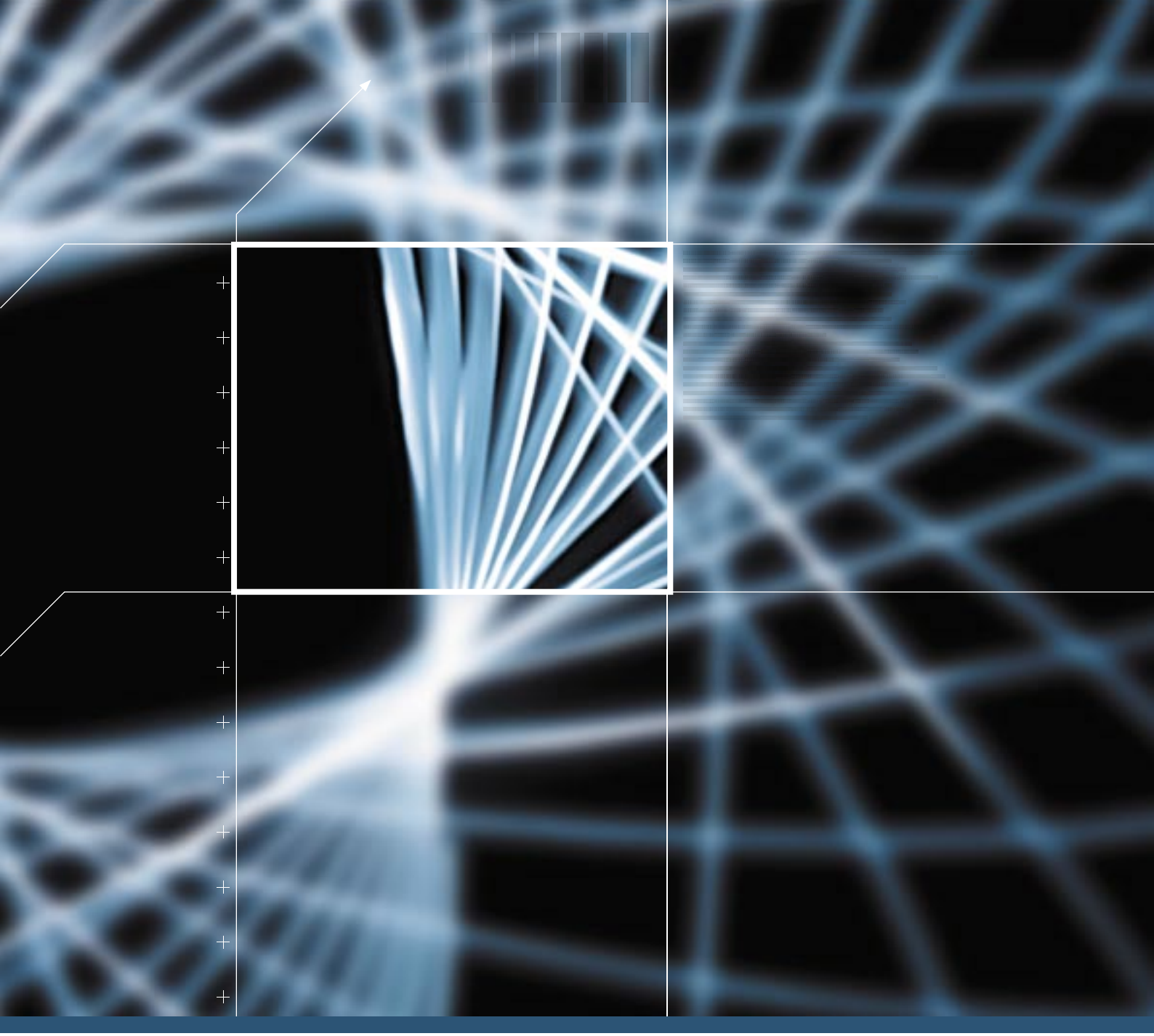

GOOD PRACTICE GUIDE

PROCESS CONTROL AND SCADA SECURITY

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 Aims and objectives

The aim of this document is to provide good practice principles for process control and SCADA security. Specifically this document:

- Provides an overview of the necessity for process control and SCADA system security
- Highlights the differences between process control and SCADA system security and IT security
- Describes the key principles used to develop this framework
- Identifies seven elements for addressing process control system security and for each, presents good practice principles.

