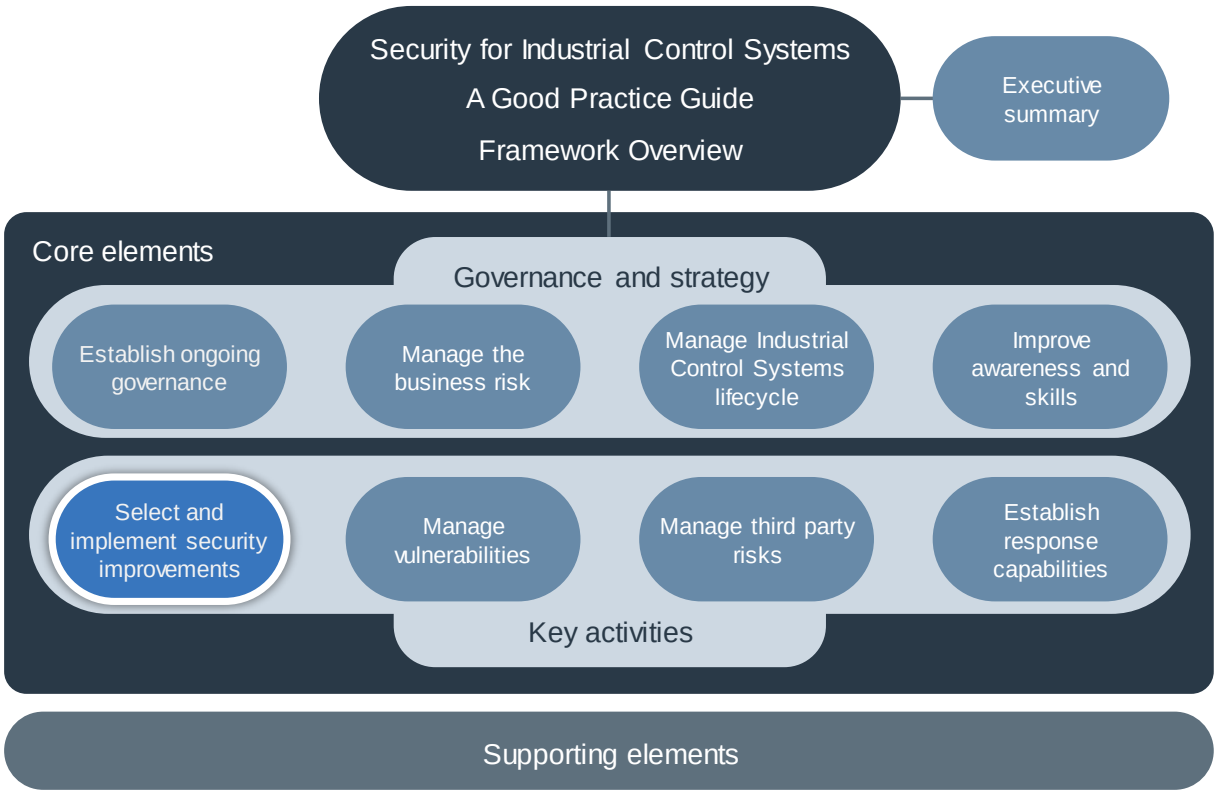
About the authors 20

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 Select and implement security improvements – summary

The objective of this guide is:

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

When securing ICS it is often easy to jump straight into implementing obvious security measures such as installing a firewall or deploying anti-malware software. However it is possible that such actions, if deployed indiscriminately, may not provide the best investment of valuable resources, such as finance and personnel. Consequently it is considered good practice to understand fully the risk faced by the control system before selecting and implementing protection measures so that available resources can be targeted in the best way.

In order to understand these risks, a risk assessment should be undertaken which assesses the ICS in scope and examines the threats, impacts and vulnerabilities that the systems face. This topic is described in more detail in the SICS Framework element 'Manage the business risk'. This risk assessment determines which are the most critical areas to address and provides the input for a selection process to ensure that the available resources are deployed in the areas where they achieve the best risk reduction.

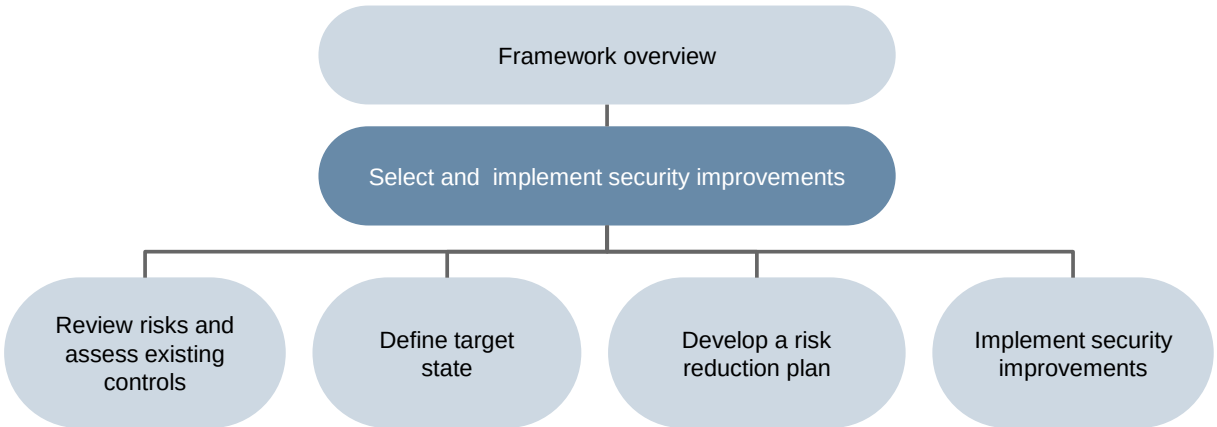
Once the business risk is well understood and a target state agreed then a suite of risk reduction (security improvement) measures can be selected to form an overall security risk reduction plan for each control system or site. A security risk reduction plan will consist of a variety of process, procedural and managerial protection measures and not just a suite of technical solutions.

