Cyber Security Working Group

1 Contents

2 Revision History

Version	Date	Author	Comments
0.1	09/02/11	Alan Blight	Work in progress for comment only
0.2	20/02/11	Alan Blight	Minor additions and corrections to 0.1
0.3	26/08/11	Alan Blight	Distributed to working group 26 August 2011 in two formats (with and without document tracking)
0.4	28/05/12	Alan Blight	Work in progress. Add types of attacks, rearrange order. V0.4c circulated internally for comment
0.5	11/06/12	Alan Blight	Working group feedback incorporated. Final Draft released to all 61508 Association members for comment before publication.

3 Introduction

Recent events have illustrated that process systems may be the target of a cyber-attack. In terms of functional safety, unauthorised access can be considered as an additional risk, and assessed in terms of probability, consequence, and cost of mitigation. Treating information security as a part of a risk management strategy naturally follows the lifecycle approach of IEC61508 and leads to an assessment of the threat during the design phase of a project.

The threat from unauthorised access to industrial process and infrastructure systems has been amply demonstrated and some countries (notably the US) have already taken steps to mandate a degree of cyber security.

Because each installation has unique arrangements, and security technology evolves very rapidly in response to new threats, this document uses generic cases and does not prescribe specific measures or settings. However, although the detail may differ, the principles remain valid. Similarly although there are a number of commercial products available to assist with the implementation of a security policy, this document does not seek to promote any specific commercial solution.

The aim is to provide those concerned with the design and operation of SIS with sufficient information to make an assessment of the risk, and evaluate between the possible mitigation strategies available.

4 Working Group Deliverables

1. To describe an approach to the assessment of the risk of unauthorised cyber access
2. To examine the applicability of existing and emerging standards to functional safety applications
3. To propose security practices that should be applied to a functional safety system
4. To align this proposal with the IEC61508 lifecycle
5. To examine the feasibility of compliance certification
6. To submit our findings for expert critical analysis

5 Scope

The proposals shall be applicable to UK legislation and practice. Where possible compliance with other national standards shall be considered. This is a generic document and is applicable to multiple safety-related applications.
This document is issued in June 2012 and should be reviewed annually.

6 Managing the Cyber Risk

It is proposed that the cyber risk be managed in a similar manner to physical risks - identifying the hazard and assessing the probability and consequence. In the case of cyber security the risk may be regarded as a function of threat, vulnerability, consequence and probability. However quantifying the risk may be much more difficult. Identify the threats

6.1 Assessing the Threats

The system may be at risk from those who could exploit the vulnerabilities. Examples of possible threats are:

Internal - Inadvertent contamination (eg through contaminated portable storage devices)
Accidental disruption due to testing or equipment malfunction
Disgruntled or recruited employees / ex-employees

External - Social activists (" hacktivists" - who perceive that a company does not operate in accordance with their views)
Political opponents (terrorist or state-sponsored)
Competitors (interested in stealing IP or commercial intelligence rather than disruption)
Criminals seeking to achieve financial gain (eg theft of product or installation of "scareware" which infects a system then demands a ransom for removal)
Opportunists seeking to exploit or demonstrate system vulnerability (technical challenge or commercial opportunity to sell cyber security products)

6.2 Assessing the vulnerabilities of the system

This requires an assessment of the entry points, architecture, and the protective measures currently employed. In particular, trends towards wireless technology, remote access from embedded devices, and integration of the process system into the business networks, widen the opportunity for attack. As always there has to be a balance between security and operational functionality. Early detection may enable an attack to be isolated before significant damage occurs.
The internet provides a wealth of material on types of attack but briefly the following categories should be included in the assessment:

- Denial of service - attackers flood the network with spurious data, denying access to legitimate users. In some cases multiple computers can target the system (often remotely controlled "zombies" forming a "botnet") creating a distributed denial of service attack.
- Penetration - attackers attempt to gain access to the target system. The aim may be to disrupt the system, or to install a backdoor to allow later access to the system, or to steal confidential information. There are a number of sophisticated tools available, and many exploits - such as viruses - may seek opportunistic targets rather than a specific target.
- Social engineering - the best configured system can be vulnerable if a member of staff unsuspectingly divulges sensitive information. By nature staff wish to be helpful and attackers frequently exploit this as a means of obtaining details of the system which can help them gain entry.