1.2 Terminology

1.2.1 Process control and SCADA systems

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 systems (DCS), supervisory control and data acquisition (SCADA), industrial automation and related safety systems.

1.2.2 Good Practice

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

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

The good practices summarised in this document are intended only as guidelines. For some environments and process control systems, it may not be possible to implement all of these principles. For example:

- **Good practice statement:** Protect process control systems with anti-virus software on workstations and servers

  Complication: It is not always possible to implement anti-virus software on process control systems workstations or servers

- **Good practice statement:** Obtain vendor accreditation and configuration guidance from process control system vendors prior to deployment of such software

  Complication: Some vendors will not accredit anti-virus software and other process control systems are incompatible with such software.

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

2. SECURING PROCESS CONTROL AND SCADA SYSTEMS

2.1 Overview

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 the 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 closed systems designed for functionality, safety and reliability where the prime concern was one of physical security. Increased connectivity via standard IT technologies has exposed them to new threats which they are ill equipped to deal with (for example, worms, viruses and hackers). As these process control networks continue to increase in numbers, expand and connect so the risks to the process control systems from electronic threats continue to escalate.

Procedures for supporting process control systems are compounding this still further. They are now routinely supported by vendors remotely through dial-up links or Internet connections. Modems are rarely subject to good security procedures, and these vendor system connections have been known to introduce viruses or be used for direct attacks by hackers.

A recent development in process control is the connection of systems into the wider supply chain. For example, data from tank level sensors can be used to trigger automatic re-ordering of products from the suppliers. This increased connectivity can expose vulnerable process control systems to external threats from the suppliers systems and introduce risks to other systems in the supply chain.

Secondly, commercial off the shelf software and general purpose hardware is being used to replace propriety process control systems. Such software and hardware often does not match the uniqueness, complexities, real-time and safety requirements of the process control environment. 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 impact.

2.2 Process control security framework

The widely used standards and solutions for securing IT systems are often inappropriate for the process control environment. Although process control systems are now frequently based on standard IT technologies, their operational environments differ significantly from the corporate IT

environment. While some standard security tools and techniques can be used to protect process control systems, they may need careful application or tailoring. Other security measures may be completely inappropriate or not available for use in a control environment.

For example, it may not be possible to install anti-virus protection on process control systems, owing to the lack of processor power on legacy systems, the age of operating systems or the lack of vendor certification. Also, security testing on process control systems must also be approached with extreme caution – security scanning can seriously affect the operation of many control devices. There are rarely dedicated test environments and there are few opportunities to take the systems off-line for routine testing, patching and maintenance.

This document has been developed to provide a framework for protecting process control systems from electronic attack. This framework is based on industry good practice from process control and IT security and focuses on seven key themes.

- Understand the business risks
- Implement secure architecture
- Establish response capabilities
- Improve awareness and skills
- Manage third party risks
- Engage projects
- Establish ongoing governance.