Selecting ICS security measures is by no means an exact science and 'one size' definitely does not fit all. Owing to the wide variety of legacy systems in existence and of possible architectures, it is not just a simple straightforward matter of implementing an international standard. While, there are a number of existing industry standards and guidance that can be very useful in identifying security improvements, we are far from the position of merely being able to implement a single standard. Instead it is necessary to draw on a number of these standards and guidance frameworks to secure systems.

This document provides good practice principles and implementation guidance as shown in Figure 2:

- Review risks and existing controls
- Define target state
- Identify ICS security improvements
- Develop and implement risk reduction plans.

Figure 2 – Good practice principles to select and implement security improvements



2 REVIEW RISKS AND ASSESS EXISTING CONTROLS

Before deciding upon any security measures, it is important to have a good understanding of the business risk facing the ICS. When securing an ICS, it can be tempting to implement obvious security measures such as firewalls or anti-malware software without considering the wider risk landscape. This can lead to an inefficient use of resources with excessive protection in some areas and insufficient protection in others leaving systems insecure. However, with a good understanding of the business risk, appropriate security measures can be selected that are proportionate to the business risk.

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

- Form a cross discipline risk reduction team
- Review the business risks
- Assess the current ICS security.

2.1 Form a cross discipline risk team

To undertake the risk assessment and agree the risk reduction activities it is good practice to form a multidisciplinary team including representatives from the different impacted domains. This should include (but not be limited to) the following:

- ICS security Single Point of Accountability (SPA)
- ICS team members
- IT and ICS Security Architects
- Business representatives
- Operations team representatives
- IT security representatives
- IT infrastructure representatives
- IT application representatives
- ICS vendors.

2.2 Review the business risks

If a risk assessment has not already been carried out then one should be conducted at this stage (the Manage Business Risk element of the SICS framework provides guidance on how to conduct risk assessments at organisation and system/site levels). The output of this risk assessment provides an important foundation for the selection of security improvements.

If a risk assessment has been carried out previously, this assessment should be reviewed and updated if required.

2.3 Assess current ICS security posture

Having reviewed the business risks, organisations should conduct a gap analysis of the security measures against industry good practice. There are a number of good sources for this industry good practice. A selection of these are highlighted below.

NIST 800-82

NIST 800-82 is part of the NIST standards and guidance suite entitled “Guide to Industrial Control Systems (ICS) Security”. It provides an overview of ICS systems and types, typical architectures and configurations, ICS related threats and countermeasures to protect the systems. The document provides guidance on how the controls in NIST 800-53 can be applied to ICS. This guidance on controls can be used as a useful framework against which to carry out the gap analysis for assessing the current ICS security posture.

US Nuclear Regulatory Council Reg. Guide 5.71

Appendices B and C of this regulatory guidance document provide an interpretation of the security controls from NIST 800-53 which have been tailored for the industrial control systems domain.

US DOE Cyber Security Framework Implementation Guidance

This guidance provides a mapping of the NIST Cybersecurity Framework (2014) for possible implementation to energy infrastructures. This guidance maps ten cyber security and risk management domains used in the energy sector against the NIST Cybersecurity Framework (2014) and provides a method for assessing the maturity of cyber security protection of ICS.

IEC 62443

This emerging group of standards provides a holistic framework for the management of ICS security. IEC 63443-3-3-3:2013 section 4 describe the elements of management system against which the security of ICS can be assessed.

There are many other useful standards and sources of guidance available, including industry specific guidance, which may be useful providing a framework against which to assess the current ICS security posture.

The output of the current ICS security posture assessment should include:

- A list of vulnerabilities identified
- A list of gaps against industry good practices for which further assessment should be conducted
- Candidate short term ‘quick win’ and longer term security improvements that have been identified during the assessment and can be used as input to risk reduction planning.

3 DEFINE TARGET STATE

Once an organisation has assessed its business risks and current security position, the next stage is to define a target risk profile for the organisation and the strategy required to achieve this.

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

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

3.1 Agree target risk profile

It is important to agree a target risk profile that accurately reflects the risk appetite of the organisation and is based on the organisation's own strategic objectives and external influences. The profile should describe the organisation's desired cyber security outcomes.

The profile can be used to perform a gap analysis to identify areas where the organisation currently meets or exceeds aspects of the risk profile but also more importantly, areas where it falls short. These should be the main areas of focus for additional risk reduction measures to improve the security of the ICS.

