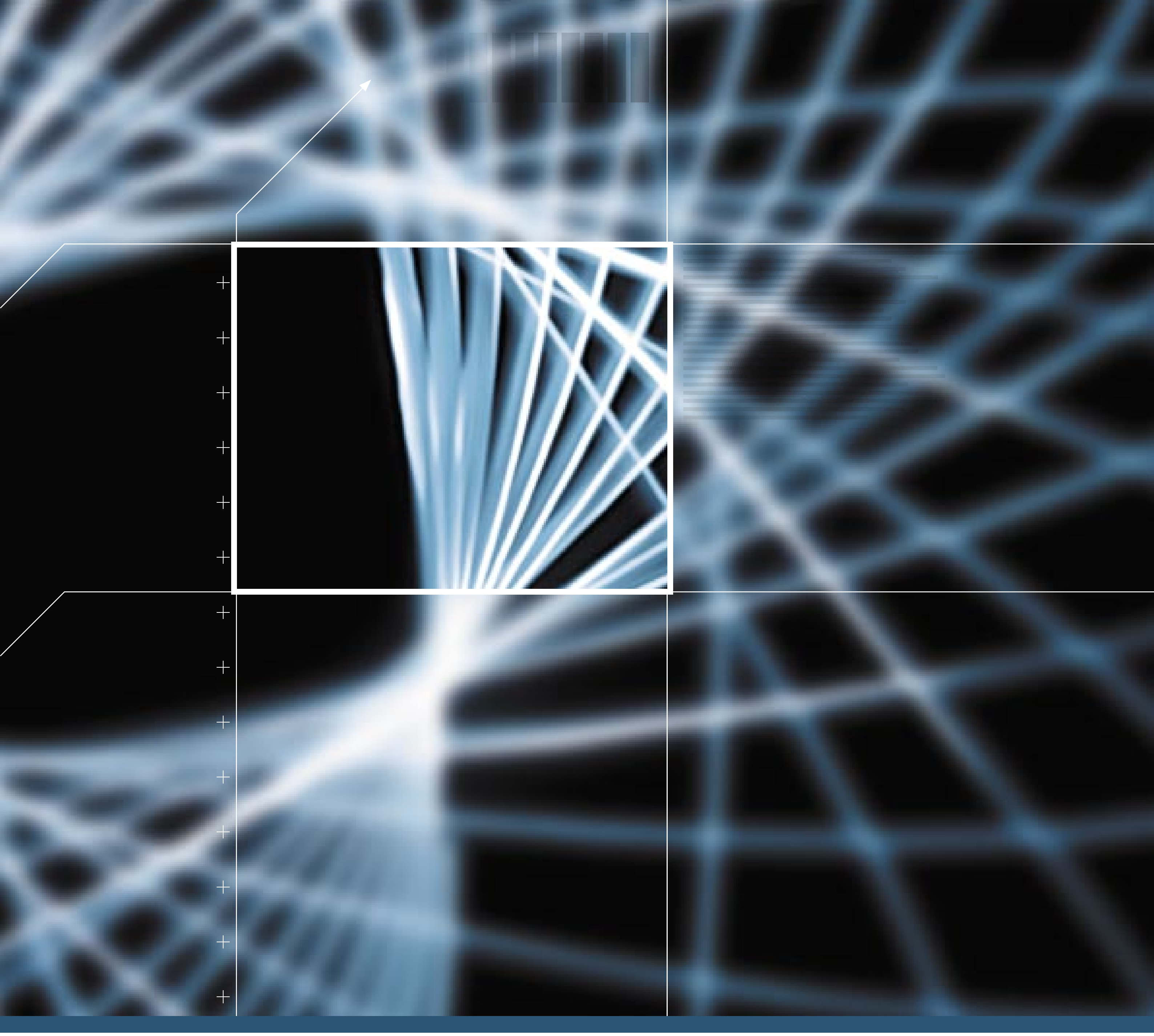

GOOD PRACTICE GUIDE

PROCESS CONTROL AND SCADA SECURITY

GUIDE 5. MANAGE THIRD PARTY RISK

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.

Disclaimer
Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favouring by CPNI or PA Consulting Group. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

CPNI and PA Consulting Group shall also accept no responsibility for any errors or omissions contained within this document. In particular, CPNI and PA Consulting Group shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

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.

