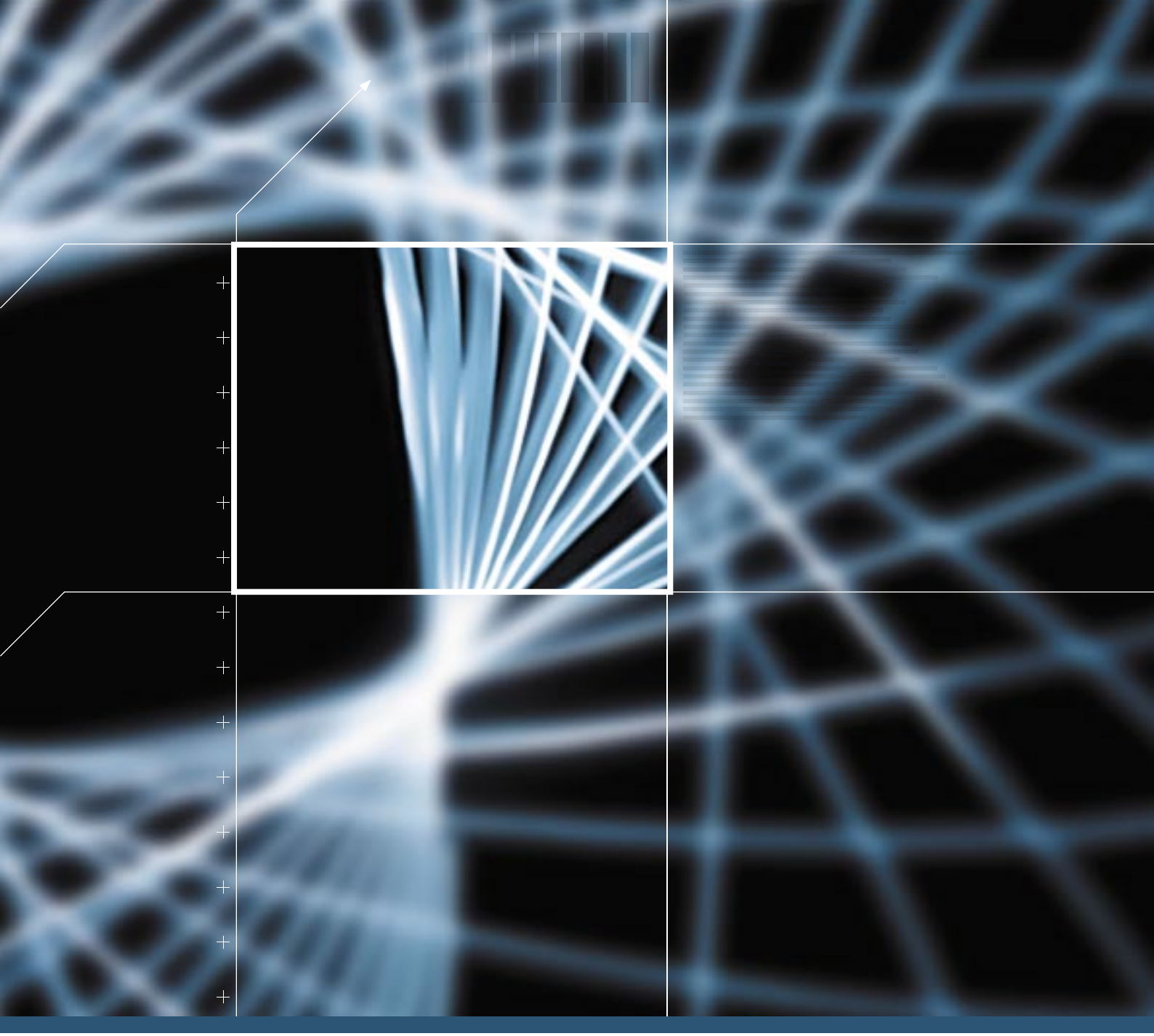

GOOD PRACTICE GUIDE

PROCESS CONTROL AND SCADA SECURITY

GUIDE 6. ENGAGE PROJECTS

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

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.

