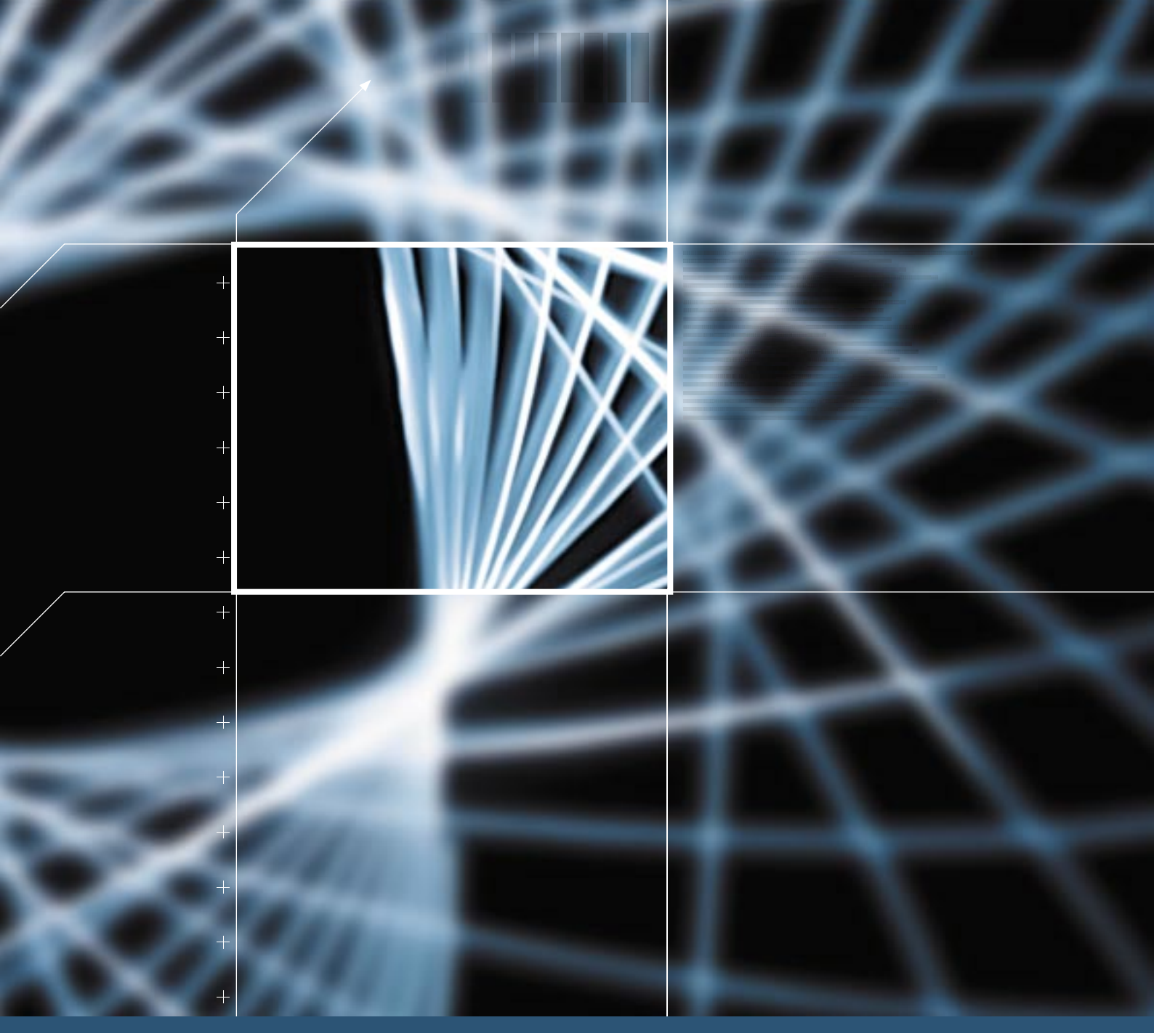

GOOD PRACTICE GUIDE

PROCESS CONTROL AND SCADA SECURITY

GUIDE 2. IMPLEMENT SECURE ARCHITECTURE

CPNI
Centre for the Protection of National Infrastructure

This guide is designed to impart good practice for securing industrial control systems such as: process control, industrial automation, distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems. Such systems are used extensively across the nation's critical national infrastructure. The paper provides valuable advice on protecting these systems from electronic attack and has been produced by PA Consulting Group for CPNI.

