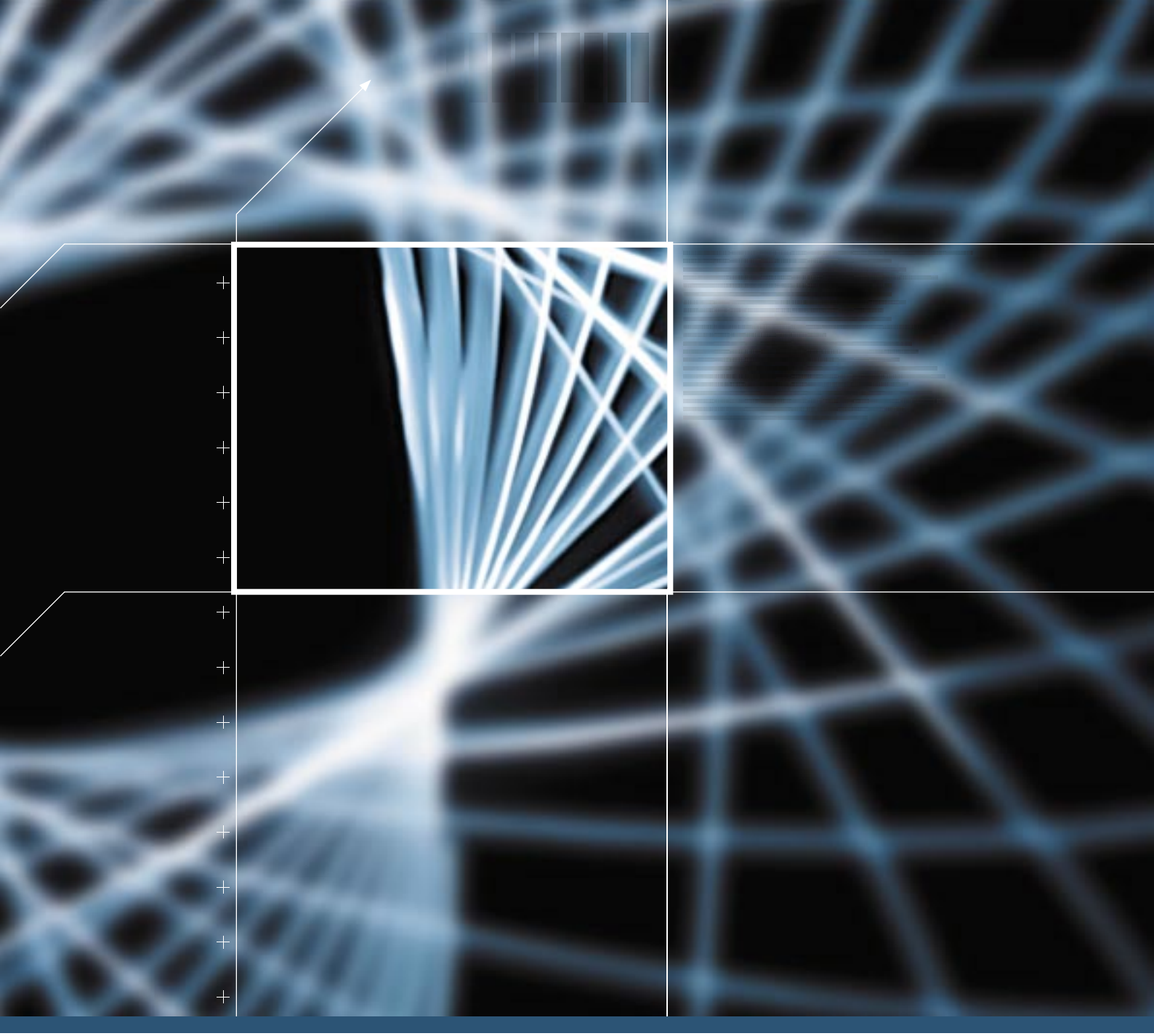

# GOOD PRACTICE GUIDE

## PROCESS CONTROL AND SCADA SECURITY

GUIDE 1. UNDERSTAND THE BUSINESS 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.