3.2 Develop a risk reduction strategy

Once a target risk profile has been agreed it is useful to then develop a risk reduction strategy. This considers each of the risks and determines the high level action required. For each risk there are three types of action available:

- **Implement risk reduction measure** (or security control) – the remainder of this document considers the selection of these controls in more detail
- **Implement continuity plan** – this topic is covered in SICS Framework element 'Establish response capabilities'
- **Tolerate the risk** – the decision to tolerate a risk should be agreed by business leadership, recorded in a risk register and reviewed on a regular basis. These risks typically fall within an organisation's risk appetite and may be the residual risk following the implementation of secure measure. Under some circumstances a decision may be taken to tolerate a risk that exceeds the organisation's risk appetite for a period of time, for example prior to some planned change, but this decision should be tracked and monitored.

3.3 Map security measures to risks

In order to ensure that selected security measures properly address the risks identified in the risk assessment, it can be useful to map the security measures to the identified risks. For each risk, consider which of the security measures would reduce it. This will highlight any gaps where security improvements have not been identified for particular risks. Once this is done the security improvement measures can be assigned a priority, based on the business risk. This prioritisation can then be used in risk reduction planning.

4 DEVELOP A RISK REDUCTION PLAN

There are a number of widely published standard control sets that can be useful in securing ICS. However, many of these tend to be focussed on the IT environment rather than ICS where recommendations for implementation tend not to be easily applicable to ICS. So whilst these can be useful for securing ICS environments, they require careful interpretation and tailoring before adoption.

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

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

4.1 Hold a risk reduction workshop

Only once there is a good understanding of the business risk, can the main task of selecting possible protection measures to address each of the prioritised vulnerabilities proceed. This is often best done in a workshop where a number of parties with different views of the issues, can contribute to the selection of appropriate protection measures. The architecture selection should not be carried out by one person in isolation, as they are not likely to have a view of the entire system or knowledge of the issues from different perspectives.

The output from the risk reduction workshop should combine the actions to implement the security improvement measures and a secure architecture into a Risk Reduction Plan. The Risk Reduction Plan should contain quick wins and longer term risk reduction measures.

4.2 Identify quick wins

Quick wins are those risk reduction measures that are typically less complex, lower cost, and can be implemented in a relatively short period of time. The implementation of these measures allows an organisation to gain immediate benefits and reduce the gap between its current risk state and its target profile. An added benefit is that it can help gather support for longer-term solutions and reduce any resistance to change that may exist within the organisation.

4.3 Form a risk reduction plan

For each of the business risks and associated mapped and prioritised security measures, (see section 3.3) organisations should identify the actions required to implement risk reduction measures. Identified actions should cover the implementation of the technical, management and operational elements of the measures that will be required for effective implementation. They then need to assign a priority to each of the actions based on the business risk. These prioritised actions will form the basis of the Risk Reduction Plan.

Although the task of selecting security improvements may sound simple, it is often much more difficult than expected owing to the wide range of factors affecting the choice of controls each of which introduce their own constraints. The factors to be considered can be split into seven areas: cost, strength of protection, business case, impact on existing systems, implementation, delivery, and solutions.

4.3.1 Consider the cost

Some of the security measures may be relatively inexpensive, involving minor changes to the configuration of existing systems or minor modifications to existing working practices. However, the implementation of other security measures may require a new system or creation of new working practices or procedures that may involve additional capital or revenue expenditure.

The cost effectiveness of the solution needs to be considered against the strength of the protection measure and its ability to maximise the security benefits with a finite amount of financial resource. The ongoing operational cost of the security protection measure also needs to be considered over its life as this will provide a more accurate representation of its cost.

4.3.2 Assess the strength of protection

Assessing the strength of a security control can be difficult. However defining simple scales indicating the strength of controls can simplify the decision making process. The strength of the security controls (e.g. password vs. multifactor authentication) needs to be proportionate to the desired risk mitigation effect on operational impacts.

It also needs to be recognised that security is only as strong as the weakest link, so it is important that the weakest elements in the security architecture are identified and managed.

A guiding principle for security measure selection is to select an architecture that is based on defence in depth. Layers of security measures are more effective than a single security measure which would render the security architecture ineffective if compromised.

4.3.3 Construct a business case

It may be necessary to construct a business case in order to secure funding for ICS security improvements. This business case should clearly articulate the current risks and the need for security improvements. The content from SICS Framework element ‘Establish ongoing governance’ may be useful in constructing this business case. The case should also clearly show how the proposed investments would change the business risk profile for the ICS and should clearly articulate the residual risk.

The key elements of the business case are:

- An overview of the business risk profile (including the potential threats, impacts of incidents and vulnerabilities).
- The benefits of improved ICS security to the risk profile and the business. For example, availability of operational data in a secure manner to support operational efficiencies and asset management initiatives. These additional benefits should be included in the business case.
- Prioritised list of options and the basis of the recommendations
- The requirements for a security programme, key activities, resources and costs.

Further guidance on developing a detailed business case for security can be found in the NIST 'Guide to Industrial Control (ICS) Systems'[1].

4.3.4 Evaluate the impact on existing systems

When defining the target security solution, it is important to evaluate the impact that security will have on the systems and their operational use. Care should be taken to identify solutions that do not adversely affect the performance of the system, its usability, or key features like safety.

