EMERGING GOOD PRACTICE FOR CYBER SECURITY OF INDUSTRIAL CONTROL SYSTEMS AND SCADA

R.S.H. Piggin*

**Atkins Ltd, United Kingdom.*
Richard.piggin@atkinsglobal.com

Keywords: SCADA, ICS, IACS, Security, Cyber Security.

Abstract

This paper examines the development of good practice for Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition) SCADA security. Good practice and standards are reviewed, along with indications on future developments.

1 Introduction

Currently, security of critical systems is a concern across industry and a focus for Governments. Specific best practice is still emerging, particularly in the nuclear sector. This has the potential to be a regulatory risk. This paper addresses the current best practice approach, given international and UK guidance and other well-established methods from across industry. Nuclear best practice and forward looking strategy for the industry are discussed. The paper has reviewed non-nuclear guidelines and standards, and provides an overview of these documents and the concepts they establish for process control systems.

2 Current situation

Recently there has been a dramatic rise in concern regarding Cyber Security, along with the opportunities and threats emanating from the use of cyberspace. In the 2010 National Security Strategy, the UK Government rated cyber attacks as a 'Tier 1' threat and allocated £650 million over a four-year period to develop a UK response to the increasing threats [6]. Recent high profile events, including the Stuxnet and Duqu malware incidents highlight the potential threat to industrial control systems and have focused the attention of Governments and the wider public alike [6, 2]. A report published for the UK Government Cabinet in 2011 estimated the cost to the UK economy of cyber crime at £27bn per annum. Whilst the impact upon citizens and government is significant, the cost to business was shown to be even larger at £21bn [5]. The report's authors believe the research shows the mostly likely outcomes in the absence of a comprehensive picture, due to underreporting through fear of reputational damage.

3 Organisational approaches to information assurance

Organisations generally manage information risk using Information Assurance (IA) processes based on the ISO/IEC 27001 and ISO/IEC 27002 standards, originally developed in the UK. The ISO/IEC 27001/27002 series standards provide a framework for Cyber Security under the explicit control of management. However, compliance is voluntary. These standards provide formal requirements to obtain certification – the emphasis encourages ownership and accountability of security. They provide for a risk-based management system that specifies the overarching structural requirements for information management frameworks. As such, they are flexible, depending on the requirements of the specific organisation in question and do not require specific security measures to be implemented.

4 ICS and SCADA security

For more specific technical guidance on Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) security in the UK, organisations are directed to the Centre for the Protection of National Infrastructure (CPNI) series of Good Practice Guides in the first instance and in particular, the CPNI 'Process Control and SCADA Security' Good Practice Guides [6]. These provide a high-level approach to securing control systems, using the best of industry practices such as strategies, activities or approaches, which have been shown to be effective through research and evaluation.

The Office for Nuclear Regulation's approach to securing control systems is to utilise the best practice of both the CPNI and CESG – the UK Government's National Technical Authority for Information Assurance (IA) and responsible for IA policy and guidance. A caveat to this approach is that, the Information Assurance guidance from CESG is focused upon data assurance and does not map directly to the requirements of control systems.

A notable combined approach to security and safety is to use the Functional Safety standard IEC 61508 Safety Integrity Level (SIL), as a measure of reliability and/or risk reduction and align this to Business Impact Levels (BIL). Business Impact Levels are used by the UK Government in the Security Policy Framework and the CESG HMG IA Standard No. 1 for protecting the Confidentiality, Integrity or Availability of assets [4]. They are used by the UK Government, government suppliers and in Critical National Infrastructure [1]. The Impact Levels relate directly to Confidentiality protective markings: Impact Levels 1 and 2 – PROTECT, Impact Level 3 – RESTRICTED, Impact Level 4 – CONFIDENTIAL, Impact Level 5 – SECRET and Impact Level 6 – TOP SECRET. However, there is no equivalent set of markings for Integrity or Availability, hence the method to

use a dependability approach to combine Availability and Integrity for control systems.