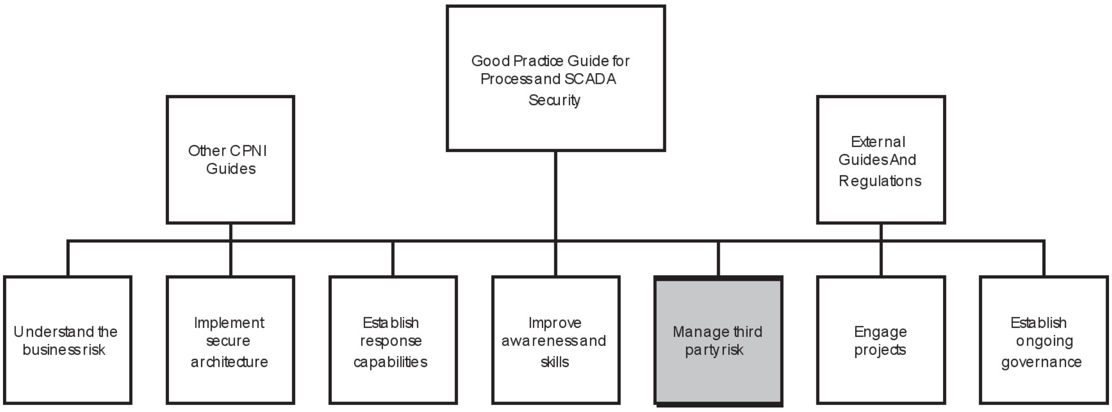
Good Practice Guide for Process and SCADA Security
Other CPNI Guides
External Guides And Regulations
Understand the business risk
Implement secure architecture
Establish response capabilities
Improve awareness and skills
Manage third party risk
Engage projects
Establish ongoing governance

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 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 **'Manage Third Party Risk'** guide builds on the foundation provided in the high level good practice guide and provides good practice guidance managing third party risks to process control system security.

This guide does not provide detailed policies or methodologies.

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

2. MANAGE THIRD PARTY RISK SUMMARY

The security of an organisation's process control systems can be put at significant risk by third parties, e.g. vendors, support organisations and other links in the supply chain, and therefore warrants 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 as part of the process control security programme and steps should be taken to reduce the associated risk.

In the past process control systems were often bespoke systems that were written in house. Nowadays most control systems are developed by specialist third parties and vendors. Consequently third party products and services are present in almost all process control systems, and with them are a number of associated risk factors.

Awareness or visibility of the third party risk is the key to enabling an organisation to begin to manage them. The recognition of potential security gaps enables the organisation to seek appropriate engagement with vendors and support organisations in order to mitigate the identified risk.

The common perception of third party risk, relating to process control systems focuses on remote access connections to the operational control systems. However, the picture is much wider than this technical concern hence the need for a good practice guide in this framework dedicated to the topic. There are different categories of third parties such as control system vendors, support providers and different elements in the supply chain. Each of these has their own related issues.

When considering the vulnerability of process control systems the importance of assessing the wider supply chain can easily be overlooked. Seemingly innocuous systems that provide systems support can have significant direct or indirect impact on critical systems.

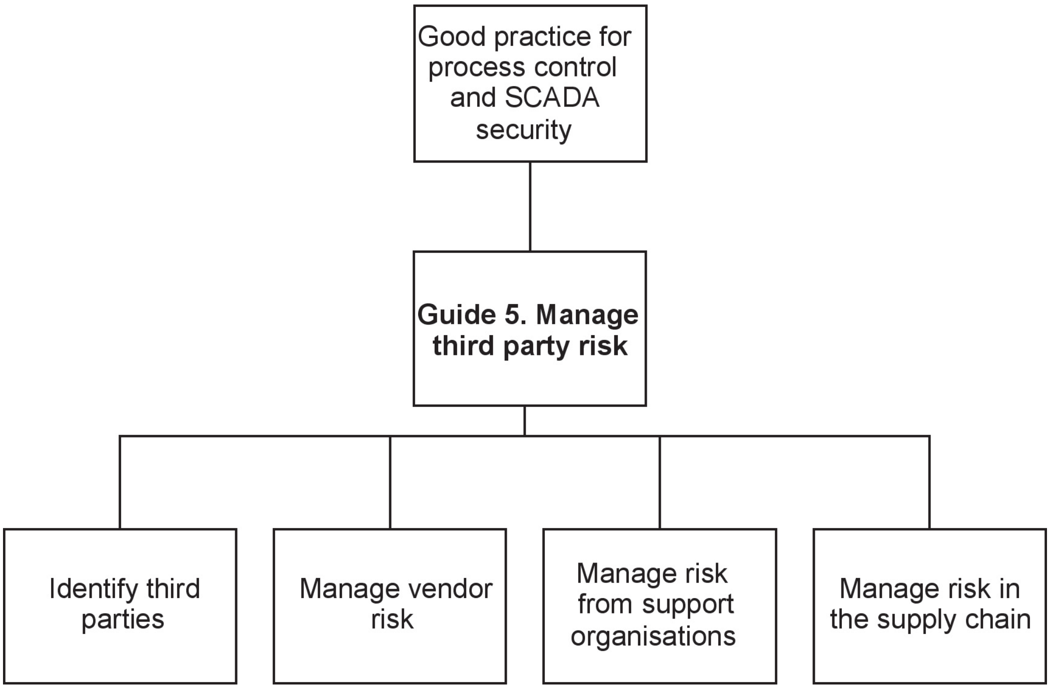
Good practice for process control and SCADA security
Guide 5. Manage third party risk
Identify third parties
Manage vendor risk
Manage risk from support organisations
Manage risk in the supply chain