4.3.5 Assess the ease of implementation

Some security controls are easier to implement than others and may therefore be favoured by sites or organisations in the short term. For example, disabling a remote connection when it is not in use provides temporary protection and is easy to implement.

The implementation of some of the security measures may be quick because they may involve minor changes to the configuration of existing systems or minor modifications to existing working practices. However, the implementation of other security measures may involve the implementation of a new system or creation of new working practices or procedures and that can be time consuming.

Advice should be sought from vendors in determining the implementation plan, as some will support certain configurations and what works for one may not work for another.

Organisations also need to consider what testing of a security solution might be required before it can be deployed in a live ICS environment. Additional testing will add to costs and increase deployment timescales.

4.3.6 Plan for delivery

The implementation of some security controls may be constrained by monetary considerations or the staff resources available at a site level.

Organisations should therefore consider who would be responsible for the implementation of the security controls. In particular they should identify which measures will require the involvement of existing members of ICS staff and whether the staff identified can make any associated time available.

An organisation needs to consider both 'quick wins' and 'long-term' measures when selecting the appropriate architecture and implementation plan.

Security controls may take some time to implement (e.g. network redesign and firewall implementation) so it is important to consider simple and low cost interim measures, which can provide some increased protection in the short-term.

Relatively simple security measures that may be quickly implemented include:

- Better configuration of existing systems
- Anti-malware protection
- Tightening access controls
- Backup and restore capability
- Physical security
- Removal of unused connections.

When considering security measures, it is important to assess the existing expertise of staff as this may shape what security measures are delivered, and identify additional training requirements. Ongoing support and maintenance must also be considered as this may introduce additional remote access requirements, operational effort, or a need to upgrade hardware or software.

[1] http://csrc.nist.gov/publications/PubsDrafts.html

4.3.7 Select solutions

The risk reduction measures should be considered in terms of the defence in depth architecture as a whole i.e. a suite of measures not just point solutions.

Where possible, standard solutions should be used that are already available and organisations should aim for a common approach to minimise cost and complexity, and achieve other benefits. These approaches include:

- **Reuse proven solutions** – tried and tested architecture should be reused where applicable. This can simplify implementation. However, it should be noted that solutions already in place may not be appropriate or may need significant tailoring for use in the ICS environment.
- **Known quality standard** – reuse of existing solutions should ensure that the same level of quality is applied to ICS, for example, different parts or sites.
- **Ease of management** – incident response and support can be improved where consistency exists in ICS solutions.
- **Economies of scale** – using a standard solution may result in greater purchasing power and some influence over security design improvements.
- **Skills and expertise** – efficiencies in training and support can be achieved where standard solutions are applied.
- **Diversification** - may be required for critical systems to mitigate the impact of common vulnerabilities where standard solutions are not desirable.

Where available, consideration should be given to adopting solutions approved by the ICS system vendor. These solutions should have undergone detailed integration and accreditation by the vendor but assurances about testing and accreditation should be sought.

Selection of security controls should be based on risk. There is no point in investing in a strong and expensive security measure for a low risk threat or a minimal impact event when the investment could be better deployed elsewhere.

The selection of a secure architecture is not just concerned with technical measures; the associated processes and the procedural and management requirements also need to be considered.

Where possible, organisations should consider using services and solutions that are already available, for example those provided by the IT department. Solutions may need tailoring to the operating environment of ICS, for example phased deployment of anti-malware updates which may require additional testing.

When drawing up the possible security controls, there is a need to develop a number of different options or scenarios, with different strengths or possibly different costs. This might aid the financial decision making process.

Where services are not available in-house consider sourcing these from third parties. Examples of possible external services are:

- Firewall management and monitoring
- Networks and telecommunications management and monitoring
- Infrastructure management and monitoring
- Server management and monitoring

Further details on outsourcing can be found in the CPNI guide, ‘Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision’2. This guide is a general document and is not specific to ICS.

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

5 IMPLEMENT SECURITY IMPROVEMENTS

Having identified the security controls required it is necessary to develop a plan for implementing those controls.

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

- Agree the implementation plan
- Implement security improvements.

5.1 Agree implementation plan

Once a security risk reduction plan has been agreed, and approved, then the next task is to define the implementation plan. The implementation of security improvements in an ICS environment can be complex and there can be a significant risk of system disruption caused by the implementation of security controls. Careful planning is needed to minimise the risk of disruption to systems operation and deployment testing should be considered prior to implementing measures in the live environment. Rollback plans should be included within the implementation plans in case problems are encountered.

Factors to consider in implementation planning are:

- **Prioritisation of systems** – the most critical systems should generally be addressed before less critical systems however the vulnerability of the system should also be considered.
- **Costing** – it may not be possible to deploy all the risk reduction measures at the same time owing to budget pressures. In this case interim security measures should be considered.
- **Resource availability** – the personnel required to implement the security controls are often in very short supply. Often there are few personnel with the appropriate skills and frequently there are requirements for them to work on other competing initiatives. Consequently the implementation plan is often impacted by the availability of appropriate resources.
- **Rate of change limit** – there is a limit to the amount of change that businesses can absorb at any one time. In order to maintain a low risk and orderly deployment it is important that the implementation plan is not too aggressive.
- **Implementation approach** – risk reduction measures can be implemented using a direct approach (immediate adoption), a parallel approach (immediate adoption but with fall back), or a phased approach (adoption at different times). For large or complex plans a phased approach should be considered to minimise the risk of implementation problems.
- **Dependencies** – the implementation plan should consider all the dependencies identified. Some of these have already been mentioned (e.g. resources) however there may be some risk reduction

measures that are prerequisites to others. An example could be the removal of modems which might be dependent on an alternative means of secure remote access being in place first.