The US Department for Homeland Security has a freely downloadable Cyber Security Evaluation Tool (CSET) which guides users through a process to assess their network security practices. The output from CSET is a prioritised list of recommendations, derived from a number of published guidelines, for improving the security of the system. The tool is available here :
http://www.us-cert.gov/control_systems/satool.html

Finally remember that devices such as smart printers, PDAs, and embedded devices can also be vulnerable. Any device connected to your network should be assessed. Although at the time of writing there are no known cases of attacks directly against a PLC, this should not be discounted in the future.

6.3 Consider the consequences

The consequence of a cyber-attack depends upon the nature of the site and the aims of the attacker. This is outside the scope of this document, but it is no exaggeration to say that the output of some process sites can directly affect a national economy, and have huge potential for damage to the population and environment.

6.4 Consider the probability

The probability for internal attacks (whether inadvertent or deliberate) is higher because they can be initiated from within the security perimeter, and without robust security measures they can be launched very easily.
A dedicated external attack against a well-defended target requires significant time and resource and would probably only be justified if there was significant gain to be made in the eyes of the perpetrator. There have been instances of socially motivated "Hacktivist" groups recruiting voluntary assistance online to form botnets of enormous power, but so far these attacks tend to be targeted against commercial sites

7 Functional safety and IT systems

In many cases cyber security rests with IT professionals and they may not be familiar with the different needs of a functional safety system. Implementation of a cyber-security policy will require close co-operation between automation engineers, plant operators, and IT professionals.

	IT System	FS System
Component Lifecycle	Up to 5 years	Up to 20 years
Performance	Typically high throughput, can tolerate delays and retries	Availability and integrity more important than throughput
Response Time	Response time generally not critical. Components may be rebooted	Response time may be part of safety case
Authentication	Often centrally managed user accounts	Often local to each device. May be very basic
Upgrades	May be centrally managed and quickly implemented	Must be carefully managed and tested to avoid compromising system and safety certification. Usually implemented one device at a time. May require local access which may be difficult for some components
Add-ins	Numerous third party products such as anti-virus	Proprietary operating system means no third party add-ins.
Support	Widely available	Available from vendor only

8 61508 Association Recommended Practices

This document sets out to describe current best practices in maximising security for functional safety systems, but does not seek to prescribe specific measures, since these will depend on the application, and any existing constraints of the installation.

8.1 References

The following documents are recommended as a baseline for best practices (this is a rapidly evolving landscape and readers should check for latest versions):
1. National Institute of Standards and Technology (NIST) Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security (June 2011)
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
2. Control Systems Security Program (CSSP) Standards & References
http://www.us-cert.gov/control_systems/csstandards.html
3. U.S. Department of Homeland Security Recommendations for Standards Developers (April 2011)
http://www.us-cert.gov/control_systems/pdf/CatalogofRecommendationsVer7.pdf
4. United States Computer Emergency Readiness Team (US_CERT) Advisory-11-199-01: Security Recommendations to Prevent Cyber Intrusions
http://www.us-cert.gov/cas/techalerts/TA11-200A.html

8.2 Overview

Securing the functional safety system is not just an engineering issue - it includes procurement, training, physical security, and operational procedures. Owners and operators will need to engage with other stakeholders early in the process and set up cross-functional measures to design, implement and operate a security system which is effective but does not prevent efficient operation of the plant. Early management approval will help secure funding and establish a security culture in the business.