Figure 2 – Manage third party risk document structure

3. IDENTIFY THIRD PARTIES

3.1 Context of this section within the overall framework

This element of the framework focuses on identifying all the third parties that relate to the security of process control systems. This involves reference to the process control security inventory produced in the Understanding Business Risk framework element. This section references the inventory to identify relevant third party risk in order to ensure that they are appropriately managed.

Within this guide identifying third parties is the foundation for the remaining three sections.

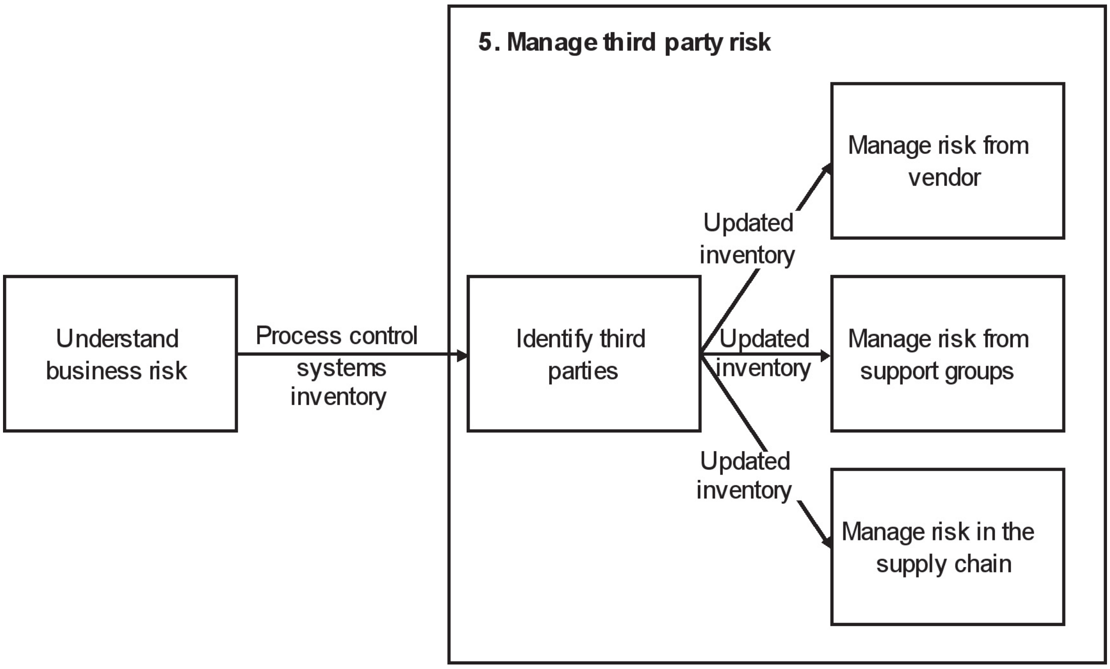
5. Manage third party risk
Understand business risk
Process control systems inventory
Identify third parties
Updated inventory
Updated inventory
Updated inventory
Manage risk from vendor
Manage risk from support groups
Manage risk in the supply chain

Figure 3 – Where 'identify third parties' fits in the framework

3.2 Rationale

The identification of which third parties are associated with process control assets enables the organisation to plan and mitigate the risk that they pose.

3.3 Good practice principles

The relevant good practice principle in the overarching document Good Practice Guide Process Control and SCADA Security, is:

- 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.