- **Training plan** – the implementation plan should also cover all the requirements for training. This should not just include the needs for the technicians deploying solutions but also support and maintenance personnel and all users and operators of the systems.
- **Communications and awareness** – the implementation plan should include the required communication and awareness elements to inform the relevant parties of the changes taking place.
- **Procedure development and testing** – the implementation plan should also include the development of all the associated procedures that support the security controls. It should be noted that it is not just a case of writing and publishing these procedures; often a significant amount of effort is required to embed these into day to day activities.
- **Testing** - the implementation plan should include all the relevant elements of testing. This includes integration testing, deployment testing and assurance that the measures have been implemented correctly. This might take the form of a formal security audit or post-implementation review.

5.2 Implement security improvements

The implementation of security controls can proceed only once the implementation plan has been completed, reviewed and signed-off. Throughout the implementation process there are a number of areas to consider:

- **Change control** – all changes to ICS should follow an appropriate change control process as these changes may impact both the ICS and IT systems. Further down the value chain the changes might need to be managed under different change control process such as for the plant systems and for the IT systems. As changes are made, the change control process should ensure that the system diagrams, inventory and risk assessments are updated. If not then the process should be modified or checks undertaken to ensure all information is up to date. In addition, the security aspects of changes triggered by operational needs should be considered when managing changes.
- **Post implementation reviews** – once the security controls are implemented, an assurance exercise should be undertaken to ensure that the controls have been deployed in accordance with the design of the security architecture. This could take a variety of forms, from an implementation checklist to full security reviews or audits. Penetration testing should only be done under strict conditions (e.g. plant shutdowns) as it is not uncommon for this type of test to shutdown ICS and corrupt process plant controllers. It is also possible to assess the risk reduction achieved by the implementation of controls and to ascertain whether it sits within the organisation's risk appetite.
- **Communications and awareness** – throughout the implementation process it is important to provide appropriate communications. This ensures that all relevant stakeholders are aware of the latest status and developments in the implementation project.

The job of ICS security is not finished when all the risk reduction measures have been implemented to form the complete security architecture. This is only one milestone in the ICS security lifecycle. There is an ongoing task to ensure that the ICS remain appropriately secured into the future. This is further described in SICS Framework Element 'Manage Industrial Control Systems lifecycle'.

6 CASE STUDY: WATER CO.

Water Co. is a water company that operates in wholesale and retail on a regional scale. They cover the whole chain from abstraction of water through treatment and then distribution and retail to households and businesses. Water Co. does not run any waste water treatment as part of their operations.

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.

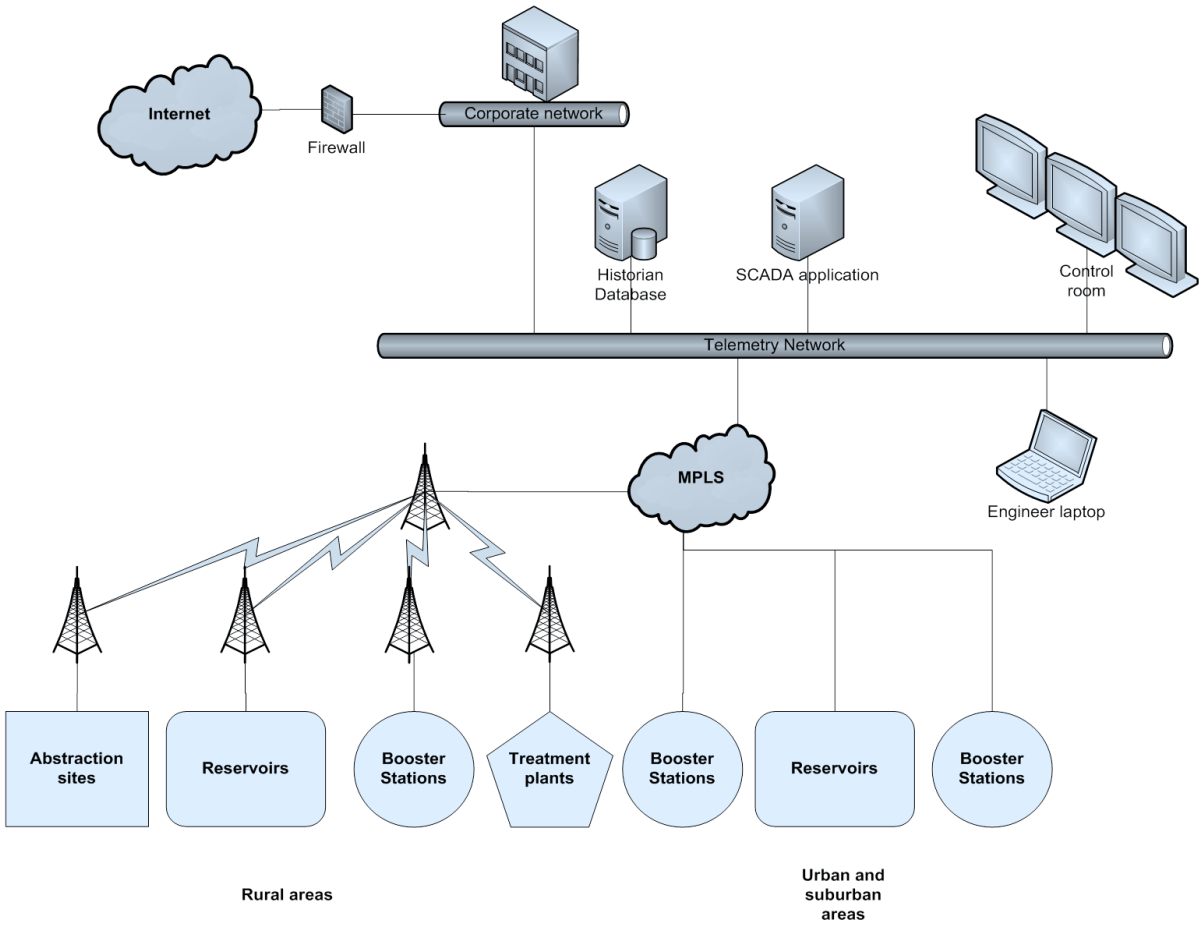
The technical infrastructure supporting those systems is quite heterogeneous with systems which have been acquired over the years. An ambitious technology refresh project is going to start soon. This project responds to the need to renew some obsolete technologies and increase the real time analysis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