8.3 Quick Check List

This is intended as a bullet point list of security considerations. It should not be regarded as an exhaustive check list; site considerations and limitations of the hardware and software used will affect the options available:

- Ensure components are physically secure (eg in locked cabinets, in secure areas)
- Implement robust passwords wherever possible (including at the controller). Change default passwords on software packages and hardware devices
- Consider carefully the security vulnerabilities of embedded "smart" devices such as phones or printers before connecting them to the system
- Consider carefully the security implications of wireless transmission and use robust encryption for any wireless traffic
- Disable un-used ports where possible, including web server and ftp connections. Minimise keep-alive settings and other settings which hold a disconnected port open
- In particular all USB ports should be disabled. Peripheral devices should use alternative connections.
- Use robust firewalls and anti-malware protection on your programming and SCADA PCs
- Create a site strategy to implement updates to Windows, software packages, and PLC firmware
- Create a site strategy to periodically reassess the security situation and measures taken
- Create Windows accounts on the programming and SCADA PCs with appropriate privileges and enforce login / logout. Users should have the lowest privilege appropriate for their function.
- Enforce roles and users on your SCADA package with appropriate privileges. If possible password protect programming and configuration projects from unauthorised access
- Implement a Change Management policy to control access and track changes to SCADA, configuration and programme
- Implement a disaster recovery strategy with safe backup files.
- Implement an education policy to train staff about the dangers of connecting unauthorised devices (such as memory sticks) to the system, and alert them to the possibility of social engineering to gain information about the system.

8.4 Procurement and Specification

New projects and upgrades to existing installations should have a mandatory obligation to include security considerations as part of the specification and procurement process. This will require an evaluation of the trade-off between information security and operational effectiveness. There should be a clear statement of the security requirements of the system or project.
Requests for Quotation should include the following:

- Any architecture constraints or requirements
- Any operational constraints or requirements
- Any compliance standards or recommendations to be met
- Any interfaces to existing systems or devices, and security requirements for such interfaces
- Any performance requirements or certification requirements for new products
- Any security features required in new hardware or software (eg authentication, encryption)
- Consider making security part of the Site Acceptance Test

8.5 Architecture

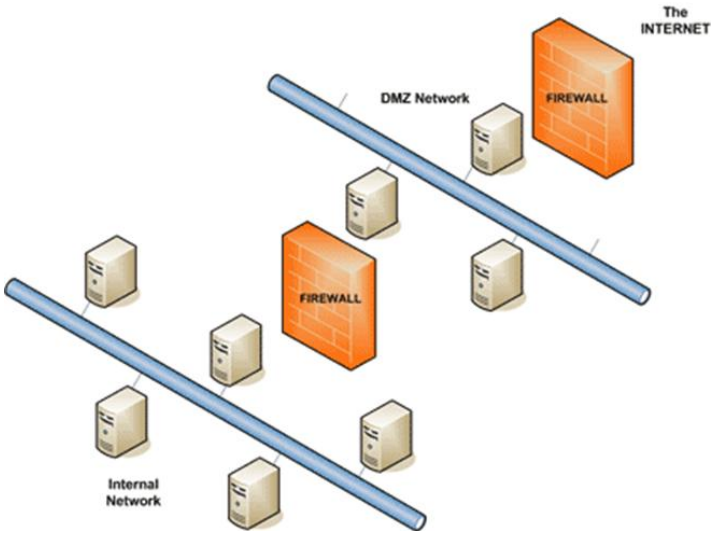
For most installations the US Department of Homeland Security "Defence in Depth" strategy provides sound guidelines on creating a robust architecture. The architecture is discussed in detail here http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf
The salient points are:

- Implement multiple layers of defence to counter multiple threats
- Divide networks into functional zones and identify interconnections between zones
- Determine rules for data exchange through these conduits between zones
- Deploy firewalls (preferably from 2 different vendors) to enforce these rules in both directions
- Route external access through demilitarised zones (DMZ) to act as buffers

One way of implementing a defence in depth architecture is to use the ISA99 strategy of zoning. A zone is a grouping of logical or physical assets that share common security requirements, so there is a relationship with the functional models of ISA88 and ISA95. This strategy allows more stringent security measures to be applied to the highest risk zones (such as the safety zone) whilst reducing the cost of implementing those measures across all zones. Each zone has a defined boundary and conduits tunnel communication between zones. Channels are used to communicate between devices within the zone.