# 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.

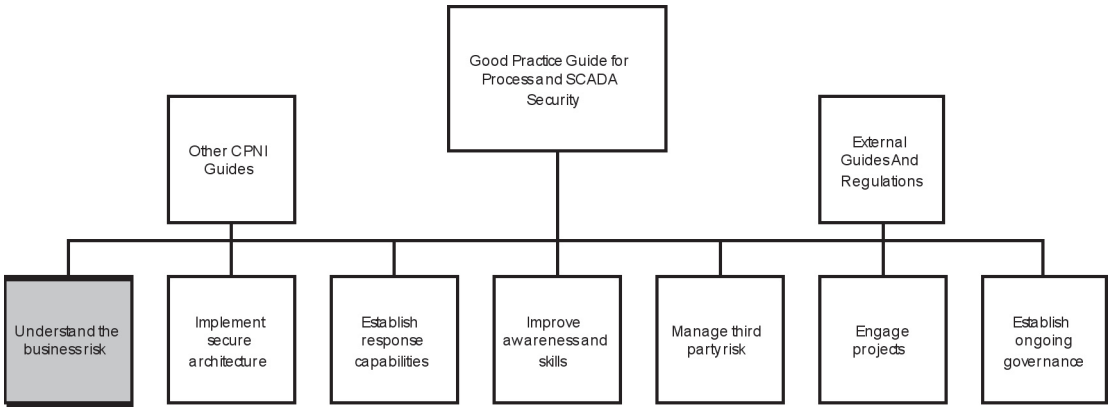


**Figure 1 – Where this guide fits in the Good Practice Guide framework**

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 '**Understand the Business Risk'** guide builds on the foundation provided in the high level good practice guide and provides guidance on assessing the business risk and ongoing assessment of this risk.

This guide does not provide detailed risk assessment techniques 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 telemetry engineers
- Information security specialists
- Physical security specialists
- Business leaders
- Risk managers
- Health and safety officers
- Operations engineers
- Auditors.

# 2. UNDERSTAND THE BUSINESS RISK SUMMARY

The first step in improving the security of process control systems is to gain a thorough understanding of the business risk in the context of electronic security. 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 what should be the appropriate levels of security protection.

Any security improvements should be based on the level of risk facing a particular system to ensure that an appropriate level of protection is provided. For example a low risk system is likely to require less protection than a high risk system. However these protection measures need to be correctly deployed in order to achieve the full security benefit. An understanding of the business risk is a key driver to where such protection measures are deployed.

Understanding the business risk is not a one off exercise – it is an ongoing process. Once a risk assessment has been carried out and the relevant security improvement measures have been implemented, it is important to maintain an ongoing view of the business risk as time progresses, threats change and more vulnerabilities are identified.

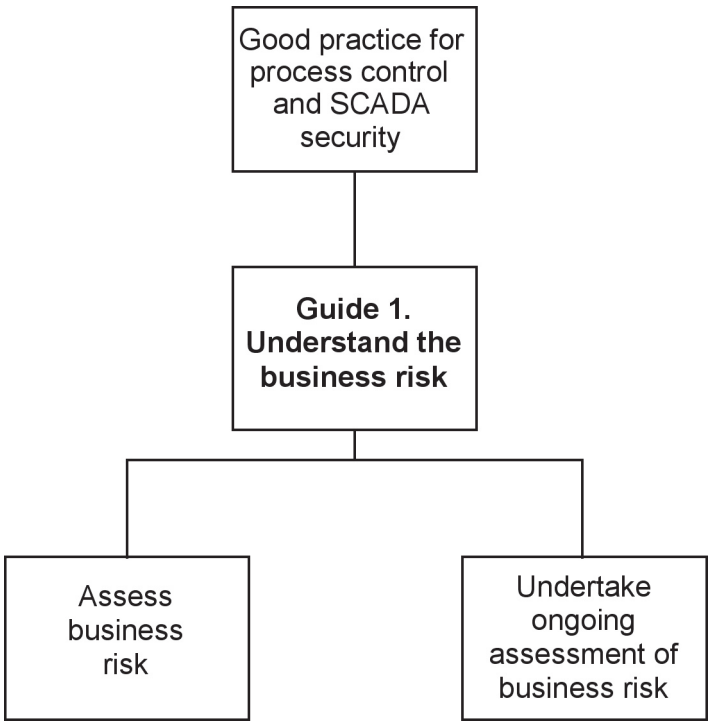


**Figure 2 – Understand the business risk document structure**

## Definitions

**Risk** – Possibility of an event occurring that will have a negative impact on the control system. The event may be the result of one threat or a combination of threats.