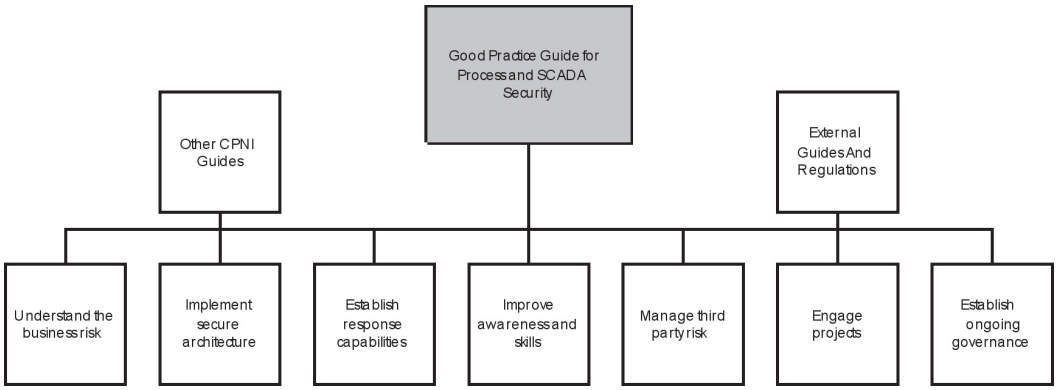

Figure 1 - Where this guide fits in the Good Practice Guide framework

Each of these elements is described in more detail in their separate documents, this document provides an overview of all the guides in the framework. All the guides in the framework can be found on the CPNi website at www.cpni.gov.uk/protectingyourassets/scada.aspx

2.2.1 Guiding principles

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

i. Protect, Detect and Respond

Constructing a security framework for any system is not just a matter of deploying protection

measures. It is important to be able to detect possible attacks and respond in an appropriate manner in order to minimise the impacts.

Protect: Deploying specific protection measures to prevent and discourage electronic attack against the process control systems.

Detect: Establishing mechanisms for rapidly identifying actual or suspected electronic attacks.

Respond: Undertaking appropriate action in response to confirmed security incidents against the process control systems.

ii. Defence in Depth

Where a single protection measure has been deployed to protect a system, there is a risk that if a weakness in that measure is identified and exploited there is effectively no protection provided. No single security measure itself is foolproof as vulnerabilities and weaknesses could be identified at any point in time. In order to reduce these risks, implementing multiple protection measures in series avoids single points of failure.

In order to safeguard the process control system from electronic attacks (e.g. hackers, worms and viruses), it may be insufficient to rely on a single firewall, designed to protect the corporate IT network. A much more effective security model is to build on the benefits of the corporate firewall with an additional dedicated process control firewall and deploy other protection measures such as anti-virus software and intrusion detection. Such a multi-layer security model is referred to as defence in depth.

iii. Technical, Procedural and Managerial protection measures

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

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

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

3. UNDERSTAND THE BUSINESS RISK

3.1 Overview

Before embarking on a programme to improve security, an organisation must first understand the risk to the business from potential compromises to process control systems. Business risk is a function of threats, impacts and vulnerabilities. Only with a good knowledge of the business risk can an organisation make informed decisions on appropriate levels of security and required improvements to working practices. Processes must be established to continuously reassess business risk in the light of ever changing threats.

3.2 Objective

To gain a thorough understanding of the risk confronting the business from threats to process control systems in order to identify and drive the appropriate level of security protection required.

3.3 Principles of good practice

3.3.1 Assess business risk

- Undertake a formal risk assessment of the process control systems to:

i. Understand the systems

- Conduct a formal inventory audit and evaluation of the process control systems. Throughout this, it is important to capture, document and place under change control: what systems exist, what the role of each system is, their business and safety criticalities, where they are located, who the designated owner of each system is, who manages each system, who supports each system and how the systems interact.

ii. Understand the threats

- Identify and evaluate the threats facing the process control systems. Possible threats may include: denial of service, targeted attacks, accidental incidents, unauthorised control, or viruses, worms or Trojan horse infections.

iii. Understand the impacts

- Identify potential impacts and consequences to the process control systems should a threat be realised. Examples of such consequences may include: loss of reputation, violation of regulatory requirements (e.g. health and safety, environmental), inability to meet business commitments, or financial losses.

Note: Where process control systems are critical elements of the supply to other key services, impacts may not be contained within the business but could have serious and potentially life threatening consequences.

iv. Understand the vulnerabilities

- Undertake a vulnerability assessment of the process control systems. Such a review should include: evaluation of the infrastructure, operating systems, applications, component software, network connections, remote access connectivity, and processes and procedures.