TABLE OF CONTENTS

1. Introduction 2

1.1 Terminology 2

1.2 Background 2

1.3 Process control security framework 2

1.4 Purpose of this guide 3

1.5 Target audience 3

2. Implement secure architecture summary 4

3. Implement secure architecture 5

3.1 Context of this section within the overall framework 5

3.2 Rationale 5

3.3 Good practice principles 5

3.4 Good practice guidance 5

3.4.1 Prioritise vulnerabilities based on business risk 6

3.4.2 Hold a risk reduction workshop 7

3.4.3 Agree target architecture 7

3.4.4 Factors to consider when selecting security measures 7

3.4.5 Risk reduction measure check list 11

3.4.6 Agree implementation plan 12

3.4.7 Implement security improvement measures 13

Appendix A: Document and website references 15

General SCADA references 17

Acknowledgements 20

1. INTRODUCTION

1.1 Terminology

Throughout this framework the terms process control system and process control and SCADA system are used as generic terms 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 Background

Process control and SCADA systems are making use of, and becoming progressively more reliant on standard IT technologies. These technologies, such as Microsoft Windows, TCP/IP, web browsers and increasingly, wireless technologies, are replacing conventional proprietary technologies and further enabling bespoke process control systems to be replaced with off the shelf software.

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

Firstly process control systems were traditionally only designed for the purpose of control and safety. Due to the need for connectivity for example for the extraction of raw plant information or for the ability to perform direct production downloads, the once isolated systems are being connected to larger open networks. This exposes them to threats that these systems where never expected to encounter such as worms[1], viruses and hackers. Security through obscurity is no longer a suitable kind of defence.

Secondly, commercial off the shelf software and general-purpose hardware is being used to replace proprietary process control systems. Many of the standard IT security protection measures normally used with these technologies have not been adopted into the process control environment. Consequently, there may be insufficient security measures available to protect control systems and keep the environment secure.

There are potentially serious consequences should these vulnerabilities be exploited. The impacts of an electronic attack on process control systems 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.

1.3 Process control security framework

Although process control systems 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 the IT security experts and after tailoring some standard security tools and techniques can be used to protect process control systems. Other standard security measures may be completely inappropriate or not available for use in a control environment.

[1] The Wikipedia reference for a worm – A computer worm is a self replicating computer program. It uses a network to send copies of itself to other systems and it may do so without user intervention. Unlike a virus, it does not attach itself to an existing program. Worms always harms the network (if only consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

This process control security framework is based on industry good practice from the fields of process control and IT security. It focuses on seven key themes to address the increased use of standard IT technologies in the process control and SCADA environment. The framework is intended to be a point of reference for an organisation to begin to develop and tailor process control security that is appropriate to its needs. The seven elements of the framework are shown below in Figure 1.

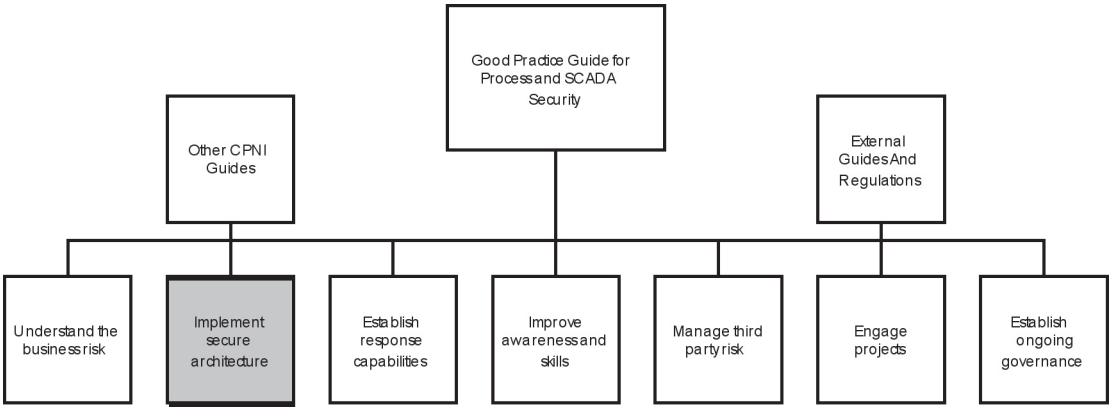

Figure 1 – Where this guide fits in the Good Practice Guide framework

Each of these elements is described in more detail in their separate documents, this document provides good practice guidance on understanding the business risk. All the documents in the framework can be found at the following link http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx .

1.4 Purpose of this guide

The CPNI **'Good Practice Guide - Process Control and SCADA Security'** proposes a framework consisting of seven elements for addressing process control security. This **'Implement Secure Architecture'** guide builds on the foundation provided in the high level good practice guide, and provides good practice guidance on deciding on appropriate security architecture for process control systems.

This guide does not provide detailed technical solutions, architectures or standards.

1.5 Target audience

This guide is aimed at anyone involved in the security of process control, SCADA and industrial automation systems including:

- Process control, SCADA and industrial automation engineers
- Telemetry engineers
- Information security specialists
- Physical security specialists
- Business leaders
- Risk managers
- Health and safety officers
- Operations engineers.

2. IMPLEMENT SECURE ARCHITECTURE SUMMARY

This 'Implement secure architecture' element of the good practice framework addresses the definition and implementation of secure architectures for control systems.

When faced with securing a control system it is often easy to jump straight into implementing obvious security measures such as installing a firewall or deploying anti-virus software. However it is possible that such actions may not be the best investment of valuable resources, such as finance and personnel, if deployed indiscriminately. 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 control systems in scope and examines the threats, impacts and vulnerabilities that the systems face. This topic is described in more detail in the 'Understand the business risk' element of this framework, the location of this guide can be found in Appendix A. The risk assessment determines what 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 then a suite of risk reduction (security improvement) measures can be selected to form an overall secure architecture for the control system. In this context the term 'architecture' is used in the wider sense to cover the human elements of the systems as well as the technologies. A secure architecture will consist of a variety of process, procedural and managerial protection measures and not just a suite of technical solutions.

Selecting process control security measures is by no means an exact science and 'one size' definitely does not fit all. Owing to the relatively immature nature of the field of process control security and the wide variety of legacy systems in existence it is not just a simple matter of complying with international standards. There are a number of industry standards currently under development across the industry but we are far from a position of merely being able to implement a standard set of security protection measures. A sample list of these standards can be found in Appendix A.

Once a secure architecture has been selected all that is needed is for it to be implemented. This may sound straightforward however the process of implementing these solutions can be risky and can cause system outages if not managed carefully.

3. IMPLEMENT SECURE ARCHITECTURE

3.1 Context of this section within the overall framework

This section uses the outputs from the 'Understand business risk' section to select a suite of appropriate security measures and form a secure architecture which can then be implemented to secure the control systems.