**Risk appetite** – The level of risk, used to determine what an acceptable risk is.

**Threat** – Any circumstance or event with the potential to harm an process control and SCADA system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

**Likelihood** – The probability of a specified outcome.

**Impact** – The consequences of a threat taking place.

**Vulnerability** – The degree to which a software system or component is open to unauthorized access, change, or disclosure of information and is susceptible to interference or disruption of system services.

# 3. ASSESS BUSINESS RISK

## 3.1 Context of this section within the overall framework

Assessing the business risk is the precursor to all of the subsequent themes within this process control security framework and the output of this activity is used in a variety of other framework elements.

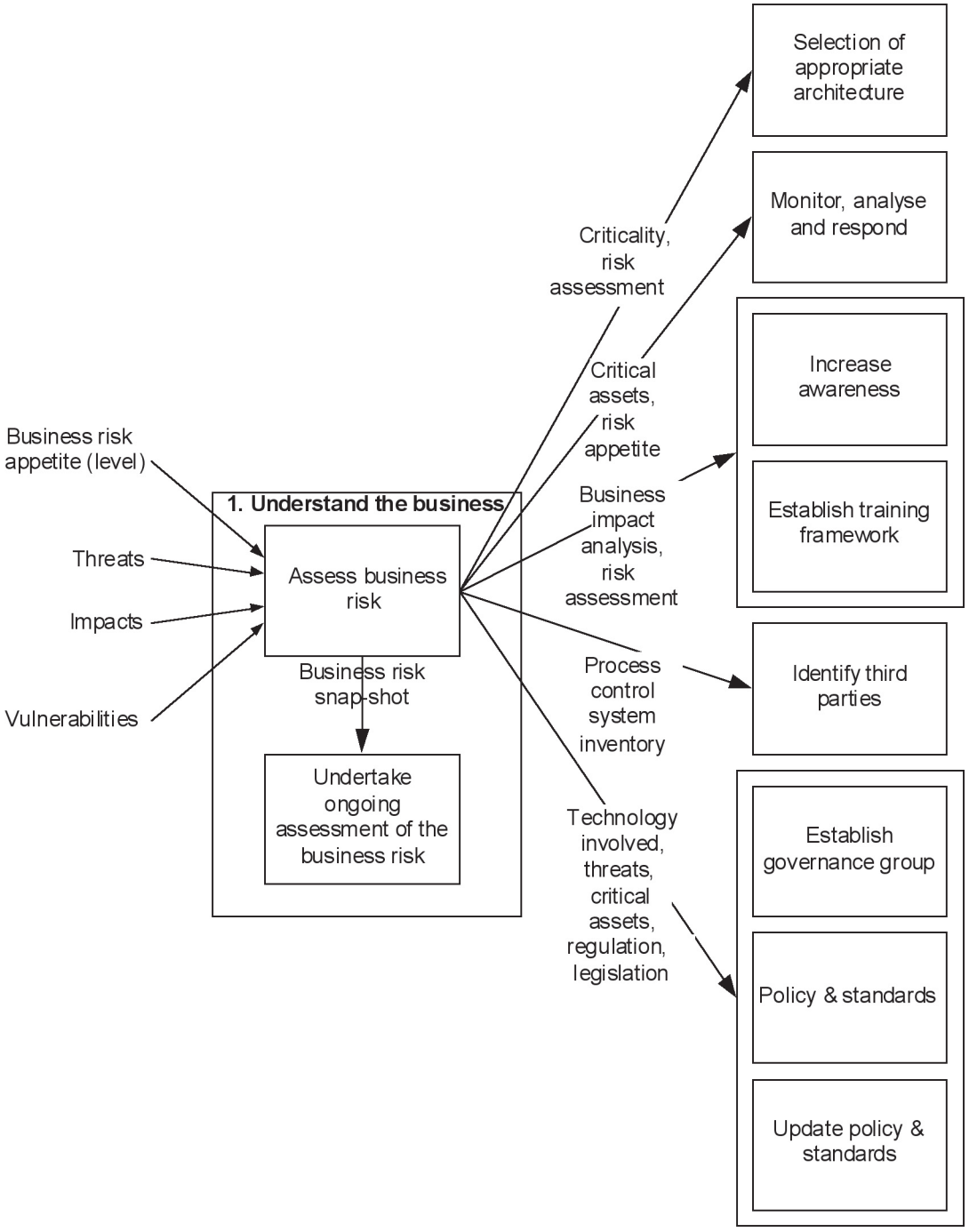


**Figure 3 – Where 'Assess business risk' fits in the framework**

## 3.2 RATIONALE

Organisations need to understand the risk that their businesses are facing in order to determine what an appropriate risk appetite (risk level) is, and what security improvements are required in order to reduce the level of risk exposure to align with the risk appetite.

## 3.3 Good practice principles

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

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

- 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. Identify extent of systems and the identity of all interfaces, hard and soft.

- 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, viruses, malicious code installed on machines, worms or Trojan horse infections.

- 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 elsewhere

- 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.

## 3.4 Good practice guidance

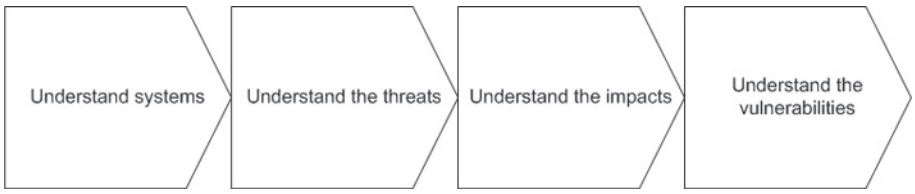


**Figure 4 – Key steps in assessing the business risk**

### 3.4.1 Understand systems

In order to understand the process control security risk facing a business, a thorough understanding is needed of the systems that constitute that business. The first step in this process is to agree the scope that this risk analysis will cover. The scope boundaries need to be clearly drawn and any systems that are identified as out of scope should have clear agreements about whose scope they are within. Also appropriate assurance of the level of security protection for these systems should be sought.