3.3.2 Undertake ongoing assessment of business risk

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

The detailed good practice guide can be found at:
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

4. IMPLEMENT SECURE ARCHITECTURE

4.1 Overview

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

4.2 Objective

To implement technical and associated procedural security protection measures, commensurate to the business risk, that will provide a secure operating environment for the process control systems.

4.3 Principles of good practice

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

Detailed guidance on how to select appropriate security measures and implement them to form a secure architecture is provided in the detailed guide Implement Secure Architecture.

The following sections provide key good practice design principles for possible security measures that may be used to form a holistic secure architecture.

4.3.1 Network architecture

- Identify all connections to the process control system
- Minimise the number of connections to the process control system and ensure that there is a valid business case for any remaining connections
- Segregate or isolate process control systems from other networks where possible
- Implement dedicated infrastructure for mission or safety critical process control systems
- Remove, where possible, TCP/IP connections between safety systems (e.g. emergency shut down systems) and process control systems or other networks. Where this is not possible, a risk analysis should be undertaken.

4.3.2 Firewalls

- Protect connections between process control systems and other systems appropriately (e.g. with a firewall and demilitarised zone (DMZ) architecture)
- Deploy firewalls with tightly configured rule bases
- Firewall configuration should be subject to regular review
- Firewall changes should be managed under strict change control
- Implement appropriate firewall management and monitoring regimes
- Firewalls should be managed by appropriately trained administrators
- A 24/7 capability for the management and monitoring of firewalls should be established.

Further guidance can be found in the CPNI good practice guide on firewalls, see appendix A for the location of this guide.

4.3.3 Remote access

- Maintain an inventory of all remote access connections and types (e.g. virtual private network or modems).
- Ensure that a valid business justification exists for all remote access connections and keep remote connections to a minimum.
- Implement appropriate authentication mechanisms (e.g. strong authentication) for remote access connections.
- Carry out regular audits to ensure there are no unauthorised remote access connections.
- Implement appropriate procedures and assurance mechanisms for enabling and disabling remote access connections.
- Restrict remote access to specific machines and for specific users and if possible, at specific times.
- Undertake security reviews of all third parties that have remote access to the control systems.
- Ensure that remote access computers are appropriately secured (e.g. anti-virus, anti-spam and personal firewalls).

4.3.4 Anti-virus

- Protect process control systems with anti-virus software on workstations and servers. Where anti-virus software cannot be deployed other protection measures should be implemented (e.g. gateway anti-virus scanning or manual media checking)
- Obtain accreditation and configuration guidance from process control system vendors prior to deployment of such software.

4.3.5 E-mail and Internet access

- Disable all email and internet access from process control systems.

4.3.6 System hardening

- Undertake hardening of process control systems to prevent network based attacks. Remove or disable unused services and ports in the operating systems and applications to prevent unauthorised use.
- Understand what ports are open and what services and protocols used by devices (especially embedded devices such as PLCs and RTUs). This could be established by a port scan in a test environment. All unnecessary ports and services should be disabled (e.g. embedded web servers).
- Ensure all inbuilt system security features are enabled.
- Where possible restrict the use of removable media (e.g. CDs, floppy disks, USB memory sticks etc.) and if possible removable media should not be used. Where it is necessary to use removable media then procedures should be in place to ensure that these are checked for malware prior to use.

4.3.7 Backups and recovery

- Ensure effective backup and recovery procedures are in place, and are appropriate for the identified electronic and physical threats. These should be reviewed and regularly tested.
- Test the integrity of backups regularly through a full restore process.
- Store backups at on and off site locations.
- Media should be transported securely and stored in appropriately secure locations.

4.3.8 Physical security

- Deploy physical security protection measures to protect process control systems and associated networking equipment from physical attack and local unauthorised access. A combination of protection measures is likely to be required which could include, drive locks, tamper proof casing, secure server rooms, access control systems and CCTV.