Water Co. have performed a risk assessment and established a security governance structure. Water Co. have now a clear view of the business risk that their relatively insecure ICS environment is creating and the governance group has decided to address this without any further delay through a two phase security programme:

1. Mitigating critical and major risks on the existing legacy architecture until the new system technology refresh project delivers its outcomes
2. Ensuring that in future, security is built-in the design of new systems starting 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.

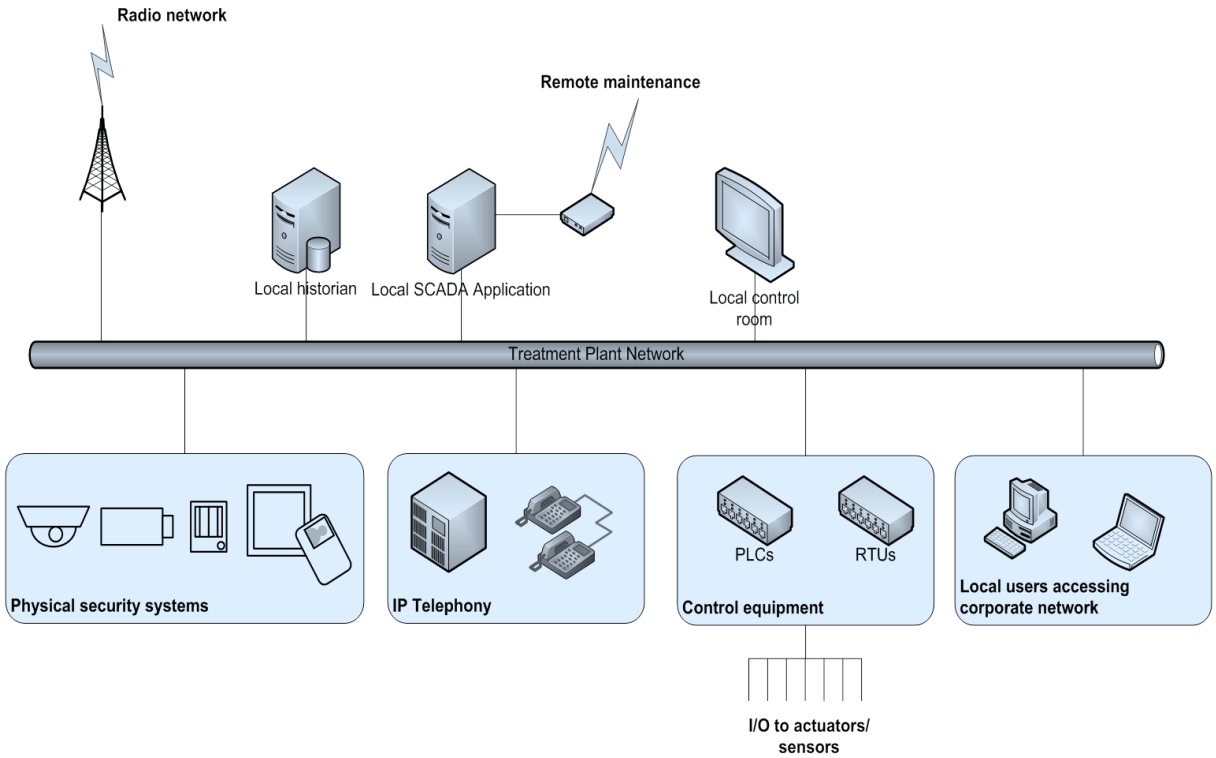
The Water Co. current regional architecture is described below.