In many cases process control systems may have been installed many years ago and detailed knowledge of their operation and configuration may not be readily available. In order to understand the business risk this information needs to be determined (where it is not immediately available) and collated into a full system inventory.

There are a number of questions that need to be considered when gathering an inventory:

- How many locations, sites, systems and assets exist?
- What systems reside at the site?
- Where does the site and system fit in the overall 'value' or 'supply' chain?
- What is the business and operational criticality of each site and system?
- What contributions do the systems make to process or personnel safety?
- What production and other operations are carried out by the site?
- Are there any Safety, Health and Environmental or other regulatory implications?
- Do the assets form part of the Critical National Infrastructure (CNI)? For further information on what might constitute the CNI please consult www.cpni.gov.uk.
- Who is the single point of accountability (SPA) for each site, system and asset?
- Who are the key vendors and third parties relating to the systems?
- Who are the key support organisations at the site (IT, process control, off-site third party, on-site third party or in-house)?
- What are the site's critical system assets?
- What connections and data feeds are there to and from the control systems (include manual data feeds as well as electronic connections)?
- Are there any known issues with systems?
- What projects are underway or scheduled?
- What are the contact details for the local personnel and vendors?
- What are the dependencies relating to the site?
- Are there summary and detailed system and network diagrams?
- Is all documentation secure and under a management of change procedures?

The answers to these questions enable the organisation to create a process control inventory. The inventory is a fundamental building block with respect to this process control security framework and is the input to many other themes and sections. This inventory should be sufficiently detailed to provide the appropriate determination of risk.

Inventories are notoriously difficult to generate and keep up to date. An ideal situation might be to maintain a single inventory that can provide summary level of information together with the detail. If this is being done for a large organisation then it may not be practical to construct a single detailed inventory. A hierarchical inventory might be more appropriate where a central high level inventory is maintained together with a links to local site inventories, which contain the detail.