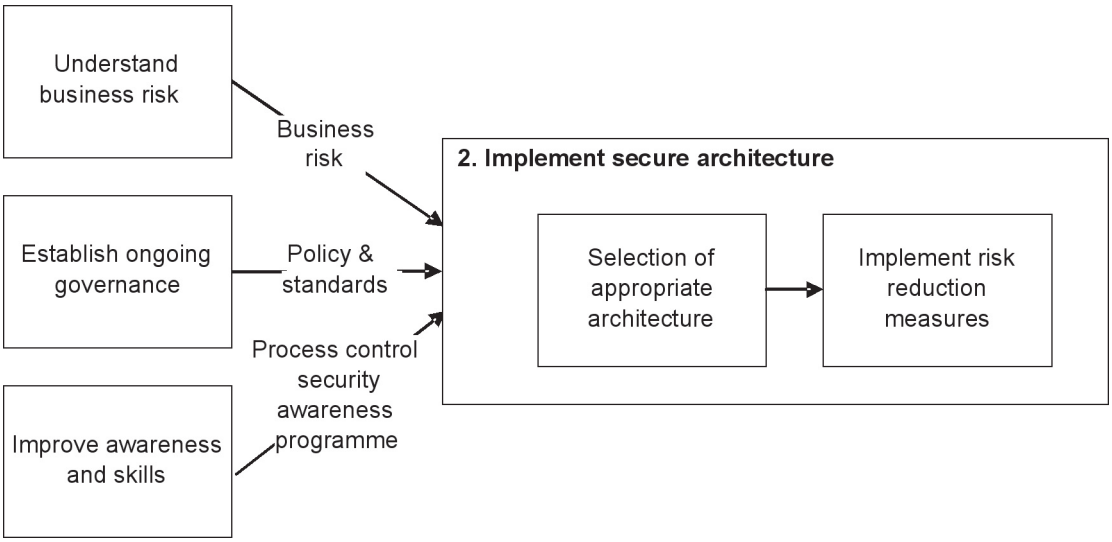

Figure 2 – Where 'Implement secure architecture' fits into the framework

3.2 Rationale

Designing a secure architecture for a control system can be a difficult exercise as there are so many different types of systems in existence and so many possible solutions, some of which might not be appropriate for the process control environment. Given limited resources it is important that the selection process ensures that the level of protection is commensurate with the business risk and does not rely on one single security measure for its defence.

3.3 Good practice principles

The relevant good practice principles in the overarching document 'Good Practice Guide Process Control and SCADA Security' are:

- Select appropriate security measures (based on business risk) to form a secure architecture
- Implement selected risk reduction measures.

3.4 Good practice guidance

This element of the framework covers the definition and implementation of a secure architecture for the process control systems under consideration. This is achieved through the selection of a suite of appropriate protection measures, which will effectively address the business risk

identified. The following is a high level overview of a process that could be adopted for the architecture selection and implementation.

- Understand the business risk
- Prioritise business vulnerabilities based on business risk
- Hold an architecture workshop
- Agree target architecture
- Define implementation plan
- Implement security improvement measures.

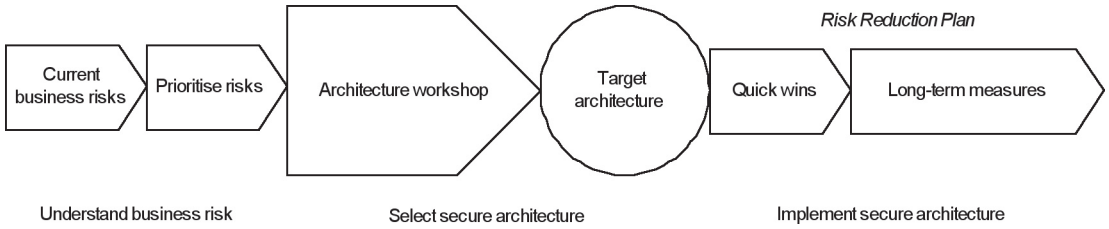

Figure 3 – High level processes for implementing secure architecture

The key elements that need to be considered throughout this process are described in the following sections.

3.4.1 Prioritise vulnerabilities based on business risk

Before deciding upon any security measures it is important to have a good understanding of the business risk facing the control systems. When faced with the task of securing a control system it can be very tempting to jump straight into implementing obvious security measures such as firewalls or anti-virus software without considering the wider risk landscape. This approach can result in poorly secured systems as all the protection measures have not been considered as a holistic architecture. A good understanding of the business risk is needed to ensure that appropriate security measures are selected so that the system is protected in proportion to the business risk – i.e. not too much protection (inefficient use of resources) and not too little (insecure systems).

Understanding the business risk focuses on four key elements which are listed below and described in more detail in the 'Understand the business risk' element of the framework.

- systems
- threats
- impacts
- vulnerabilities.

The output of this process is an understanding of the key systems, the threats they pose and the vulnerabilities which could be exploited. This is an essential prerequisite for the definition of a secure architecture.

3.4.2 Hold a risk reduction workshop

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

When forming a team to undertake this workshop it should include (but may not be limited to) the following:

- Process control security Single Point of Accountability (SPA)
- Process control team members
- Business representatives
- Operations team representatives
- IT security representatives
- IT infrastructure representatives
- IT application representatives
- Process control vendors.

Once assembled, the team can progress with examining the identified risk factors and selecting appropriate risk reduction measures.

3.4.3 Agree target architecture

The key objective of the risk reduction workshop is to consider the risk factors and vulnerabilities identified in the risk assessment. Each of the risks should be taken in turn and analysed.