Figure 3 - Water Co Regional Network



One of Water Co. main sites is described below:

Figure 4 - Water Co water site



A high number of security gaps have been identified during the risk assessment, including:

- Lack of segregation and filtering for the ICS environment (centrally and on remote sites)
- Uncontrolled remote connections to the ICS
- Poor anti-malware coverage on ICS
- No patch management on ICS
- Weak password protection on local HMIs in the field
- Lack of redundancy in the infrastructure
- Industrial control network used for other services (physical security, IP telephony, remote enterprise users)

An extract of Water Co. ICS security risk register is provided below.

Figure 5 - Extract of Water Co. risk register

Risk Instance	Risk Level	Vulnerability	Threat Source	Threat Event	Vulnerability Level	Threat Level	Impact	Comments
Penetration or propagation of malware into the ICS environment through the corporate network or through uncontrolled GPRS dial-up connections	Critical	Lack of segregation of ICS environment & lack of controls over remote maintenance connections	i. Service provider ii. Hackers	i. Accidental/ Malware ii. Penetration	High	Medium	Critical	Due to the poor protection of the infrastructure, the feasibility of an attack or the potential for malware protection is considered as high. The consequences on the control environment could lead to prolonged disruption of service.
Passive listening on RF network	Low	No encryption of RF network	Hacker	Passive listening	Medium	Low	Low	Passive listening of communications on unencrypted RF connections. The impact of passive listening is judged limited as there is no specific confidentiality associated to the data. However the information gathered through passive listening could be used to build a more elaborate attack
Control of local processes through direct access to field HMIs on remote, unmanned sites	High	Weak physical security & poor password policy on local HMI	Physical intruder	Physical breach, bypass of authentication mechanisms	High	Low	Medium	Through physical access to a local facility, local processes could be tampered with through HMIs which have poor password protection. This would cause local impacts that would be detected through the regional control room

Considering the risks and the need to find a cost effective interim solution before the technology refresh project progresses, Water Co. decided on the following **interim** mitigation strategy:

- Address where possible the technical risks associated with legacy systems, prioritise “quick wins” and solutions that can be used with new target technologies. This architecture refresh will the life of systems and minimise the training cost associated with technologies including:
  - New unique remote access solution coming through the Corporate Internet connection and replacing all other local solutions, this solution provides remote connectivity to the internal ICS gateway (see below)
  - New DMZ provided by an industrial firewall, the DMZ hosts the internal ICS gateway which is composed of a terminal server and a file staging server

  - Use of IPSEC VPN tunnels to protect traffic on radio network
  - Implementation of VLANs on local plant to segregate ICS, enterprise, telephony and physical security traffic
  - Hardening of the perimeter equipment but no attempt to change old technology on the industrial network.
- Use alternate solutions where technical security controls costs are prohibitive for this interim period including:
  - Increase physical security to control access to control equipment in water treatment plant (several layers of security: several access control zones, locked cabinets, new Intrusion Detection sensors, contact switch on cabinets with feeds to control room)
  - Increase awareness and organisational procedures to manage DMZs used to protect access to HMIs
  - Increased preventive monitoring arrangements during the interim period coupled with an efficient incident response capability.

The new interim architecture designed by Water Co. is represented in the following diagrams. Even though this infrastructure still has security flaws, this constitutes a significant improvement over the previous situation.