It should be noted that these inventories are a source of sensitive information, which would be very useful for an attacker. Consequently these inventories should be appropriately secured. Access to these inventories should be restricted to the minimum number of people that need access to this information.

Dependencies: it is important to understand any dependencies between systems (both for systems in scope and out of scope). Some parts of an industrial system might be dependent on the outputs of another system in the supply chain. For example an oil refinery might be dependent on a pipeline for its feedstock. Consequently, when determining the business risk for a refinery, the 'upstream' dependencies such as the supply pipeline should be adequately considered in the risk assessment. Similarly 'downstream' dependencies should also be considered. Extending the above example to include a chemicals plant that uses a by-product of the refinery then the chemicals plant is a 'downstream dependency and should also be subject to some level of scrutiny in the risk assessment.

### 3.4.2 Assessing the business risk

There are many ways in which business risk can be defined. One useful definition is to express the risk as a function of the likelihood of a risk occurring and the impact that would result if that risk were to occur. Risk is the summation of all the individual risks from identified threats

**Business risk = F (Likelihood x Impact)[2]. (1)**

The likelihood of a risk occurring can be expressed in terms of Threat, Target Attractiveness, and Vulnerability,

**Likelihood = F (Threat x Attractiveness x Vulnerability). (2)**

The attractiveness term relates to how attractive a target might be to a potential attacker. For example an attacker might find a nuclear power plant to be a more attractive target than a paper bag manufacturing plant! This attractiveness term may not apply to some risk, for example a worm infection. Most worms are indiscriminate in who they infect and therefore any vulnerable system is at risk. Consequently the attractiveness term is not relevant in this case.

The attractiveness term contributes to the likelihood of a risk occurring (i.e. a more attractive target is more likely to be attacked) and for simplicity can often be incorporated within the threat term.

Combining (1) and (2) gives an expression for business risk in terms of threat, attractiveness, impacts and vulnerabilities.

**Business risk = F (Threat x Impact x Attractiveness x Vulnerability). (3)**

The following sections describe the remaining elements required to understand the business risk.

[2] Guidelines for analysing and managing the security vulnerabilities of fixed chemical sites. AIChE - 2003.

### 3.4.3 Understand threats

Process Control Security threats are numerous and can originate from a variety of sources. It is important to consider the common threats but consideration should also be given to a particularly company or type of organisation. For example an oil company that is active in particularly sensitive regions of the world may have a different threat profile from a transport company operating solely in the UK.

Threat sources that should be considered include (but should not be limited to):

- Hackers
- Internal attackers
- Criminals
- Illegal information brokers
- Disgruntled staff
- Staff undertaking unauthorised actions ( e.g. accessing the Internet)
- Corporate intelligence
- Contractors
- Foreign intelligence services
- Organised crime
- Terrorists
- Protesters and activists (e.g. environmental, political, animal rights).

Types of threat that should be considered include (but should not be limited to):

- Worms (generic, targeted)
- Hackers (internal, external, external with insider knowledge)
- Viruses
- Trojans or backdoors
- Bots and spyware
- Loss of integrity
- Loss of availability (denial of service)
- Loss of confidentiality
- Unauthorised control.

These threats are somewhat generic so it is useful to consider these into example scenarios so that the impacts and any related vulnerabilities can be considered more specifically, care needs to be taken to ensure that the scenarios chosen are wider enough to consider all threats. Example consequences scenarios include, but are not be limited to:

- Systemic loss of all machines based on a particular operating system (e.g. Windows, Unix, VMS etc.)
- Systemic loss of Ethernet/IP networking technologies
- Loss (or reduction) of functionality of process control systems
- Loss of connectivity between the process control systems and
    - Corporate networks
    - Other systems (e.g. supply chain, laboratory systems or other companies)
    - Remote field devices
- Unauthorised change of setpoints or configuration by malicious or inadvertent actions
- Accidental change of system configuration by an authorised user

- Attack by disgruntled employee
- Loss of integrity or availability of historical data
- Loss of confidentiality of process and related information.