3.4 Good practice guidance

This section requires the existence of a process control system inventory which provides the starting point for identifying all third parties. The production of a process control security inventory is described in the 'Understand the Business Risk' guide. For each item in the inventory, determine what (if any) third parties are associated with each item. It could be that an inventory item could be associated with a number of different third parties. When performing this analysis the following questions should be considered:

- Who is the system vendor?
- Who provides support?
- How is the support provided?
- What service level agreements exist?
- Which sub-contractors are involved?

Definitions:

Vendor – A person, organisation or integrator that provides software, hardware, firmware and/or documentation to the organisation for a fee or in exchange for services.

Support – The 'provision of capabilities for' or the ability 'to interface to' the process control systems. e.g. monitoring systems, resetting passwords, problems, bug fixes, etc.

Sub-contractor – Person or entity that enters into a contractual agreement with a prime contractor to perform a service or task.

The length of the initial third party inventory review is entirely dependent on the size of the inventory created. Care should be taken to strike an appropriate balance when capturing the third party data. If too little is recorded then it may not be enough for further analysis during later stages. If too much is captured then it will be difficult to maintain. Where third party information wasn't available in sufficient detail during the inventory collation, this information should be sought as part of this element of the framework. Any new information should be added to the inventory to keep it up to date.

4. MANAGE RISK FROM VENDORS

4.1 Context of this section within the overall framework

Managing the risk from vendors builds on the previous section identify third parties and focuses specifically on working with the vendors of the process control systems. The output from this section is used in the Implementing Secure Architecture and Establishing Response Capabilities framework elements.

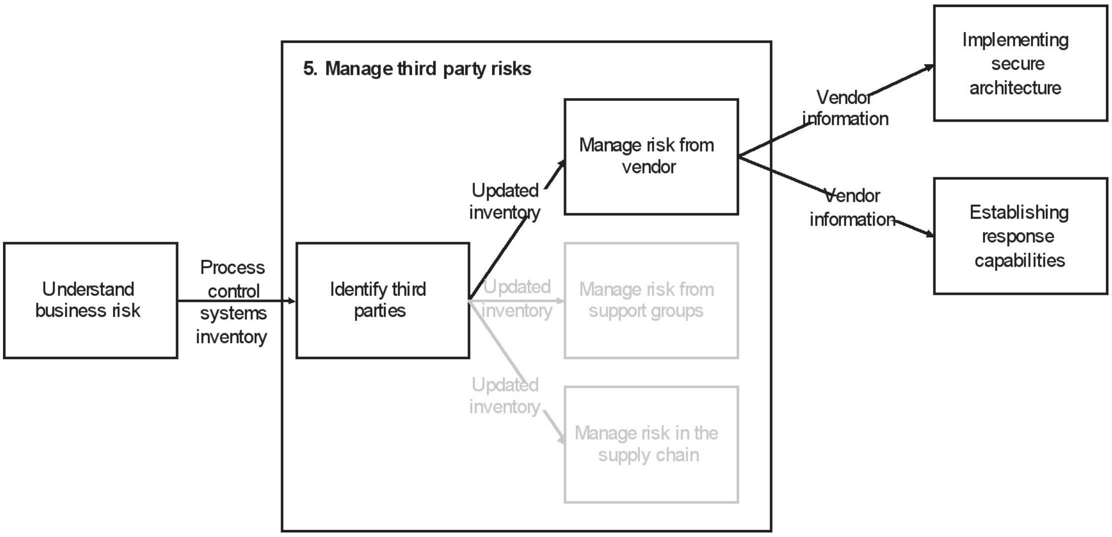
5. Manage third party risks
Understand business risk
Process control systems inventory
Identify third parties
Updated inventory
Manage risk from vendor
Updated inventory
Manage risk from support groups
Updated inventory
Manage risk in the supply chain
Vendor information
Vendor information
Implementing secure architecture
Establishing response capabilities

Figure 4 – Where 'manage vendors risk' fits in the framework

4.2 Rationale

By developing relationships with control system vendors, organisations can influence the design of process control systems and influence the security functionality of both existing and new products.

4.3 Good practice principles

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

- 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.

4.4 Good practice guidance

By engaging in productive dialogue with the process control system vendors, the organisation has an opportunity to build a relationship with them so that it can better understand the capabilities and limitations of the vendor's products and services. This relationship will also enable the organisation to better communicate their specific application needs and the associated security requirements to the vendor.