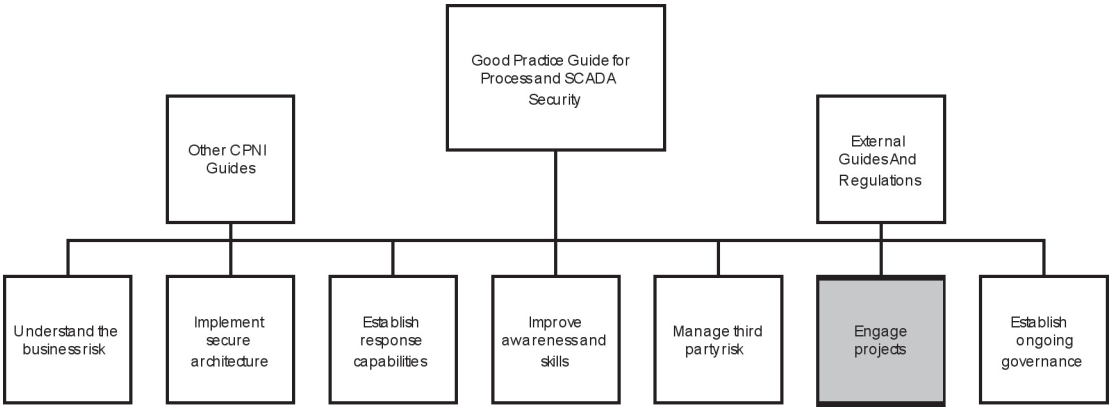

Figure 1 – Where this guide fits in the Good Practice Guide framework

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 **'Engage Projects'** guide builds on the foundation provided in the high level good practice guide and provides good practice guidance on building security considerations into process control security projects.

This guide does not provide detailed process control security requirements as these will vary from system to system.

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 and automation, telemetry and SCADA engineers
- Information security specialists
- Physical security specialists
- Business leaders
- Risk managers
- Health and safety officers
- Operations engineers
- Project managers
- Procurement managers.

2. ENGAGE PROJECTS SUMMARY

Process control systems are usually installed with an expectation of a long service life and minimal changes to these systems during their lifetime. However saying this for all control systems in use is probably an over generalisation. In many organisations there are often a number of process control system related projects underway, any of which could have security implications.

Projects such as new control systems, control system changes, IT system changes, upgrades, the implementation of management systems information and introduction of new connections brings in a process control security risk and should be subjected to a risk assessment.

Once a system has been risk assessed then any projects that might affect it need to be engaged so that security can be built into the project from an early stage. Any new system on a 'green field' site should build security requirements into the design and build process from an early stage. The assurance of these requirements should be assessed throughout the project life cycle.

Process control security issues are often relegated to later stages of projects and it is likely that in these cases a decision taken at an early project stages about possible project options will not consider the relative security implications. This means the project team are neglecting a vital component that will almost definitely impact time and resources at a later stage in the project, and more seriously it can also reduce the overall effectiveness of the security protection framework.

Implementing security protection measures into systems is notoriously more difficult and costly to do once the systems have been built and deployed. Of greater importance is the fact that bolting on security measures to an existing, live system is often less effective. Dealing with security risk by integrating protection measures into the project development processes at an early stage is more effective, avoids overruns and is usually less costly.

3. PROJECT ENGAGEMENT

3.1 Context of this section within the overall framework

This guide takes a number of other elements of the good practice guide framework relating to policy and standards, risk assessment and third party considerations and incorporates them into a guide dedicated to engaging process control security projects.

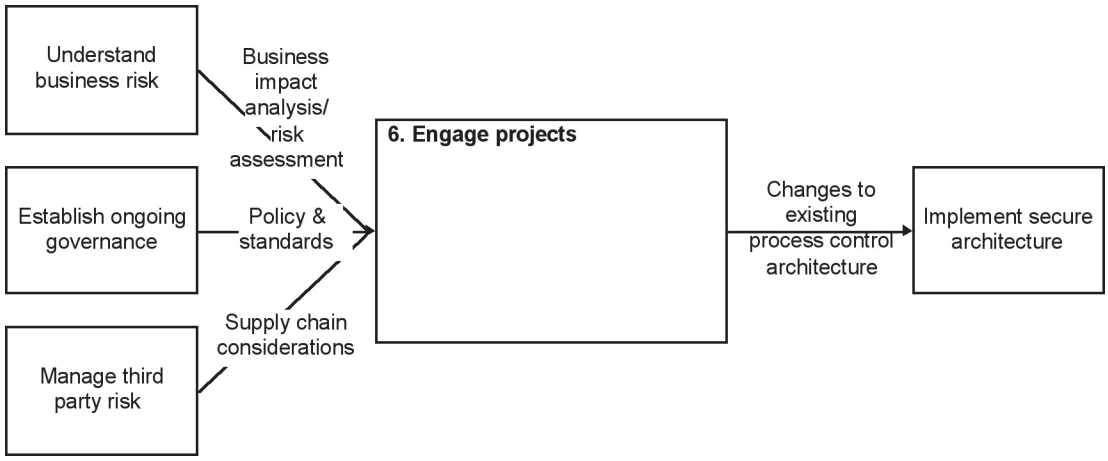

Figure 2 – Where 'Engage projects' fits in the framework

3.2 Rationale

Build security into process control systems at early stages by embedding quality security requirements into the organisation's design and build process. Bolting security on to a system after it has been built is far less effective and usually more expensive.

