Good Practice Guide

Process Control and SCADA Security

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 NISCC.
Disclaimers

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 NISCC or PA Consulting Group. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, NISCC and PA Consulting Group accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Institution of Engineering and Technology (IET) state that:

While the authors and the publishers believe that the information and guidance given in this work are correct, all parties must rely upon their own skill and judgement when making use of them. Neither the authors nor the publishers assume any liability to anyone for any loss or damage caused by any error or omission in the work, whether such error or omission is the result of negligence or any other cause. Any and all such liability is disclaimed.

Acknowledgements

PA and NISCC 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.

We are pleased to announce that the Institution of Engineering and Technology (www.theiet.org) have reviewed this Good Practice Guide and commend it to industries that use Process Control and SCADA technology.
## TABLE OF CONTENTS

1. **Introduction** 4  
   1.1 Aims and objectives 4  
   1.2 Terminology 4  

2. **Securing process control and SCADA systems** 5  
   2.1 Overview 5  
   2.2 Process control security framework 5  

3. **Understand the business risk** 8  
   3.1 Overview 8  
   3.2 Objective 8  
   3.3 Principles of good practice 8  

4. **Implement secure architecture** 10  
   4.1 Overview 10  
   4.2 Objective 10  
   4.3 Principles of good practice 10  

5. **Establish response capabilities** 15  
   5.1 Overview 15  
   5.2 Objective 15  
   5.3 Principles of good practice 15  

6. **Improve awareness and skills** 16  
   6.1 Overview 16  
   6.2 Objective 16  
   6.3 Principles of good practice 16  

7. **Manage third party risk** 17  
   7.1 Overview 17  
   7.2 Objective 17  
   7.3 Principles of good practice 17  

8. **Engage projects** 19  
   8.1 Overview 19  
   8.2 Objective 19  
   8.3 Principles of good practice 19  

9. **Establish ongoing governance** 20  
   9.1 Overview 20  
   9.2 Objective 20  
   9.3 Principles of good practice 20
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 document; and
- identifies seven stages 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 (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 supplier’s 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

2.2.1 Guiding principles

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

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.
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

4.3.1 Network architecture

- Identify all connections to the process control system.
- Reduce 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 with a firewall and demilitarised zone (DMZ) architecture.¹
- 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.

¹ Additional information on Firewall Deployment for SCADA and Process Control Networks can be found in the NISCC website.
• Firewalls should be managed by appropriately trained administrators.
• A 24x7 capability for the management and monitoring of firewalls should be established.

4.3.3 Remote access

• Maintain an inventory of all remote access connections and types (eg virtual private network or modems).
• Ensure that a valid business justification exists for all remote access connections.
• Implement appropriate authentication mechanisms (eg 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 (eg 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 e-mail 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.
• Ensure all inbuilt system security features are enabled.
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.

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 process 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 passcards is logged.

4.3.10 Wireless networking

- Avoid wireless networking in process control systems where possible. Where wireless networking cannot be avoided, carry out a thorough risk assessment and deploy appropriate protection measures.

4.3.11 Security patching

- Implement processes for deployment of security patches to process control systems.

  - These processes should be supported by audit and deployment 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.

4.3.12 Personnel background checks

- Ensure all staff with operational or administration access to process control systems are appropriately screened. See BS7858 for further information.

4.3.13 Passwords & 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 Security scanning

- Implement security scanning where possible. Security scanning is a widely used tool for vulnerability management in IT networks. However, 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.

4.3.16 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.

4.3.17 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).

4.3.18 Security testing

• Security testing should be carried out where possible, for example penetration testing. 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 assurance that they are not vulnerable to common denial service attacks.

4.3.19 Device connection procedures

• Establish a procedure to verify that devices are free from virus or worm infections before being connected to process control networks.
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 UNIRAS for advice and support.

- Ensure that appropriate electronic security response and business continuity 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.
6. IMPROVE AWARENESS AND SKILLS

6.1 OVERVIEW

An 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.

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.
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.
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 project development life cycle (e.g. tender, commissioning, factory acceptance testing and commissioning).
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**

- Obtain senior management support for process control system security.
- Identify impacts of legal and regulatory requirements on process control security.
- Ensure process control system security practices align with the business and operational needs.
- Define roles and responsibilities for all elements of process control security.
- Appoint a single point of accountability for process control security risks.

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.

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.
About the authors

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

**PA Consulting Group** is a leading management, systems and technology consulting firm, with a unique combination of these capabilities. Established over 60 years ago, and operating worldwide from over 40 offices in around 20 countries, PA draws on the knowledge and experience of more than 3,000 people, whose skills span the initial generation of ideas and insights all the way through to detailed implementation.

**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

**National Infrastructure Security Co-ordination Centre**
PO Box 832
London
SW1P 1BG
Tel: 0870 487 0748
Fax: 0870 487 0749
Email: enquiries@niscc.gov.uk
Web: www.niscc.gov.uk

For further information from NISCC on process control and SCADA security:
email: scada@niscc.gov.uk, Internet: www.niscc.gov.uk/niscc/scada-en.html