For each risk there are three types of action available:

- Deploy risk reduction measure (or security improvement measure) – the remainder of this section considers the selection of these measures in more detail.
- Deploy continuity plan – this topic is covered in the framework element 'Establish Response Capability', the location of this document can be found in appendix A
- Treat as residual risk (take no action) – where a decision to treat a risk as residual, this should be agreed by business leadership and recorded in a risk register. Residual risk should be reviewed on a regular basis.

3.4.4 Factors to consider when selecting security measures

Although the task of selecting risk reduction measures sounds simple it is often much more difficult than expected owing to the wide range of factors affecting the choice of measures each introducing their own constraints. The factors to be considered can be split into six areas: cost, strength of protection, business case, implementation, delivery and solutions.

Cost

The cost to implement 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 involve 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.

Ongoing operational costs of the security protection measure need to be considered.

Strength of Protection

Considering how strong a protection measure is, can be difficult to determine, however defining simple scales indicating the strength and cost of measures can simplify the decision making process.

Security is only as strong as the weakest link, 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.

Business case

It may be necessary to construct a business case in order to secure funding for control system security improvements. This business case should clearly articulate the current risks and the need for security improvements. The output from the Understand the Business Risk element of the framework may be useful in constructing this business (see appendix A). The case should also clearly show how the proposed investments would change the business risk profile for the control systems 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 improving security of control systems including improved risk profile post improvements (i.e. the business benefit).
- The requirements for a security programme, key activities, resources and costs.
- The return on security investment (ROSI).

When constructing a business case it is often useful to articulate the return on security investment (ROSI). However this can be difficult to determine in hard figures owing to the lack of data available in process control and SCADA security incidents.

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

Implementation

Some security measures are easier to implement than others and may therefore be favoured by sites in the short term. For example, disconnecting a dial up modem when it is not in use provides limited protection, but is easy to implement.

The implementation of some of the security measures will take relatively little time 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.

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

Consider what testing of a security solution might be required before it can be deployed in a live control systems environment. Additional testing will add to costs and increase deployment timescales.

Delivery

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

Consider who would be responsible for the implementation of the security measures. In particular they should identify which measures will require the involvement of existing members of process control 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.

When considering security measures do not forget to consider staff training requirements and ongoing support and maintenance. This may just be a financial cost but often this may introduce additional remote access requirements or a need to upgrade hardware or software.

Solutions

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

Where possible use standard solutions that are already available and aim for commonality in approach to minimise cost and complexity and achieve other benefits such as:

- **Reuse proven solutions** – proven architecture solutions should be reused where applicable.

- **Known quality standard** – reusing an existing solution should ensure that the same level of quality is reproduced in different parts of the process control system or on different sites.

- **Easier to manage** – if problems or exposures are handled the same way then responding to incidents will be easier to manage as the same solution can be rolled-out to all process control systems that have used the same approach.

- **Economies of scale** – using a specific product or supplier across the organisation may result in greater purchasing power and some influence over security design improvements.

- **Skills and expertise** – reusing proven control systems security approaches enables organisations to limit the development and training required to support the security measure. If supported by a third party it may also reduce support costs.

Where available, consider adopting solutions approved by the control system vendor. These solutions should have undergone detailed integration and accreditation by the vendor. Seek assurance from the vendor of this testing and accreditation.

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

Wherever possible, use communication protocols that are firewall friendly. Non firewall friendly protocols (e.g. OPC[2]) mean that firewall rule bases cannot be tightly configured.

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

Where possible, consider using services and solutions that are already available such as those provided by the IT department. Solutions may need tailoring to the operating environment of control systems, for example phased deployment of anti virus updates.

When drawing up the possible security measures, develop a number of different options, 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

[2] The Wikipedia definition of OPC – OLE (Object-Linking and Embedding) for Process Control. The standard specifies the communication of real-time plant data between control devices from different manufacturers

Outsourcing: Security Governance Framework for IT Managed Service Provision' (see appendix A). This guide is a general document and is not specific to process control and SCADA systems.

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

There are likely to be a number of relatively simple security measures that can be quickly implemented, examples include:

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

3.4.5 Risk reduction measure check list

Once a target security architecture has been identified consider using the following checklist to verify completeness. This list is just the high level sections listed in the over arching document 'Good Practice Guide Process Control and SCADA Security'.