5 Centre for the Protection of National Infrastructure

The CPNI is the UK Government authority that provides protective security advice to the national infrastructure. Specific SCADA advice is offered by the CPNI in a series of Process Control and SCADA Security Good Practice Guides. CPNI activities include:

- funding vulnerability and protection research
- an information exchange forum that meets regularly to share information on SCADA threats, incidents and mitigation (SCSIE)
- E-SCSIE – similar to the SCSIE, but with a focus on European government and industry efforts to protect process control and SCADA systems
- a close working relationship to the security programs being developed in the USA, Canada, Australia, New Zealand and Europe. This has led to best practice sharing, in particular the bilateral publishing/adoption of guidelines with the US Department of Homeland Security and the National Institute of Standards and Technology.

The CESG's role is to protect UK interests by setting policy and assistance on the security of communications and electronic data, working in partnership with industry and academia. Its principal customers are central government departments and agencies and the Armed Forces.

The good practices summarised in the CPNI documents are intended only as guidelines. For some environments and control systems, it may not be possible or appropriate to implement all of these principles, such as anti-malware (on embedded devices for instance), in which case alternative measures would need to be employed.

The foundation of the CPNI good practice is three guiding principles:

1. Protect, detect and respond. It is important to be able to detect possible attacks and respond in an appropriate manner, in order to minimise the impacts.
2. Defence in depth. No single security measure itself is totally secure, 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.
3. Technical, procedural and managerial protection measures. Technology is insufficient on its own to provide robust protection. Appropriate procedural measures and managerial controls, such as change control, monitoring, review and compliance, enhance protection[6].

The CPNI Process Control security framework covers industrial control, process control, Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA, industrial automation and related safety systems. The framework recognises that despite systems or some components being based upon common IT technologies, the operational environments differ from that of the corporate IT environment.

CPNI cites two principal areas of concern with the increased use of standard IT technologies;

- Firstly, increased connectivity via standard IT technologies, exposing control systems to vulnerabilities that they are not capable of defending against. Traditionally, control systems had been designed for safety and reliability, and to be isolated in closed systems, with physical security being the major concern. This illustrates the significant potential vulnerabilities of industrial control systems, often with minimal built-in security measures.
- Secondly, commercial [SCADA] software and general purpose software have been used to replace proprietary control systems. Often, such systems do not cater for complexities or particular requirements of real-time systems, including safety. Many of the standard IT approaches to securing these technologies have not been adapted for use in control systems environments. This leads to insufficient security measures being employed. For instance, it does raise the issue of IP-based technology in proprietary control platforms and Windows OS used in SCADA.

CPNI guidance highlights the potential for serious consequences, should these vulnerabilities be exploited. The consequences of electronic attack can include denial of service, unauthorised control of a process, loss of integrity, loss of confidentiality, loss of reputation and health, safety and environmental impacts.

The guidelines offered by the CPNI form a framework comprising seven principal themes, along with an overarching document that addresses the following:

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

The security framework emphasises the need to be able to detect potential attacks and respond appropriately to minimise impact, and not merely implement protection measures. This approach embodies the concept of defence in depth, taking into account factors such as physical security (i.e. the site's Inner Security Barrier), fastidious management of user accounts and role-based access control, lockdown and hardening of operating systems and control of data. The

approach applies a holistic methodology that considers the following factors:

- Physical Security
- People
- Process, procedures and managerial aspects
- Technology

Further technical guidance and management standards form an evolving framework for UK implementation of industrial Cyber Security. Much of this guidance includes work done in the US, particularly the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS), both of which collaborate with CPNI. Work to date by both US organisations incorporates good practice developed by CPNI. CPNI guidance also refers to documentation from both of these sources.

The CPNI guidelines offer a generic approach to plant control and process information system security. The methodology provides a holistic framework, which incorporates all elements that should be considered when implementing a security programme. It is high level in nature and leaves the implementation decisions and detail to the organisation concerned. This is an important distinction, as some guidance will not be appropriate to the nuclear environment.