There are a number of key security aspects that will benefit from a two-way dialogue with vendors which are described in the following sections.

4.4.1 Contractual measures to manage vendor risk

Creating the correct contractual framework is an essential part of managing vendor risk. Much of the hard work is likely to have been done by either the organisations legal or procurement departments but it is important to ensure that specific process control security clauses are included within any contracts with vendors. Typical security clauses include:

Non-disclosure agreement: the vendor may be exposed to sensitive information about the organisation and it is essential that this does not get exploited or used without the permission of the organisation. This can range from an understanding of the firewall rules to system information and other intellectual property.

Vulnerability disclosure: it is important that current and future vulnerability discoveries are communicated by the vendor to system owner so that appropriate action can be taken.

Background checks/ internal security checks: the organisation should request assurance from vendors that staff have had the relevant background security checks prior to being engaged in full term employment or on contracts. Further details on pre-employment screening can be found in the CPNI guide, A Good Practice Guide on Pre-Employment Screening, on the CPNI's Personnel Security Measures website and within BS7858, locations of these documents can be found in Appendix A.

Vendor accreditation: building process control security requirements into preferred vendor selection and accreditation is an extremely powerful process to ensure that the desired security culture and approach is embedded in procurement decisions. The resulting approved vendor list can save the organisation time and money by reducing duplication and providing assurance about potential vendors. From the vendor perspective there is an incentive to get on approved vendor list as this can be a good source of business.

Security requirements for new projects: where projects for new processes or new systems are planned it is essential that security is included early on in contractual discussions, particularly if new vendors are involved. Please refer to the Guide 6 Engage Projects.

Security reviews: regular security performance reviews should be undertaken with the vendor to discuss outstanding security issues, progress against mitigation and improvement plans and to discuss the security road map.

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

4.4.2 Key vendor related topic areas to consider

By working with the vendor there are a range of ways to manage the mitigation of vendor related risk, examples include:

Anti-virus: work with vendors to ensure that anti-virus protection is incorporated into their control systems.

Patching process: agree with the vendor what process they will use for testing and accrediting security patches. Questions that should be considered are:

- Do they accredit patches?
- Will they notify customers and deploy accredited patches?
- How long does it take to accredit?
- Are there installation notes or guidance on the patches that should be deployed?

Some vendors are keen to test all security patches prior to approval for deployment. This may involve a stipulation that only patches and updates received directly from the vendor are valid for updating the system. There can be a delay involved with this approach, so it is important to work closely with the vendor to ensure that the security needs of the organisation are met, and that the vendor is aware of any additional delays that are imposed by the organisation (e.g. change control).

System hardening guidance: most process control systems and devices are initially provided quite open, meaning that they will be enabled to perform their full range of functionality. Given that your organisation will have relatively specific requirements, it is important that the remaining unused functionality is disabled to prevent unnecessary security risk. The vendors should be engaged to provide guidance on locking down or hardening the systems.

Component technologies: some process control applications have component technologies that pose a potential security risk. A number of process control systems that have database components which are often not too visible to the user but which may require patching and maintenance.

Remote support: the main risk area that needs to be addressed through engagement with vendors is remote support. Such support should be provided through a secure connection but the story does not stop there. The systems from which the vendors connect should also be secure, both physically and electronically. The personnel that connect in should have completed background checks and be appropriately trained and any client confidential information (such as system documentation) should be appropriately secured. Organisations should seek assurance (possibly through site visits or audits) on these topics.

Security Testing: organisations should encourage vendors to undertake security testing of their products to identify and eliminate security vulnerabilities. This may take the form of system design review, lab testing or penetration testing. Recent research had highlighted a number of security vulnerabilities in low level control devices such as remote terminal units (RTUs) and programmable logic controllers (PLCs). Organisations should seek assurance from suppliers and vendors that these low level control devices have been appropriately analysed to identify what ports and services are being used and whether there are any known vulnerabilities. Organisations should require the vendors to carry out testing on control systems and their components (such as PLCs) to ensure they are free from security vulnerabilities. Further guidance on testing and assurance of embedded control devices is in Guide 6 Engage Projects in this framework.

Disclosures of system communications: organisations should encourage vendors to detail which ports are used along with the protocols used.

4.4.3 Embedding the security culture in vendors

The organisation should be looking to influence the vendor's security culture so that it meets or exceeds the organisation's requirements. Typical activities that create a solid security culture and that should be encouraged or even mandated with vendors include:

- Regular security reviews
- Security audits
- A culture of security and awareness
- Open dialogue about vulnerabilities
- Security roadmap for vendor improvements
- Relationships with security vendors.