3.3 Good practice principles

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

- Identify and engage all projects that have direct or indirect process control systems implications at an early stage of their development.
- Ensure that a security architect is appointed as a single point of accountability for security risk management for the full life cycle of the project.
- Ensure standard security clauses and specifications are incorporated in all procurement contracts.
- Include security requirements in the design and specification of projects and ensure that all appropriate security polices and standards are adhered to.
- Undertake security reviews throughout the project development life cycle, for example, at the same time as health and safety checks are done
- Plan for security testing at key points of the life cycle (e.g. tender, commissioning, factory acceptance testing, commissioning and during operations).

3.4 Good practice guidance

3.4.1 Identify and engage all process control projects

In order to effectively manage process control security risk relating to projects it is necessary to have good visibility of what projects are planned and underway. In many organisations it can be difficult to determine what project activity is planned and underway and often projects are only identified late on in their life cycle when it can be too late to incorporate security requirements.

Processes should be established to highlight any projects at an early stage that might have process control security considerations. A register or inventory of projects involving process control elements should be maintained. This is to ensure that the project development processes could be modified to ensure that all projects incorporate security into the development process.

Example projects types which might have process control 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
- Changing embedded code (firmware).

3.4.2 Engage security architect

Projects with process control security implications should appoint a security architect who will be accountable for security issues throughout the project life cycle. This security architect may only work part time on the project and would advise on how the project should incorporate security requirements and provide assurance that the delivered system is appropriately secured.

Having an expert who can translate security requirements from policies and standards into a form that they can be incorporated into the project specification can be an extremely cost-effective decision to make. Building quality and accountability for security issues into the design and project life cycle ensures that process control security requirements are not forgotten and that the projects remain aware of the security implications of decisions that are made.

3.4.3 Build security requirements into procurement contracts

Security clauses are often left out of contracts due to being poorly considered and are sometimes inappropriate; in a rush to pull together security requirements some specifications from the corporate IT environment are ‘borrowed’ with little thought. Also it is common for security issues not to have been considered early enough to be incorporated in procurement contracts.

State process control security requirements at an early stage and ensure that appropriate clauses are included within procurement contracts. This will ensure that the vendor considers security as one of the fundamental requirements for the system and therefore should be delivered as part of the system.

Software coding errors can create vulnerabilities, this is the case with control systems as well as for normal IT applications 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 of the security requirements that will be expected in the delivered system. However, it is important to set an appropriate level of detail so that the contractual requirements are not too prescriptive. The contract should also clearly state what requirements are mandatory and which are optional. For further guidance on what security clauses should be considered in contracts please consult the 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 of health checks
- secure coding reviews
- security testing
- secure replacement of defective parts containing data (e.g. hard disks).

Many vendors have fed back that their users criticise the vendors for not supplying secure systems. However, such security requirements are rarely included in system specifications and procurement contracts. Including significant security measures in proposals where this is not requested in the design requirements can put a vendor's proposal in an unfair light from a cost point of view and could be detrimental in the selection process. By clearly stating security requirements in procurement contracts users can clearly communicate their security expectations and can ensure a level playing field for vendors competing for the business. Security for process control systems should be considered a core requirement for all systems, not an optional extra.

Further guidance on this security requirements can be found in the Cyber Security Procurement Language for Control Systems document by Idaho National Laboratory and also the Catalog of Control System Security Requirements document produced by the DHS, links to these documents can be found in appendix A.

3.4.4 Build security requirements into design specifications

Building process control security into the design and build process at the project stage seems obvious but is often overlooked or not done at all by many organisations. A relatively small investment at the project stage will be far cheaper than bolting on security later, or dealing with overruns and design changes that impact the whole system.

Security requirements should be considered no differently from any other functional requirements. They should be clearly expressed and included in any functional design specifications.

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 business risk is not considered 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.

For a list of topics that should be considered when developing system security requirements please refer to the organisation's policy and standards and the framework element Implement Secure Architecture

Further guidance on requirements can be found in the Cyber Security Procurement Language for Control Systems document by Idaho National Laboratory and also the Catalog of Control System Security Requirements produced by the DHS, links to these documents can be found in appendix A.

3.4.5 Review security throughout the development life cycle

Security is an important part throughout the entire project life cycle but has particular relevance in the early stages. The diagram below shows how security topics should be considered throughout the development life cycle.