6 ISA-99 Industrial Automation and Control System Security

Other work that influences practice in the UK is that of the US International Society of Automation (ISA). The ISA has published the ISA-99 series of standards that deal with Industrial Automation and Control Systems (IACS) Security. This series is also referenced by CPNI. These provide high-level generic guidance, and the first comprehensive set of standards to cover IACS.

Collaboration between ISA and IEC is developing a similar series of technical standards for IACS Security under IEC 62443 Industrial Communication Networks - Network and System Security, which will incorporate a management framework that embodies the approach of the ISO/IEC 27000 series.

The intended audience for the ISA-99 standards are those designing, implementing, or managing industrial automation and control systems and applies to users, system integrators, security practitioners, and control systems manufacturers and vendors.

The focus of the ISA-99 Committee is addressing IASC, where compromise could result in:

- endangerment of public or employee safety
- loss of public confidence
- violation of regulatory requirements
- loss of proprietary or confidential information
- economic loss
- impact on national security

The control system scope includes:

- hardware and software (including Operating System, system and application software and data) in DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems
- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations

ISA-99 standards have been used in the SCADA security aspects for the US Smart Gird standard NISTIR 7628 [8]. Future developments of ISA-99 will be incorporated into the IEC 62443 series of standards.

7 IEC 62443 - Industrial Communication Networks and System Security

IEC 62443 standards are based on the published ISA-99 series of technical reports and standards. The IEC 62443 documents have been revised to comply with ISO/IEC editorial requirements. The intention of the ISA-99 committee has been to have the broadest reach of the standards (ISA standards are US-centric). The IEC 62443 Working Group recognised the benefit of collaboration, as opposed to producing separate standards [7]. The product of this collaboration is the same standards, now with an international impact, but with different timescales due to the different work plan, editing and voting requirements. The structure of the IEC 62443 series is shown in Figure 1.

The IEC 62443 series focuses upon on industrial automation and control systems. Business planning and logistics systems, generally referred to as enterprise systems are not within the scope, however the integrity of data exchanged between enterprise and industrial control systems is considered.

IEC 62443-1 Part 1 introduces the following concepts to address Industrial Automation and Control Systems security in a holistic framework:

- Security objectives
- Foundational requirements
- Defence in depth
- Security context
- Threat-risk assessment
- Security program maturity
- Policies
- Security zones
- Conduits
- Security levels
- Security level lifecycle

The security objectives for industrial control systems contrast the traditional information assurance approach, which focuses upon three objectives – Confidentiality, Integrity, and Availability (CIA). Information security (typically back office) primary concern is confidentiality and the implementation of necessary access controls needed to assure

it, integrity may be the second priority, with availability as the lowest. This contrasts with IACS, where the priority is different. IACS system security is primarily concerned with maintaining the availability of the system. Since there are inherent risks associated with industrial processes, they are controlled, monitored, or affected by industrial automation and control systems. For this reason integrity is normally of secondary importance. Confidentiality is usually the least important priority as data is often in raw form, lacking context and often changes rapidly due being status based. Industrial control systems embody a different approach from CIA, which is often closer to the reverse, AIC, with the priorities of Safety, Reliability and Availability being paramount.