4.4.4 Influencing the vendor security roadmap

A key benefit of building a good working relationship with vendors, is the opportunity of working with them to influence the direction and pace of their security development i.e. the vendor's security roadmap. This is a potential 'win-win' as the vendor can get valuable market insights and the organisation can mitigate vulnerabilities through improving the vendor's products and services.

Recent advances in the accreditation of anti-virus software and operating system patches by a number of key vendors has been influenced to some extent by the purchasing power of a number of large organisations looking to improve the security of process control systems. By engaging in an ongoing dialogue with the vendors organisations were able to communicate their priorities and concerns at the inability to protect against viruses. The communication of these requirements from a number of organisations enabled the vendors to build business cases to allow for research and development in this area. This has resulted in better security features in the control system products.

5. MANAGE RISK FROM SUPPORT ORGANISATIONS

5.1 Context of this section within the overall framework

Manage risk from support organisations builds on the identified third parties and focuses specifically on working with support organisations. The outputs from this section may be used in the 'Implement Secure Architecture', 'Establish Response Capabilities' and 'Improve Awareness and Skills' elements of the good practice framework.

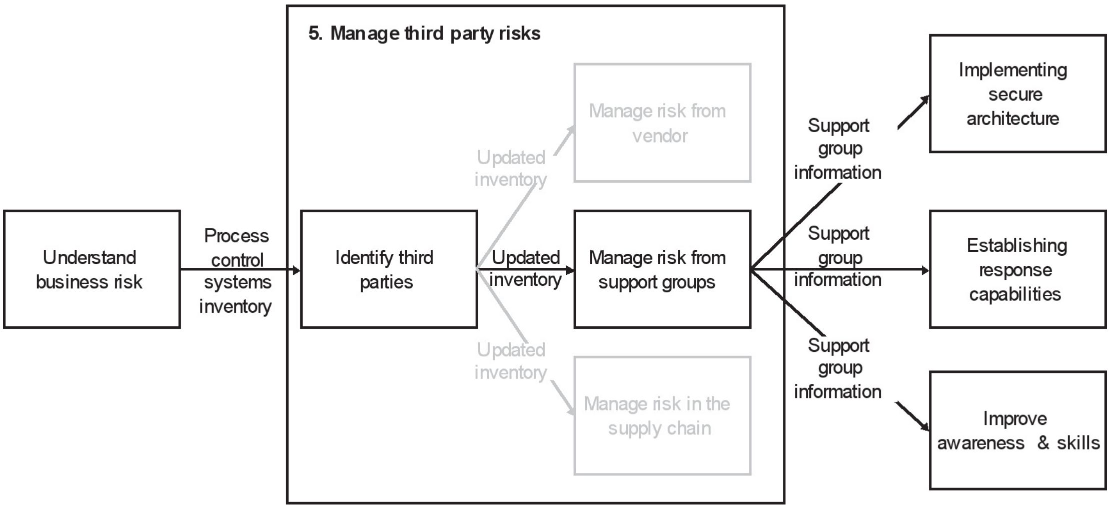
5. Manage third party risks
Understand business risk
Process control systems inventory
Identify third parties
Updated inventory
Manage risk from vendor
Updated inventory
Manage risk from support groups
Updated inventory
Manage risk in the supply chain
Support group information
Support group information
Support group information
Implementing secure architecture
Establishing response capabilities
Improve awareness & skills

Figure 5 – Where Manage Risk from Support Groups fits in the framework

5.2 Rationale

By developing a relationship with third party support organisations the related potential security risk can be managed.

5.3 Good practice principles

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

- 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. This is 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

5.4 Good practice guidance

As with many areas within the IT environment, there are many process control system that are supported in some way by third parties. Consequently the security of process control systems is often critically dependent on the support organisation and the services that they provide, such as:

- network and telecommunications provision and support
- IT infrastructure management
- application and system monitoring and support.

Third party support of process control systems enables an organisation to receive specialist support whilst also reducing the cost associated with training and recruitment. When new technologies or services are introduced it is the third party who must ensure that they have the appropriate resources to provide effective support.

In addition to the common services described above, organisations may wish to consider increased use of third parties to provide additional security and administration services as part of the wider security architecture. Examples of such services include:

- System operation, security and performance monitoring
- Security patching
- Firewall management and monitoring
- Intrusion detection monitoring
- Anti-virus protection
- Regular security monitoring routines e.g. log monitoring, remote access connections, password changes etc.