Figure 6 - Water Co Regional Network – Interim solution

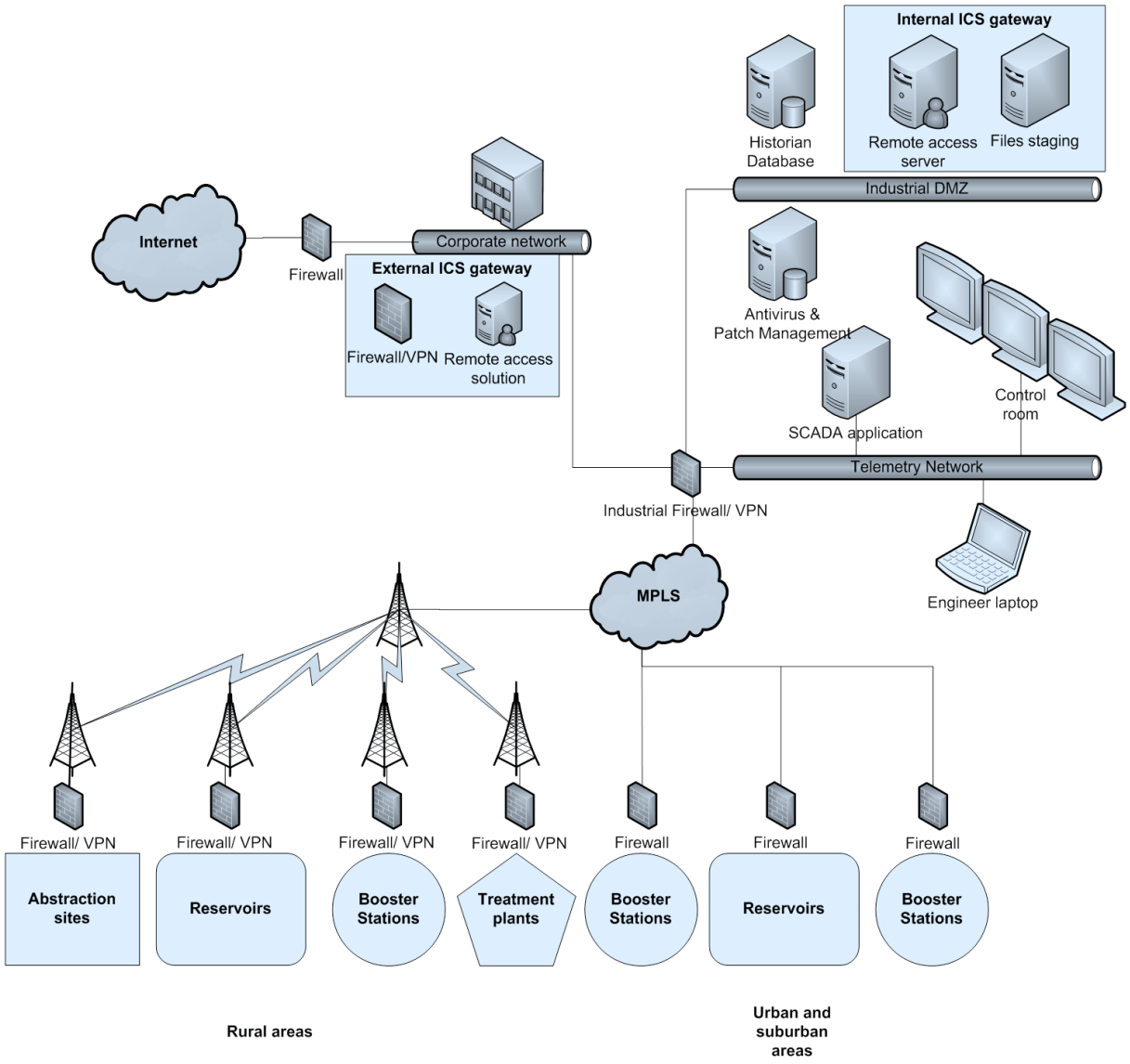
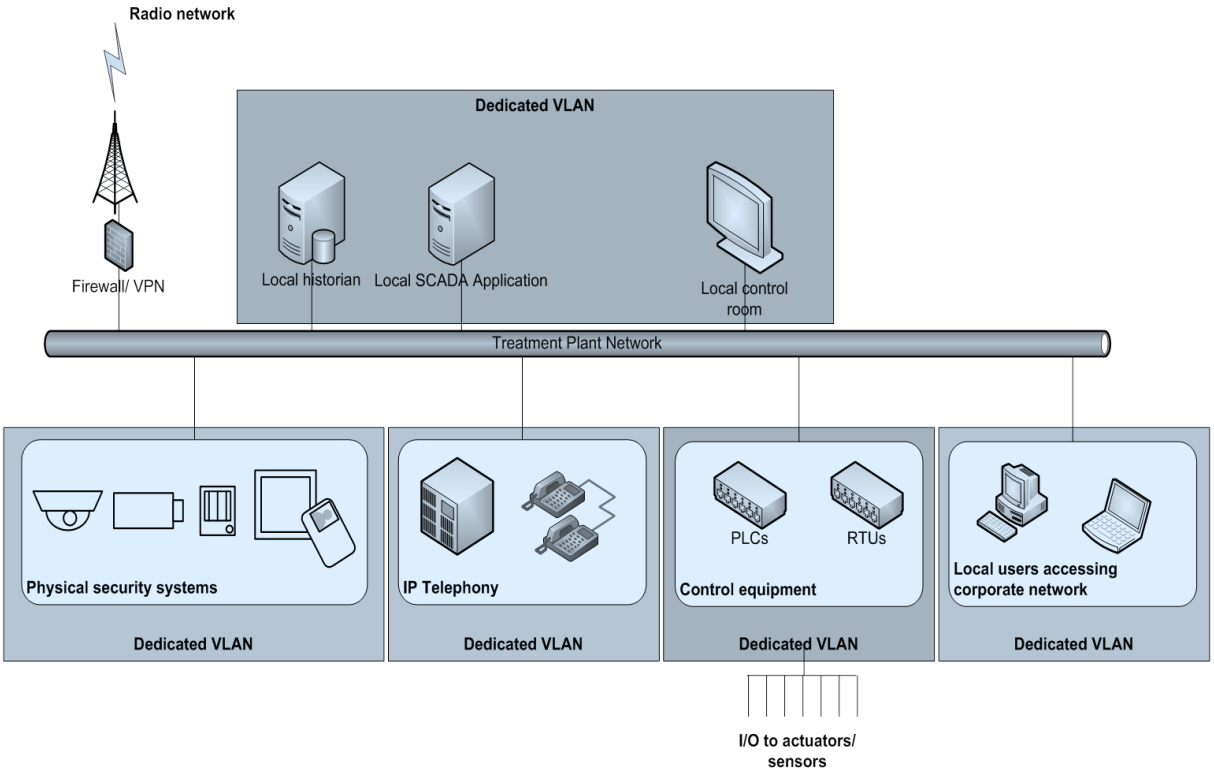


Figure 7 - Water Co site - interim solution



This strategy was approved by the ICS Security Governance Group of Water Co. It did retain an estimated level of residual risk that is **still above their normal risk appetite**, but after discussion with the Board of Directors and the recognition that this would only be for the **interim period**, this was signed off, provided that increased reporting on the status of the ICS security risk will be maintained until the new target architecture is introduced.

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/