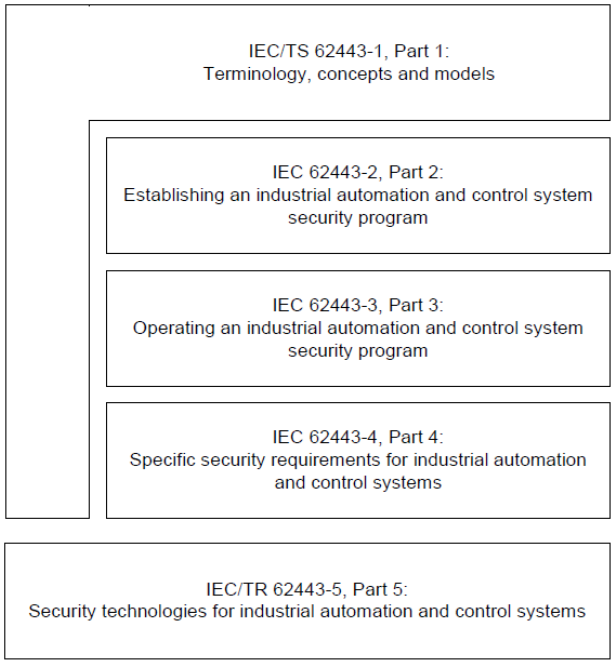

Figure 1: IEC 62443 Series - source IEC 62443 WG10.

Operational or component requirements may change the priority in a control system. Also, the timeliness of industrial control systems further differentiates them from business systems, system response times can be in single milliseconds as opposed to business systems running in second or several second time frame, that are tolerant to delay. Theses differing requirements will necessitate different counter measures to meet the security objectives.

The foundational requirements concept in IEC 62443 develops the security objectives that distinguish IACS security requirements from the simplistic CIA triad concept. The foundational concepts are:

- Access control (AC) – Control access to selected devices, information or both to protect against unauthorised interrogation of the device or information.
- Use control (UC) – Control use of selected devices, information or both to protect against unauthorised operation of the device or use of information.
- Data integrity (DI) – Ensure the integrity of data on selected communication channels to protect against unauthorised changes.
- Data confidentiality (DC) – Ensure the confidentiality of data on selected communication channels to protect against eavesdropping.
- Restrict data flow (RDF) – Restrict the flow of data on communication channels to protect against the publication of information to unauthorised sources.
- Timely response to event (TRE) – Respond to security violations by notifying the proper authority, providing the reporting needed for forensic evidence of the violation, and automatically taking timely corrective action in mission critical or safety critical situations.
- Resource availability (RA) – Ensure the availability of all network resources to protect against denial of service attacks.

The concepts of security zones and conduits are relevant to the approach taken in current good practice, particularly in the nuclear sector, where different safety classes are segregated. Security zones define boundaries for areas with the same level of security, given the premise that security levels are unlikely to be homogenous across an asset. Security zones as would be expected, can be either logical or physical.

The conduit concept deals with the flow of information in and out of security zones. To address electronic communication as opposed to other forms, the concept of a communications conduit is proposed.

The security level method provides the ability to categorise risk for a zone or conduit. This is presently a qualitative approach to addressing security for a zone. It can be applied to compare and manage the security of zones within an organisation and would need to be defined by an organisation. Presently, there are three recommended coarse levels: 3) high, 2) medium and 1) low impact. Three applications of Security Levels (SLs) are defined:

- SL(target) – Target Security Level for a zone or conduit
- SL(achieved) – Achieved Security Level of a zone or conduit
- SL(capability) – Security Level capability of countermeasures that can be used within a zone or conduit or inherent Security Level Capability of devices or systems that can be used within a zone or conduit

The intention is to develop mathematical representations of risk, threats and countermeasures. As knowledge and experience of security incidents, threats and countermeasures increases, this concept will move to a quantitative approach for design, selection and verification of SLs. It will have applicability to end user companies and vendors of IACS and security products. This is an immature concept that is likely to take a significant time to develop and be adopted (especially by vendors). The critics of this approach argue that there is a danger of indicating a capability (of a device) and assuming an appropriate level of protection to a system

i.e. defining a component SL does not guarantee that the same SL is met by the system as a whole. This corresponds to the concept of Safety Integrity Level (SIL) and the end to end scope of the Safety Function and its application across the complete system, not components or parts of a system in the Functional Safety standard IEC 61508.

8 NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security

The US National Institute of Standards and Technology (NIST) have produced the ICS guide similarly focused, as the other good practice already mentioned at SCADA, DCS and PLCs [9]. The motivation to undertake the work is a statutory obligation and under a US Homeland Security Presidential Directive. The authors acknowledge contributions from the ISA-99 committee, ISA and CPNI.