4.3.9 System monitoring

- Monitor in real-time process control systems to identify unusual behaviour which might be the result of an electronic incident (e.g. an increased amount of network activity could be the result of a worm infection). A variety of parameters should be defined and monitored in real-time and compared with system baselines for normal operation to provide an indication of unusual behaviour.
- Where possible, implement intrusion detection and prevention systems to provide a more granular view of network activity. These systems should be tailored to the process control environment.
- Review and analyse regularly a defined suite of control system log files. Backup important log files and protect from unauthorised access or modification.
- Give due consideration to the installation of physical monitoring systems such as closed circuit television cameras or tamper alarms on physical enclosures. This is especially important for remote sites.
- Ensure that access to secure areas via pass cards is logged.

4.3.10 Wireless networking

- Wireless networking is a hot topic in the field of industrial control systems owing to the significant business benefits it provides. However wireless systems can introduce significant risk consequently wireless systems should only be used where a thorough risk assessment has been carried out that considers both operational and security risks.
- The field of wireless security is constantly changing and solutions that were thought to be secure only a couple of years ago are now recognised as being vulnerable. Wireless systems should be secured using industry best practices. Regular verifications should be made to determine whether industry best practice has moved on.
- When designing and deploying wireless solutions ensure that the security mechanisms in the solution are understood and correctly configured.
- Further details on securing wireless systems can be found in the guides listed in appendix A.

4.3.11 Security patching

- Implement processes for deployment of security patches to process control systems.
- These processes should be supported by deployment and audit tools.
- The processes should make allowance for vendor certification of patches, testing of patches prior to deployment and a staged deployment process to minimise the risk of disruption from the change.
- Where security patching is not possible or practical, alternative appropriate protection measures should be considered.

Further guidance on general patch management can be found in the CPNI guide, see appendix A for the location of this guide This guide is a general document and is not specific to process control and SCADA systems.

4.3.12 Personnel background checks

- Ensure all staff with operational or administration access to process control systems are appropriately screened.

Further details on pre-employment screening can be found in the CPNI guides, on the CPNI website and in BS7858, see appendix A for the location of these guides.

4.3.13 Passwords and accounts

- Implement and enforce a password policy for all process control systems that cover strength of passwords and expiration times. It is recommended that passwords are changed frequently, but where this is not possible or practical, alternative appropriate protection should be considered.
- Regularly review all access rights and decommission old accounts.
- Where possible change vendor passwords from default settings.
- Passwords may not be deemed necessary for some functions (e.g. view only mode).
- Consider stronger authentication methods for critical functions.

4.3.14 Document security framework

- Document a full inventory of the process control systems and components.
- Document the framework that provides the security for the process control systems and regularly review and update to reflect current threats. This document should include details of the risk assessments, assumptions made, known vulnerabilities and security protection measures deployed.
- Ensure all process control system documentation is secured and access limited to authorised personnel.

4.3.15 Resilient infrastructure and facilities

- Systems should be installed using appropriate infrastructure, such as redundant networks.
- Equipment should reside in environmentally controlled areas to ensure equipment is being maintained at the appropriate ambient conditions.
- Where necessary fire suppressions systems should be installed to protect control systems.

4.3.16 Vulnerability Management

- Implement a vulnerability management system to ensure that vulnerabilities are kept to a minimum in the process control environment. A common method of vulnerability management is security scanning. There are potentially serious risks of scanning process control systems and this should only be performed at carefully chosen times, for example, plant shut downs or on a test environment. Undertake a full risk assessment prior to any scanning activities.

4.3.17 Starters and leavers process

- Implement procedures that ensure new starters receive the appropriate accounts, authorisation levels and security training when they join a process control team.
- Implement procedures to ensure that confidential information and documentation is retrieved, accounts are deactivated and passwords are changed when personnel leave process control teams or when team members change roles and responsibilities.

4.3.18 Management of change

- Certify that all systems are subject to strict change control processes. Security assessments should be included in these processes. It may be necessary for changes to be assessed and approved by multiple change control processes (e.g. a firewall modification might be subject to both IT and plant change management processes).