Choosing which services could be supported by a third party needs to be based on the criticality of the system, the support required, availability of appropriately skilled internal resources and maintenance scope.

Further details on outsourcing can be found in the CPNI guide, the location of this guide can be found in appendix A.

Engaging third party support organisations to support process control systems can introduce risk as well as being part of the security solution. The key risk areas that should be considered are:

- Remote support connections
- Personnel security
- Contractual issues
- Security awareness and training.
- Physical security
- Confidentiality.

Each of these topics is discussed further in the following sections.

Third party support organisations often perform similar functions and services to control system vendors. Consequently the good practice principles are very similar to those drawn up for managing vendor risk and focus on the need to have clear contractual agreements, good working relationships and clear communication channels.

5.4.1 Remote support connections

Third party support must ensure that any new technology introduced to a secure process control system is authorised by the organisation. The addition of devices such as modems or routers to enable remote or out-of-hours support are a potential risk and must only be used with the prior authorisation of the organisation and should be appropriately secured. There is likely to be a trade-off between convenience and security and many third parties may offer significant price reductions by offering remote support. To minimise the risk associated with remote access/ support the following must be considered:

- Deny access until connections are protected
- Ensure that access rights are regularly reviewed and audited
- Ensure that facilities and systems from which the support organisation connects should also be secure, both physically and electronically
- Ensure that all client confidential information (such as system documentation) is stored securely
- Connections have a time limited applied.

Organisations may wish to obtain assurance on the above topics via site visits, reviews or audits.

5.4.2 Personnel security

A key part in any system security framework is the human element. Personnel security aspects should be considered when assuring the security of third parties.

All personnel should complete appropriate background security checks as a routine part of the third parties' recruitment process.

Further details on pre-employment screening can be found in the CPNI guide, A Good Practice Guide on Pre-Employment Screening and within BS7858, locations of these documents can be found in appendix A.

CPNI provide advice on the continual screening of employees as well as pre-employment screening (see appendix A).

5.4.3 Vendor contractual issues

There are a number of security elements that should be considered in any third party support contracts:

- **Right to audit** – Include clauses to ensure the right to audit or review third party services, systems and premises.
- **Confidentiality of information** – Include clauses to ensure the confidentiality of client confidential information (such as system documentation). Ensure a non disclosure agreement is in place.

- **Appropriate service level agreements** – Ensure that the service levels are clearly defined in the contract and that they are appropriate to the organisation's requirements.

5.4.4 Security awareness and training

Third party support personnel should have an appropriate level of security awareness. Not everyone needs to be a security expert but individuals should have the appropriate technical, procedural and operational security awareness to perform their role securely. Topics may include:

- **Policy and standards** – ensure that all personnel are aware of what policies and standards are in place for the systems being supported.
- **Specific business security processes** – the organisation may have specific security processes that will need to be communicated to third parties
- **Response and continuity planning** – ensure that a third party support organisation has appropriate response and continuity plans in place
- **Skills** – ensure that personnel have the practical skills and training to perform the support function. There are a number of industry standard qualifications associated with security and support, but it is important to gain assurances that the personnel have both the appropriate practical knowledge and formal qualifications.

Further information can be found in the 'Improve Awareness and Skills' good practice guide.

6. MANAGE RISK IN THE SUPPLY CHAIN

6.1 Context of this section within the overall framework

This element of the framework focuses on identification of connections and dependencies within the supply chain that were identified in the Understand the Business Risk element and managing the associated risk. The two key outputs of this element are 'Implement Secure Architecture' and 'Establish Response Capabilities'.