The purpose of the document is to provide guidance on securing control systems, and other systems that perform control functions; as such, this is the broadest of control system definitions. The guide provides an introduction to industrial control systems, utilising models of various typical configurations. These are then described with typical threats, vulnerabilities and appropriate counter measures. Due to the nature of control systems, their varied application and potential impacts, the guide covers a number of different approaches and techniques, but cautions against using the guide as checklist of requirements. In common with the other definitions of good practice, a risk-based approach is recommended to secure specific systems and balance operational, business and security requirements.

Both NIST and CPNI provide some guidance for specific services, however since practice is variable across industrial sectors, it is difficult to recommend specific rules, which should be determined by the organisation concerned. Further good practice is referenced from the now defunct Industrial Automation Open Networking Association (IAONA) and ISA-99/IEC 62443 documents. It is recommended that these are considered when developing specific rule sets.

The strategy to secure the control system with a combination of security policies and carefully configured security measures to form a defence in depth layered security is recommended. The set of security measures is extensive and provides specific guidance for control system applications. These cover the complete lifecycle of the control system and includes risk assessment, management control, personnel, operational control, physical and environmental protection, contingency planning, incident response intrusion detection, identification, authorisation, authentication, role-based access control, audit and accountability, encryption, remote access and training.

The NIST SP 800-82 document references another NIST publication – NIST SP 800-53 Recommended Security Controls [Measures] for Federal Information Systems and Organisations. The purpose of this publication is to provide guidelines for selecting and specifying security measures for information systems for federal agencies, and is applicable to US critical infrastructure. NIST SP 800-82 refers to Appendix I, which provides security measure enhancements for Industrial Control Systems. Where ICS systems cannot support or organisations deem that it is not appropriate to implement security measures or security enhancements (for example if performance, safety or reliability may be adversely impacted), then the organisation is required to provide a comprehensive rationale for selection of alternative compensating measures and explain why the baseline measures were not suitable.

Appendix E of SP 800-82 provides a table that maps NIST SP 800-53 to ISO/IEC 27001 security measures and vice versa, where the functionality is similar. NIST is in the early phases of integrating the ISO/IEC 27001 management approach into NIST standards and publications. This matches the good practice being developed in ISA-99/IEC 62443 and in Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities produced by the US Nuclear Regulatory Commission.

9 NERC CIP standards

The North American Electric Reliability Corporation (NERC) is tasked with ensuring the reliability of the North American (US and Canada) bulk power system, which excludes nuclear facilities. NERC is certified by the US Federal Energy Regulatory Commission to establish and enforce reliability standards.

NERC (Critical Infrastructure Protection) Standards CIP-002-3 to CIP-009-3 form a Cyber Security framework for the identification and protection of critical cyber assets to support reliable operations. Critical assets are identified through trisk-based assessments [10].

The NERC standards framework is holistic, covering:

- Cyber Security – Critical Cyber Asset Identification
- Cyber Security – Security Management Controls
- Cyber Security – Personnel & Training
- Cyber Security – Electronic Security Perimeter
- Cyber Security – Physical Security of Critical Cyber Assets
- Cyber Security – Systems Security Management
- Cyber Security – Incident Reporting and Response Planning
- Cyber Security – Recovery Plans for Critical Cyber Assets

Each NERC CIP standard defines:

- asset owner applicability
- requirements to be met
- measures: to illustrate requirements met
- compliance monitoring process and Compliance Enforcement Authority
- violations and their severity.

The guidance is strategic and prescriptive, with very limited supporting documentation. For tactical and practical implementation, other sources of good practice are required, such as the NIST series of security documents.