### 3.4.4 Understand Impacts

Once threats have been converted into threat scenarios then it is much easier to consider the impact that these might cause. Consider each scenario for each site, system or sub system and consider what the real life impacts might be, not only on that system, but also for any system that it is dependent upon. For example if considering a DCS controlling a power station for a chemicals plant then do consider what impact the loss of that system would have on the operation of the chemicals plant, including the effects on safety. When determining these impacts, do refer back to the inventory and dependencies already identified.

**Classification of impact:** in risk assessment it is usual to quantify the possible impacts or consequences of a threat in terms of monetary value. This is particularly the case when considering financial risk. However when considering process control security risk it can be difficult to determine accurate financial impacts for security incidents. Such quantification of the financial consequences is a whole specialist field in itself and can be more than is needed to assess process control security risk in order to identify appropriate security measures.

In order to avoid excessive effort in determining the impacts of a risk it is often possible to express impacts in terms of business specific language rather than as a monetary figure. For instance, being able to communicate the impact of a possible threat facing a process control system in terms of the effect on that system makes the risk much more understandable. For example the impact of a worm infection on a control system might result in a decision to shut down the plant operations.

Examples of possible ‘real life’ impact descriptions are:

**Safety, Health and Environmental event or damage to plant:** an event that results in either harm to individuals, the environment or damage to the plant.

**Non-compliance with regulatory requirements or minor Safety, Health and Environmental event:** an event that results in the site being non-compliant with regulatory requirements. For example, a consistent breach (e.g. excessive flaring in a chemicals plant or refinery on start up or shut down) or loss of regulatory historical data.

**Forced controlled shutdown of operations:** an event that results in the emergency shutdown system being automatically invoked with no human intervention. For example, when view is lost of all or some of the production processes.

**Elected controlled shutdown of operations:** an event that results in the site electing to shutdown its operations. For example, when view is lost of all or some of the production processes.

**Reduction in operating efficiency:** an event that would result in the plant continuing its operations in a less efficient or profitable manner or result in reduced production. For example, the raw material mix is changed resulting in the product being produced in a less efficient manner.

**No Impact:** no impact on operations.

Other impacts that should be considered are:

- loss of confidential information
- damage to Critical National Infrastructure
- loss of business continuity
- reputation
- value or supply chain.

**Time variance of impact:** when considering the impact of a particular threat then it is important to consider how that threat might vary with time. For example an incident may initially have only a minor impact but if that were to be allowed to continue over a long time period then it's severity of impact might be increased. An example of this is the loss of environmental monitoring information which may not be serious in the short term but is likely to be much more critical in the long term owing to legal and regulatory requirements around availability and integrity of this information.

**Successive impacts:** the effect of coincident or successive impacts should be considered, this is especially important where a common cause failure could be responsible.

### 3.4.5 Understand vulnerabilities

Understanding vulnerabilities involves a detailed review of all the system elements, (e.g. servers, workstations, network infrastructure etc.) to determine any vulnerabilities that exist. Examples of common vulnerability areas include but are not limited to:

- Connections to other systems
- Remote access
- Physical security
- Anti-virus protection
- Access control
- Passwords and accounts
- Security patching
- System monitoring
- System resilience and continuity
- Third parties who produce code for plant systems.

When considering the security of the overall system it is important to remember that a system is only protected as well as the weakest link. For example there is little benefit from having a well managed, tightly configured firewall if there is a poorly protected modem connection to the outside world thus bypassing the firewall.

### 3.4.6 Outputs of understanding the business risk

The key outputs from this are:

- inventory
- prioritised sites and systems
- list of key threats based on impact assessment
- prioritised vulnerabilities.

## 3.5 Applying this risk assessment approach

Most of this guidance is directed at the site or system level. In a large organisation with many sites and geographies to consider it may not be practical to work at this level. Consequently it is necessary to break the problem down into more manageable tasks. This can be done by performing a high level, lightweight risk assessment across the whole organisation or enterprise and then performing a more detailed assessment for each of the systems or sites shown in (Figure 5).