Firewalls are used to protect the conduits. The aim should be to minimise the number of conduits that need to be defended. Consideration will need to be given about which protocols can provide widest coverage. Particular attention should be paid to devices that can bridge zones, such as wireless enabled field devices

Demilitarised Zones (DMZ) are used to isolate external connections. A DMZ is an intermediate network which acts as a buffer between external access and the trusted internal network. Devices in the DMZ have access to external sites but there is no direct conduit to the trusted network. The DMZ network has different addresses and is protected at both ends by a firewall

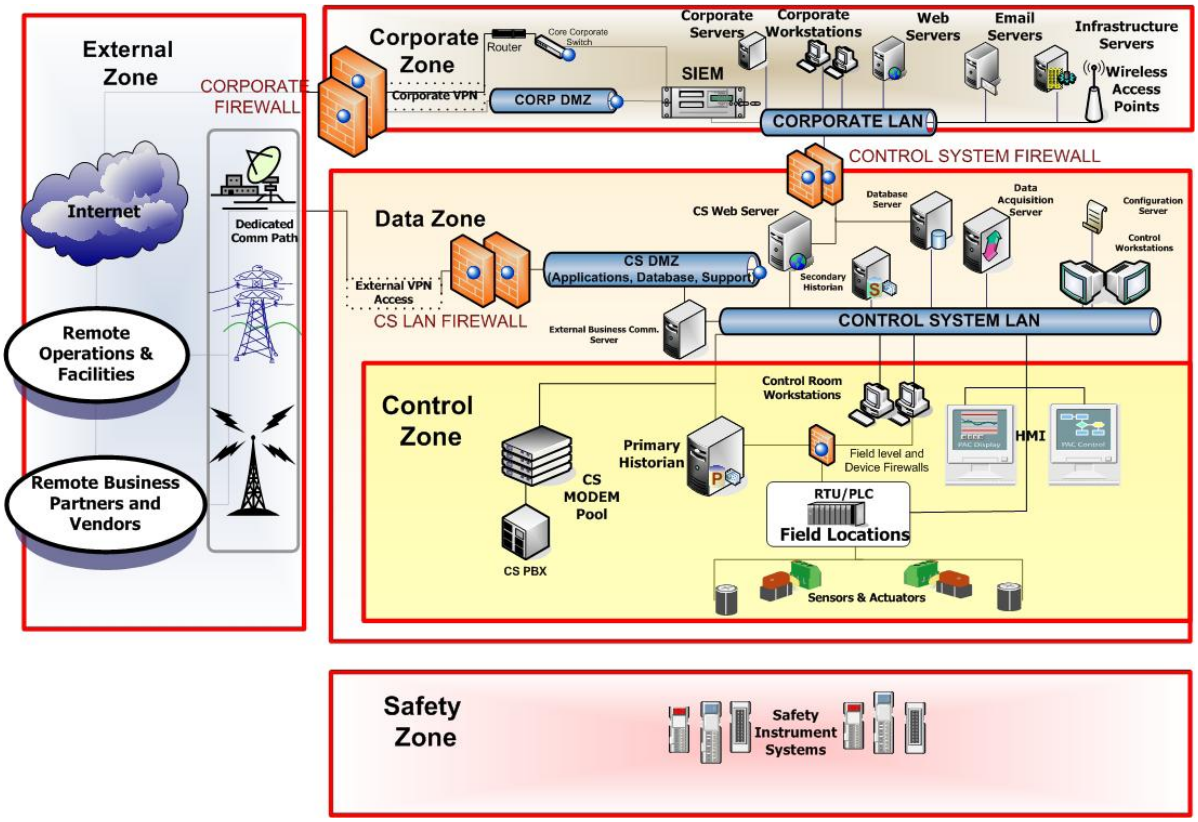


A fully protected system will also incorporate defence measures to detect and mitigate firewall breaches, such as