4.3.19 Security testing

- Security testing should be carried out where possible. It is rarely possible to do security testing in the live environment, so testing should be done in dedicated testing environments or on backup systems, where available, or during plant shut downs.
- All IP enabled control devices should undergo security testing to gain an understanding of what services and sorts are available and to provide assurance that they do not posses any known vulnerabilities.

Further details on penetration testing can be found in the CPNI guide (see appendix A for the location of this guide). This guide is a general document and is not specific to process control and SCADA systems.

4.3.20 Device connection procedures

- Establish a procedure to verify that devices are free from virus or worm infections before being connected to process control networks.

The detailed good practice guide can be found at:
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

5. ESTABLISH RESPONSE CAPABILITIES

5.1 Overview

Implementing security mechanisms across process control systems is not a one off exercise. Threats to the security and operation of process control systems develop and evolve over time and organisations should therefore undertake continuous assessment of process control system security. This includes identifying, evaluating and reacting to new vulnerabilities, changes in security threats and electronic security incidents (e.g. worm or hacker attacks). Establishing formal response management processes ensures that any changes to risks are identified as early as possible and any required corrective action embarked on quickly.

5.2 Objective

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

5.3 Principles of good practice

- Form a Process Control Security Response Team (PCSRT) to respond to suspected security incidents. A CNI company wishing to establish a PCSRT can approach CSIRTUK for advice and support.
- Ensure that appropriate electronic security response, business continuity and recovery plans are in operation for all process control systems.
- Ensure that all electronic security plans are regularly maintained, rehearsed and tested.
- Establish an early warning system that notifies appropriate personnel of security alerts and incidents.
- Establish processes and procedures to monitor, assess and initiate responses to security alerts and incidents. Possible responses may include: increase vigilance, isolate system, apply patches, or mobilise the PCSRT.
- Ensure all process control security incidents are formally reported and reviewed and lessons learnt are captured.

The detailed good practice guide can be found at:
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

6. IMPROVE AWARENESS AND SKILLS

6.1 Overview

A holistic approach to security includes technical, procedural and social appreciation – the success of any technical or procedural security protection measure is ultimately dependent upon the human component. Employees are both the most important resource and the biggest threat to security. Process control system personnel are often unfamiliar with IT security and IT security personnel are often unfamiliar with process control systems and their operating environment. This situation can be improved by increasing understanding through general awareness programmes, education and by increasing skills through training.

6.2 Objective

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

6.3 Principles of good practice

6.3.1 Increase awareness

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

6.3.2 Establish training frameworks

- Coach IT personnel to develop an appreciation and understanding of the process control systems and their operating environments, highlighting the differences between the security of process control systems and IT security.
- Develop appropriate IT security skills within process control teams and/or provide appropriate IT support services.

6.3.3 Develop working relationship

- Establish links between IT security and process control teams to build working relations, share skills, and facilitate knowledge transfer.

The detailed good practice guide can be found at:
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

7. MANAGE THIRD PARTY RISK

7.1 Overview

The security of an organisation's process control systems can be put at significant risk by third parties, for example, vendors, support organisation and other links in the supply chain, and therefore warrant considerable attention. Technologies that allow greater interconnectivity, such as dial-up access or the internet, bring new threats from outside of the organisation. Third parties must therefore be engaged and steps taken to reduce these potential risks.

7.2 Objective

To ensure that all security risks from vendors, support organisations and other third parties are managed.

7.3 Principles of good practice

7.3.1 Identify third parties

- Identify all third parties, including vendors and service providers, and all other links in the supply chain that are associated with the process control systems.

7.3.2 Manage risk from vendors

- Ensure that security clauses are detailed in all procurement contracts prior to agreements.
- Engage with all vendors on an ongoing basis to ensure that any current and future discoveries of vulnerabilities within the systems that they supply are identified and notified promptly to the user organisation.
- Request vendors to provide security guidance for their current control systems and a security roadmap for future system development.
- Ensure that all vendors incorporate appropriate anti-virus protection within their process control systems.
- Establish with the vendor an effective software patching process.
- Agree with the vendor system hardening procedures for the process control systems in operation.
- Identify all component technologies (e.g. databases) used within the process control systems to ensure that all vulnerabilities are managed.
- Undertake regular security reviews and audits of all vendors.