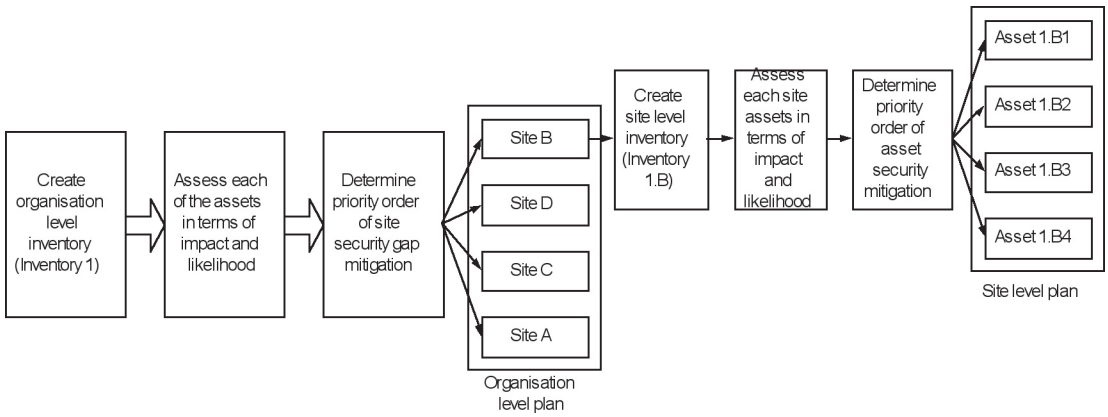


**Figure 5 High level enterprise risk assessment**

### 3.5.1 Step 1 – High level risk assessment of the enterprise

The first iteration of the risk assessment provides an enterprise level view of the process control security risk. It will provide an indication of the security gaps with the greatest impact to the enterprise by considering the 'value chain', interdependencies and impacts that have enterprise level significance. The analysis will provide the enterprise with both the priority security issues and the sites that should be addressed first.

An easy way of determining the priority order is to plot the asset scores on a Boston Grid (risk matrix). The risk parameters highlighted above can be plotted in a Site Risk Table, Table 1. In some cases each of the factors (Threat, Attractiveness and Vulnerability) will be given an equal weighting, at other times they may be weighted to reflect the situation. Care should be taken when aggregating different sites to ensure that they are using the same risk assessment otherwise the risk profile may become distorted.

| Site | Threat (T) | Attractiveness (A) | Vulnerability (V) | Likelihood (T x A x V) | Impact (I) |
|---|---|---|---|---|---|
| Site A | M | L | L | L | L |
| Site B | H | H | H | H | H |
| Site C | L | L | L | L | M |
| Site D | M | M | L | M | H |

**Table 1 – Site Risk Table**

From this risk table sites can be plotted on a Boston Grid (Figure 6) using the likelihood and impact values to indicate the high risk sites and allows determination of an appropriate priority for the site.