- IDS – Intrusion Detection Systems
- IPS - Intrusion-prevention systems
- SIEM – Security Incident and Event Management systems

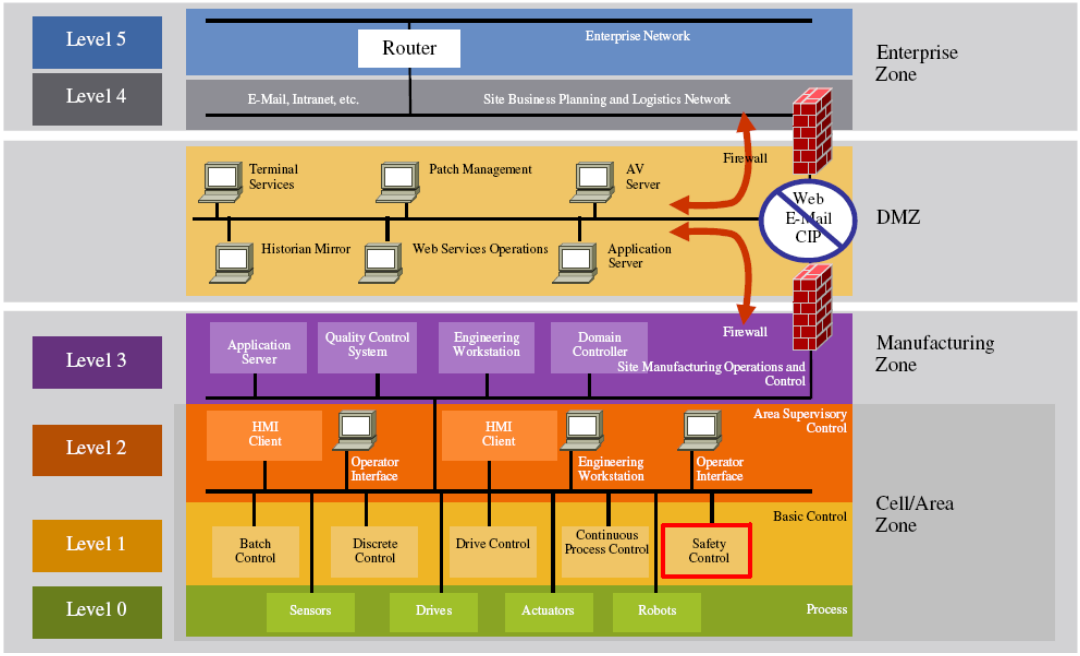
There are a number of commercially available products available, some of which have been specifically configured to work with particular manufacturer's products.

Two examples of a Defence in Depth architecture are given below. They are intended as illustrations only; many practical architectures will employ features from both models.



Source http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

One potential weakness of the defence in depth strategy as applied above is that is assumes the safety system exists behind an air gap. The air gap theory that a functional safety system can exist in an isolated communications bubble, immune from external threats, is rarely viable. The system will communicate with workstations, DCS, and HMIs, and be exposed to threats through these routes. Therefore it is recommended that the same, or higher, measures are applied to the safety zone as the Control zone, as illustrated below



Source http://www.isa.org/~tarhe/ISA%20Beyond%20Defense%20In%20Depth%202011.pdf

When considering the implementation of a defence-in depth strategy it should be noted that some experts maintain that there is a trade-off between the resources needed to purchase, configure and maintain an effective layered defence system, and the actual benefit gained. It is probably true to say that it is impossible to implement a fully secure operational system so a realistic appraisal of the deterrent effect of the security measures versus the likelihood of the attack should be made and the sophistication of the defences implemented accordingly.

8.6 Operational measures

Once a secure architecture has been created, measures are needed to maintain that level of security. Whilst physical security is outside the scope of this paper, it plays an important role in the security of functional safety systems particularly since much of the Equipment Under Control may be located in remote or inaccessible areas.