10 Nuclear Cyber Security good practice

Presently, the UK Office for Nuclear Regulation (ONR) references CPNI guidance that includes NIST, US Department of Homeland Security (DHS) and other best practice. This is generic good practice, and not sector specific. Currently, this is not mandated for control systems in the UK nuclear industry, unlike CESG conformance for data networks. This is due in part to the design and age of incumbent systems that are used in nuclear facilities, inhibiting the implementation of state of the art security measures. This position is unlikely to change for existing nuclear, with the introduction of specific technical guidance to be issued by the ONR in 2012. However, the guidance will need to address the development of networked control systems and the use of COTS IT technology. The ONR technical guidance will be based upon CPNI Good Practice Guides and other relevant international standards. The US NRC RG 5.71 is expected to be influential, as it has adopted established practice from a number of recognised sources.

The US Nuclear Regulatory Commission published Regulatory Guide (RG) 5.71 Cyber Security Programs for Nuclear Facilities to provide guidance to applicants and licensees to comply with 10 CFR 73.54 Protection of digital computer and communication systems and networks [11]. RG 5.71 consolidates knowledge and experience from ISA, IEEE, NIST and DHS. Specifically, RG 5.71 promotes a strategy and architecture based upon NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security and NIST SP 800-53 Recommended Security Controls [Measures] for Federal Information Systems and Organisations. The NRC recognises that both are based upon well-understood cyber threats, vulnerabilities and risks and both provide similarly understood countermeasures and protective techniques.

RG 5.71 develops the NIST guidance by tailoring high impact baseline security measures for the nuclear environment and provides more specific security measures. The NRC process to develop the specific security measures was peer-reviewed and open to industry comment, providing an established standard for Cyber Security that also offers a pragmatic approach.

11 European initiatives

The European Network and Information Security Agency (ENISA) works with European institutions and member states to address cyber security issues of the European Union. ENISA recently published [12] a report recommending provision of pan European ICS security guidance for every European stakeholder, to apply cross critical infrastructure, and to be applicable to those industries not necessarily considered critical thus far.

12 Conclusion

In an arena of voluntary compliance across industry, those implementing ICS and SCADA security need to keep abreast of technical developments and employ recognised best practice. The absence of regulation in industrial Cyber Security in the UK is regarded as beneficial, not stifling developments in a fast moving area. It is this environment that will cause the security case to be continuously challenged. This is in contrast with the safety case, which is very rarely changed and is often considered in isolation.

Acknowledgements

The contribution of Horizon Nuclear Power towards the review of ICS security practice is appreciated.

References

[1] Cabinet Office, “Guidance on the use of the business impact level tables”, p 3, (2009).
[2] Cabinet Office, “The UK Cyber Security Strategy Protecting and promoting the UK in a digital world”, pp 17-19, (2012).
[3] Centre for the Protection of National Infrastructure, “Good Practice Guide Process Control and SCADA Security”, pp 2-18, (2008).
[4] CESG, HMG IA Standard No. 1 Technical Risk Assessment, pp 16-17, (2009).
[5] Detica “The cost of cyber crime”, pp 2-6 (2010).
[6] HM Government, “A Strong Britain in an Age of Uncertainty: The National Security Strategy”, pp 27-30, (2010).
[7] International Electrotechnical Commission TS 62443-1-1 ed1.0 “Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models”, 7-83, (2009).
[8] National Institute of Standards and Technology Interagency Report, “Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements”, p 6, (2010).
[9] National Institute for Standards and Technology Special Publication 80-82, “Guide to Industrial Control Systems (ICS) Security”, pp 1-1 – E-4, (2011).
[10] North American Electric Reliability Corporation Reliability Standards. (2012) [online]. [Accessed 20th July 2012]. Available from World Wide Web: <http://www.nerc.com/page.php?cid=2%7C20>
[11] Nuclear Regulatory Commission, “Nuclear Regulatory Commission Regulatory Guide 5.71”, Cyber Security Programs for Nuclear Facilities, pp 4-7, (2010).
[12] ENISA, Protecting Industrial Control Systems Recommendations for Europe and Member States, pp 37-38 (2011).