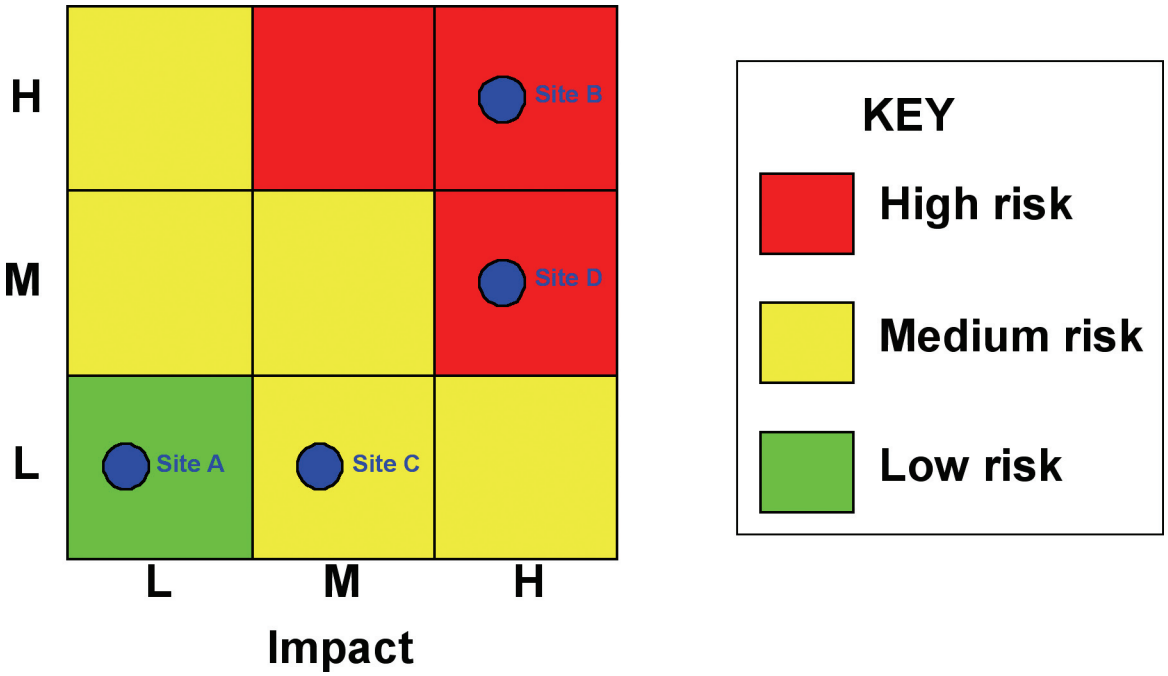


**Figure 6 – High level enterprise risk matrix**

### 3.5.2 Step 2 – Individual sites/systems risk assessment

The site risk assessment is based on the high level enterprise risk assessment and builds on the key risk areas identified. The site risk assessment analyses risk at the next level of detail down and considers the critical assets at a detailed level.

After selecting the initial site priority for the organisation, the same process can be used at a site level to help each site determine their priorities. Each site creates a more detailed inventory and then assesses the individual assets in terms of threats, impacts and vulnerabilities. This way a site can prioritise which assets or services should be tackled first.

Once an enterprise risk assessment has been carried out a similar process of understanding the systems, threats, impacts and vulnerabilities, should be followed at a site, system and asset level to understand the business risk relating to that level.

# 4. UNDERTAKE ONGOING ASSESSMENT OF BUSINESS RISK

## 4.1 Context of this section within the overall framework

This section is concerned with building the business risk assessment into 'business as usual' or ongoing BAU assurance. The process is linked to governance to ensure that systems are compliant with current standards, and ensuring that unauthorised systems changes haven't been introduced.

## 4.2 Rationale

Ensure that appropriate systems security is commensurate with the agreed business risk appetite.

## 4.3 Good practice principles

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

- 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

## 4.4 Good practice guidance

Undertaking an assessment of the business risk can be quite a long process and requires input from a number of stakeholders and resources. By defining 'triggers' that initiate the assessment process it ensures that the process is only run when needed. Such triggers are likely to vary from one organisation to another depending on the type of process, current level of security, current architecture, resources, etc. Examples of typical triggers are:

- Changes to:
  - Threat level
  - Risk appetite
- Criticality and risk of system
- Compliance assurances required
- New projects
- System changes
- Mergers and acquisitions
- Political circumstances (e.g. the change of a government, particularly in a developing country, may change the stability of the country's infrastructure and should be factored in)
- Elapsed time
- Major incident(s).

Following a re-assessment of business risk it is essential that a number of items are also re-assessed to ensure that they are still in-line with the overall business risk. They include:

- Process control security programme – to ensure the overall direction is still aligned with the business risk.
- Governance – to ensure that the structure and composition suits the business risk needs.
- Inventory – any changes to the inventory need to go through a formal change request and change control, and is communicated to appropriate stakeholders.
- Response plans – these need to accurately reflect the current systems and processes.

The process of re-assessment is likely to be resource intensive and should be proportional to the risk to critical systems. There is a natural tendency to establish a standard routine of security assessment such as an annual review for each site, system and asset. However, this may not be the most efficient use of resources as some sites may be reviewed too frequently and others not frequently enough. The frequency of re-assessment should be matched to the criticality of the systems or their impact on the enterprise and supply chain. One of the key outputs from each assessment of the business risk is an indication of how frequently reassessments of the risk should take place.

## 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