7.3.3 Manage risk from support organisations

- Undertake regular risk assessments of support organisations and ensure any required countermeasures are implemented.
- Prevent access to the process control systems by support organisations until appropriate measures to prevent or reduce potential security breaches have been implemented. Issue and agree a contract defining the terms of the connection.
- Engage with all support organisations on an ongoing basis to ensure that any current and future discoveries of vulnerabilities within their systems that interact with the enterprise process control systems are identified and notified to the user organisation.

- Increase awareness of all support organisations to fully understand the process control systems that they are supporting and agree to undertake such support in accordance with agreed security procedures.

7.3.4 Manage risk in the supply chain

- Engage with any organisation linked to the process control systems through the supply chain to provide assurance that their process control security risks are managed. Examples of such organisations might include: suppliers, distributors, manufacturers, or customers.

The detailed good practice guide can be found at:
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

8. ENGAGE PROJECTS

8.1 Overview

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 risks by integrating protection measures into the project development processes at an early stage is more effective, avoids overruns and is usually less costly.

8.2 Objective

To ensure that all projects and initiatives that may impact the process control systems are identified early in their life cycle and include, appropriate security measures in their design and specification.

8.3 Principles of good practice

- Identify and engage all projects that have 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).

The Cyber Security Procurement Language for Control Systems document by Idaho National Laboratory provides further details on this subject (see appendix A).

The detailed good practice guide can be found at
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

9. ESTABLISH ONGOING GOVERNANCE

9.1 Overview

Formal governance for the management of process control systems security will ensure that a consistent and appropriate approach is followed throughout the organisation. Without such governance the protection of the process control systems can be ad-hoc or insufficient, and expose the organisation to additional risks. An effective governance framework provides clear roles and responsibilities, an up-to-date policy and standards for managing process control security risks, and assurance that this policy and standards are being followed.

9.2 Objective

To provide clear direction for the management of process control system security risks and ensure ongoing compliance and review of the policy and standards.

9.3 Principles of good practice

9.3.1 Define roles and responsibilities

- Appoint a single point of accountability for process control security risks.
- Define roles and responsibilities for all elements of process control security.
- Obtain senior management support for process control system security.

9.3.2 Develop policy and standards

- Define, document, disseminate and manage under change control, formal policy and standards for process control system security. Ensure that the policy and standards accurately reflect the organisational requirements, support business requirements and are agreed to by all relevant parties.
- Identify impacts of legal and regulatory requirements on process control security. Ensure that these are built into the policy and standards.
- Ensure process control system security practices align with the business and operational needs.

9.3.3 Ensure compliance with policy and standards

- Implement an assurance programme to ensure that the process control system policy and standards are complied with on a continuous basis.

9.3.4 Update policy and standards

- Establish an ongoing programme to ensure that the process control security policy and standards are regularly reviewed, updated in-line with current threats and changes in legal and regulatory requirements and changes in the business and operational requirements.

The detailed good practice guide can be found at:
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

APPENDIX A: DOCUMENT AND WEBSITE REFERENCES USED IN THIS GUIDE

Section 2.2.1
Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Environments
http://csrp.inl.gov/Documents/Opsec%20Rec%20Practice.pdf

Section 4.3.2
Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
www.cpni.gov.uk/Docs/re-20050223-00157.pdf

Section 4.3.10
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/Documents/Wireless%20802.11i%20Rec%20Practice.pdf

Section 4.3.11
Good Practice Guide Patch Management
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

Section 4.3.12
A Good Practice Guide on Pre-Employment Screening
www.cpni.gov.uk/Products/bestpractice/3351.aspx

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

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/

Section 4.3.18
Best Practice Guide Commercially Available Penetration Testing
www.cpni.gov.uk/Docs/re-20060508-00338.pdf

Section 8.3
Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

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