- Network architecture
- Firewalls
- Remote access
- Anti-virus
- Email and internet access
- System hardening
- Backups and recovery
- Physical security
- System monitoring
- Wireless networking
- Security Patching
- Personnel background checks
- Passwords and accounts
- Documented security framework
- Resilient infrastructure and facilities
- Vulnerability management
- Starters and leavers process
- Management of change
- Security testing
- Device connection procedures.

There are a variety of guides available that explore some of these topics in more detail such as:

- Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
- Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision

- Good Practice Guide Patch Management
- Best Practice Guide Commercially Available Penetration Testing
- A Good Practice Guide on Pre-Employment Screening
- CPNI guide on Personnel Security Measures
- Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments
- Securing WLANs using 802,11i
- Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
- Cyber Security Procurement Language for Control Systems
- NERC Critical Infrastructure Protection (CIP)
- DHS Catalog of Control System Security Requirements
- NIST Guide to Industrial Control (ICS) Systems
- ISA SP99, Manufacturing and Control Systems Security

(see Appendix A).

3.4.6 Agree implementation plan

Once a secure architecture has been agreed, costed and funded, then the next task is to define the implementation plan. This might sound simple but the implementation of security improvements can be complex in a control systems environment and there can be a significant risk of system disruption caused by the implementation of the risk reduction measures. 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. Also back out 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 prior to less critical systems

- **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 risk reduction measures 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

- **Phased approach** – the implementation of the risk reduction measures may be carried out over an extended time period. 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 might need to be in place prior to others being implemented. 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 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 risk reduction measures. 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.

3.4.7 Implement security improvement measures

Once the implementation plan has been completed, reviewed and signed off then the implementation of the risk reduction measures can proceed. Throughout the implementation process there are a number of areas to consider:

- **Change control** – all changes to control systems should be carried out under the appropriate change control systems. As these changes may impact both the control systems and IT systems. Further down the value chain the changes might need to be managed under different change systems such as for the plant systems and for the IT systems.

  As changes are made the change control systems should ensure that the system diagrams, inventory and risk assessments are updated. If the change processes do not ensure these updates are made then checks should be undertaken to ensure all information is up to date. Also it might be worth modifying these processes to ensure system information is always up to date.

- **Post implementation reviews** – once the risk reduction measures are implemented, an assurance exercise should be undertaken to ensure that the measures 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 been done under strict conditions (e.g. plant shutdowns) as it is not uncommon for this type of test to shutdown control systems and corrupt process plant controllers

- **Communications and awareness** – throughout the implementation process it is important to provide appropriate communications. This ensures that all appropriate stakeholders are aware of the latest status and developments in the implementation project.

The job of process control security is not finished when all the risk reduction measures have been implemented to form the complete security architecture. This is only a milestone in the control system's security lifecycle. There is an ongoing task to ensure that the control systems remain appropriately secured into the future. This involves:

- Keeping policy, standards and processes up to date with current threats
- Ongoing assurance that the control systems are in compliance with the security policy and standards
- Ensuring all engineers, users and administrators are security aware and implement the processes and procedures in a secure manner
- Ensuring there is appropriate response capability to react to changes in security threats
- Ensuring that third party risk is managed.

Regular audits should be undertaken to ensure that the risk is being actively managed and that the process and procedures that have been put in place are being followed. Further guidance on managing risk can be found within the 'Understand the business risk' element of this framework.

These tasks are detailed in the remainder of this good practice guidance framework.

APPENDIX A: DOCUMENT AND WEBSITE REFERENCES USED IN THIS GUIDE

Section 3.4.2
Guide to Industrial Control (ICS) Systems
http://csrc.nist.gov/publications/PubsDrafts.html

Section 3.4.5
Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks,
www.cpni.gov.uk/Docs/re-20050223-00157.pdf

Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision,
www.cpni.gov.uk/Docs/re-20060802-00524.pdf

Good Practice Guide Patch Management,
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

Best Practice Guide Commercially Available Penetration Testing,
www.cpni.gov.uk/Docs/re-20060508-00338.pdf

A Good Practice Guide on Pre-Employment Screening,
www.cpni.gov.uk/Products/bestpractice/3351.aspx

CPNI Personnel Security measures,
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments,
www.us-cert.gov/control_systems/pdf/Zigbee%20Rec%20Pract%20-%20draft-posted%207-10-07.pdf

Securing WLANs using 802,11i –
http://csrp.inl.gov/

Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf

Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

DHS Catalog of Control System Security Requirements
www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf

DHS Control Systems Security Program Recommended Practices
http://csrp.inl.gov/Recommended_Practices.html

ISA SP99, Manufacturing and Control Systems Security
www.isa.org/mstemplate.cfm?section=homeandtemplate=/TaggedPage/getStandards.cfmandMicrositeID=988andCommitteeID=6821.