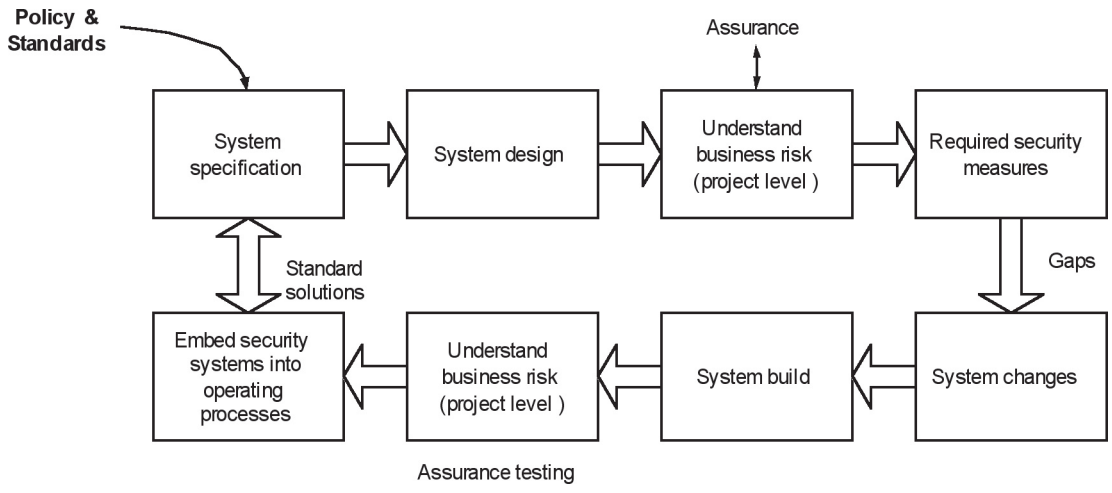

Figure 3 – Security in the development life cycle

The key stages in the development life cycle are described in the following sections. Further guidance on life cycle considerations can be found in 'Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments' (see appendix A).

3.4.6 System design security reviews

Once a project has progressed to a stage where there is a high level design and agreed architecture, the design should be reviewed against the security specifications and requirements. At this stage the system does not exist but this review can be carried out in a similar manner to live systems but as a paper-based exercise. Further guidance can be found in the Understand the Business Risk element of the good practice guide framework architecture. The review should seek to identify any gaps that exist between the proposed design and the security requirements, specifications, policy and standards.

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 to be 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 different stages of the development cycle. This would depend on how large and complex the system is and whether the implementation is in stages. Where possible these reviews should be incorporated within or at least feed into other system reviews that might already be in the implementation plan e.g. health and safety reviews etc.

3.4.7 System testing

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

Once a process control system 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 caused significant security incidents. Consequently there is great value in carrying out as much security testing as is possible before a system goes live. The output of this testing can feed into a vulnerability management regime 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 testing system 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
- Ports, protocols and services
- 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 system 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: recent research has highlighted widespread vulnerabilities in embedded systems such as low level controllers, PLCs and RTUs. A widely quoted example is of a manufacturing firm that experienced a significant disruption to it operations because an authorised security scan crashed many of the PLCs in its plant. Many of the identified vulnerabilities could be minima, but some are serious vulnerabilities and could have safety implications depending on how the devices are implemented.

Consequently it is recommended as good practice to gain assurance of such devices prior to deployment into operations. There are a number of companies who provide security testing of PLC (including MU Security and Wurldtech), further details of organisations providing this type of testing can be found in appendix A.

At the time of writing there is no industry standard to perform this assurance against (although the ISA are working on this) and there are no formal accredited bodies to perform this testing. However test tools are emerging which is dedicated to controller level testing. It is recommended as good practice that such devices are tested using one of the available tools prior to being deployed.

Factory acceptance testing: is a great opportunity to test the full system before it goes into normal operations (when further testing becomes difficult). This stage is usually carried out in the vendor's premises and typically includes a variety of acceptance tests that would be carried out by the customer or by authorised third parties (on behalf of the customer). These tests are normally based on the functional requirements and specifications defined early on in the project. As security requirements were incorporated into the functional requirements then security tests should be incorporated into the acceptance tests. Once a system has passed its acceptance tests it is very difficult to then make changes to the system to correct any security issues.

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

- Security configuration
- Vulnerability scanning of the whole system
- Penetration testing
- Firewall rule testing
- Failover/ disaster recovery testing
- Backup testing
- Patching testing
- AV update testing
- Remote access testing
- System hardening assurance.

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.

Further guidance on testing requirements can be found in the Cyber Security Procurement Language for Control Systems document by Idaho National Laboratory (see appendix A).

3.4.8 System handover

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:

- 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 the 'Understand the Business Risk' framework guide)
- Confirmation of all software on hard disks and firmware
- Up to date system documentation
- Results of factory acceptance tests and commissioning tests.

Further discussions on this topic can be found in 'Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments' (see appendix A).

3.4.9 Disposal

When replacing equipment it is essential that the subject of disposal is adequately addressed. 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 and 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 (see appendix A).

APPENDIX A: DOCUMENT AND WEBSITE REFERENCES USED IN THIS GUIDE

Section 3.4.3

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

Section 3.4.5

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

Section 3.4.7

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

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

Section 3.4.8

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

Section 3.4.9

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

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