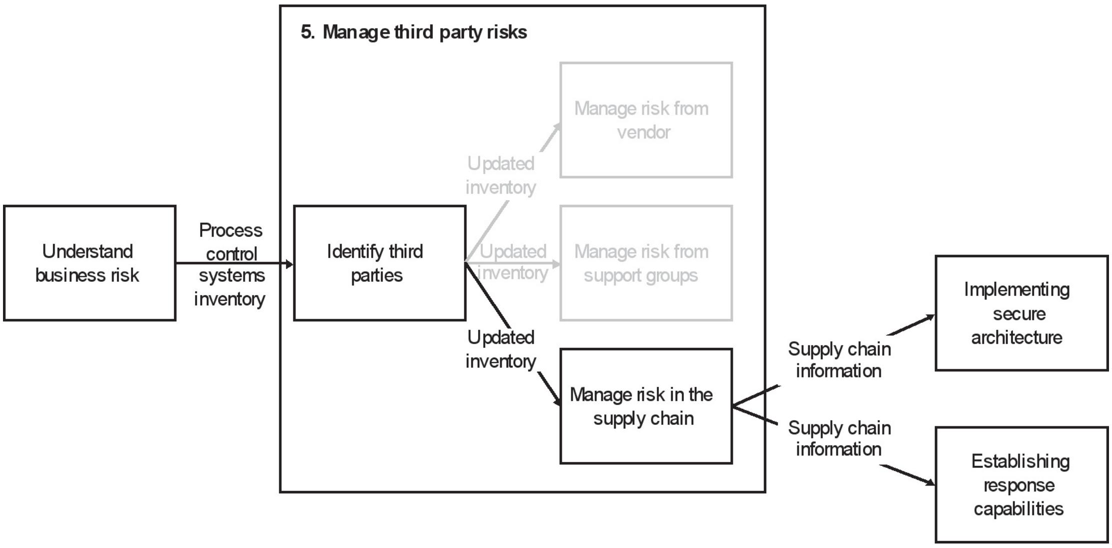
5. Manage third party risks
Understand business risk
Process control systems inventory
Identify third parties
Updated inventory
Manage risk from vendor
Updated inventory
Manage risk from support groups
Updated inventory
Manage risk in the supply chain
Supply chain information
Implementing secure architecture
Supply chain information
Establishing response capabilities

Figure 6 – Where Manage Risk in the Supply Chain fits in the framework

6.2 Rationale

Linking process control systems to other elements in the supply chain can provide significant business benefits in terms of lower costs and increased efficiencies. However such connections can introduce security risk through the implementation of network or system connections to external systems. Tighter integration into the supply chain can introduce harder dependencies and make the whole chain less resilient to disruptions to individual systems in the supply chain. Consequently a security event in one system in the supply chain could impact the whole chain and cause disruption to many other systems – possibly across a number of different organisations. Where systems form part of a larger supply chain it is important to assess the upstream and downstream dependencies and ensure all systems are appropriately protected with security measures and response capabilities.

6.3 Good practice principles

The relevant good practice principle in the overarching document 'Good Practice Guide Process Control and SCADA Security', is:

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

6.4 Good practice guidance

The fundamental requirements in managing risk in the supply chain are to understand the supply chain itself and the dependencies that exist within it. The organisation should also identify the critical paths with the supply chain. Where systems or connections span organisational boundaries, clear arrangements for security responsibilities should be agreed by the relevant parties.

There is a danger that many of the specific functions or processes within a supply chain operate in a 'silo' mentality, only concerned with what they need to do and not focussed on risk in the wider supply chain view.

Supply chain connections will vary significantly from one industry to another. Examples of some third party supply chain connections are:

- between power generation and distribution, transmission or energy trading systems
- between oil and gas production systems and trading systems
- to automated stock ordering systems
- to pipelines (upstream and downstream)
- to tanker loading facilities
- to utilities providers (e.g. gas, water, electricity, compressed air, steam etc.)
- to joint venture partners for production reporting.

There are two key risk areas that should be considered for each supply chain interface:

- interface security
- supply chain dependencies.

6.4.1 Interface security

System interfaces between process control systems can be a potential backdoor into the control systems and could provide a route for infection from viruses and worms or unauthorised access. Such connections might take a variety of forms, serial lines, modem connections, VPNs or connections via other networks or potentially the internet.

All such connections should be clearly identified, included in the process control system inventory, documented in system and network diagrams and should be appropriately secured and monitored. Disconnection plans should be established as part of the response and continuity plans.

In addition to considering these connections for interface security the connections should also be considered for dependencies as described below.

6.4.2 Supply chain dependencies

Each element in the supply chain should be assessed in terms of process control security threats. Where there are critical dependencies, i.e. where the organisation's systems are dependent upon other systems (either upstream or downstream), then assurance should be sought from the relevant third parties about how those systems are protected from a process control security point of view. In order to gain this assurance, organisations may consider security reviews, health checks or audits. If deemed necessary, appropriate response and continuity plans should be put in place for each supply chain dependency.

APPENDIX A: DOCUMENT AND WEBSITE REFERENCES USED IN THIS GUIDE

Section 4.4.1

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/

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

Section 5.4.2

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/

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