Guide to Industrial Control (ICS) Systems
http://csrc.nist.gov/publications/PubsDrafts.html

GENERAL SCADA REFERENCES

BS 7858:2006: Security screening of individuals employed in a security environment. Code of practice
www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Security/Security-Products/BS-78582006/

BS 8470:2006 Secure destruction of confidential material. Code of practice
www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030127562.

Best Practice Guide Commercially Available Penetration Testing
www.cpni.gov.uk/Docs/re-20060508-00338.pdf.

Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
www.cpni.gov.uk/Docs/re-20050223-00157.pdf.

CPNI First Responders' Guide: Policy and Principles
www.cpni.gov.uk/docs/re-20051004-00868.pdf

CPNI SCADA Good Practice Guides
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

CPNI Information Sharing
www.cpni.gov.uk/ProtectingYourAssets/InformationSharing.aspx

CPNI Personnel Security measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

Good Practice Guide Patch Management
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision
www.cpni.gov.uk/Docs/re-20060802-00524.pdf

Good Practice Guide on Pre-Employment Screening
www.cpni.gov.uk/Products/bestpractice/3351.aspx

An Introduction to Forensic Readiness Planning
www.cpni.gov.uk/docs/re-20050621-00503.pdf

Personnel Security Measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

DHS Control Systems Security Program
http://csrp.inl.gov/

DHS Control Systems Security Program Recommended Practice
http://csrp.inl.gov/Recommended_Practices.html

Guide to Industrial Control Systems (ICS)
http://csrc.nist.gov/publications/PubsDrafts.html

Securing WLANs using 802,11i
http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf

Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdfISA SP99 –

DHS Catalog of Control System Security Requirements
www.dhs.gov

Manufacturing and Control Systems Security
www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

ISO 17799 International Code of Practice for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612

ISO 27001 International Specification for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

MU Security Industrial Control (MUSIC) Certification
www.musecurity.com/support/music.html

Control System Cyber Security Self-Assessment Tool (CS2SAT)
www.us-cert.gov/control_systems/pdf/CS2SAT.pdf

Department of Homeland Security Control Systems Security Training
www.us-cert.gov/control_systems/cstraining.html#cyber

Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments
www.us-cert.gov/control_systems/pdf/Zigbee%20Rec%20Pract%20-%20draft-posted%207-10-07.pdf.

Achilles Certification Program
www.wurldtech.com/index.php

American Gas Association (AGA)
www.aga.org

American Petroleum Institute (API)
www.api.org

Certified Information Systems Auditor (CISA)
www.isaca.org/

Certified Information Systems Security Professional (CISSP)
www.isc2.org/

Global Information Assurance Certification (GIAC)
www.giac.org/

International Council on Large Electric Systems (CIGRE)
www.cigre.org

International Electrotechnical Commission (IEC)
www.iec.ch

Institution of Electrical and Electronics Engineers (IEEE)
www.ieee.org/portal/site

National Institute of Standards and Technology (NIST)
www.nist.gov

NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

Norwegian Oil Industry Association (OLF)
www.olf.no/english

Process Control Security Requirements Forum www.isd.mel.nist.gov/projects/processcontrol/
US Cert
www.us-cert.gov/control_systems/

WARPS
www.warp.gov.uk

ACKNOWLEDGEMENTS

PA and CPNI are grateful for the comments and suggestions received from the SCADA and Control Systems Information Exchange and from other parties involved with CNI protection around the globe 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

This document was produced jointly by PA Consulting Group and CPNI.

Centre for the Protection of National Infrastructure
Central Support
PO Box 60628
London
SW1P 9HA
Fax: 0207 233 8182
Email: enquiries@cpni.gov.uk
Web: www.cpni.gov.uk

For further information from CPNI on process control and SCADA security:
Internet: www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

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 process control and SCADA security:
Email: process_control_security@paconsulting.com
Web: www.paconsulting.com/process_control_security