Authentication and Access control
The following measures are recommended where practical

- Use password protection - replace default passwords
- Use strong passwords where possible (many control layer products impose restrictions here)
- Restrict physical and electronic access based on user needs
- Use separate authentication mechanisms for users of the corporate and ICS networks

Policies, Procedures and Guidelines
The following policies are recommended where practical

- Create a cross functional security team with a regular review plan. Provide training if necessary
- Plan for disaster recovery - regular backups, quarantine procedures etc.
- Implement a patch management policy for operating systems and product software /firmware
- Implement and maintain security measures such as anti-virus software
- Check for known vulnerabilities (http://www.kb.cert.org/vuls/byid?searchview)
- Quickly Revoke access control for dismissed employees
- Educate employees to be cyber aware - implement policies for regular password changes, use of personal equipment such as laptops and memory sticks, use of social networking sites etc.
- Product training - ensure employees are aware of the security features of the equipment they maintain / operate, and how they should be configured
- Consider measures to control subcontractors and other irregular visitors who may require access

More background on applying operational security to a defence in depth strategy can be found here http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

8.7 Alignment with IEC61508

Just as functional safety is about managing risk to tolerable levels rather than eliminating it completely, so information security accepts that total security is not viable. Rather the aim is to reduce the incidence of intrusion into the control and SCADA systems to an acceptable level. As always implementing a security policy will involve a trade-off between operational practicalities, financial constraints, legal and regulatory constraints

It is considered that cyber risk be considered as part of the HAZOP / risk assessment stage in terms of the probability an initiating event versus the consequence of a loss of control of all the vulnerable points in the system and the effect on risk reduction. In this case the cyber risk forms part of the process of defining the safety integrity level required.

8.8 Compliance certification

Several commercial organisations offer a product certification service. Whilst this may provide useful information, the security risk needs to be taken in a much broader context. The 61508 Association does not endorse any particular commercial certification service.

9 Annexe A - Existing and Emerging Standards

There are numerous guidelines and recommendations but few standards applicable to the specific needs of a functional safety. Many of the established and emerging standards are aimed at IT infrastructures which are more concerned with high data throughput than the availability and integrity requirements of a functional safety system. ISA-99 Security for industrial automation and control systems uses the concept of Security Assurance Levels (SALs) which can be broadly compared with SILs in that it bands the level of protection required depending on the function, but a major difference is that it uses qualitative descriptions rather than quantitative measures. The ISA99 standard consists of the following and is still evolving:
ANSI/ISA-99.01.01-2007, Security for industrial automation and control systems: Concepts, terminology and models
ANSI/ISA-99.02.01-2009, Security for industrial automation and control systems: Establishing an industrial automation and control system security program
ISA-99.02.02, Security for industrial automation and control systems: Operating an industrial automation and control system security program
ISA-99.03.02, Security for industrial automation and control systems: Security assurance levels for zones and conduits
ISA-99.03.03, Security for industrial automation and control systems: System security requirements and security assurance levels
http://www.isa.org/mstemplate.cfm?section=home&template=/TaggedPage/getStandards.cfm&MicrositeID=988&CommitteeID=6821

9.1 IS0 27000 Series

The ISO 27000 series of standards have been specifically reserved by ISO for information security matters. This of course, aligns with a number of other topics, including ISO 9000 (quality management) and ISO 14000 (environmental management). ISO/IEC 27001 describes a cyber-security management system for business / information technology systems but much of the content in these standards is applicable to Industrial systems as well.
ISO27000 series is a particularly comprehensive standard so a list of policy headings is included at Appendix A which may serve as an aide-memoire to those seeking to formulate their own policies.

ISO 27001:2005 - provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System. The broad headings (reproduced at Annexe B) give a valuable framework for formulating a security policy although many of them are not applicable to process applications.
ISO 27002:2005 - a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001. It replaces ISO 17799:2005, and has identical technical content. ISO 27002 incorporates both parts of the BS 7799 standard. Sometimes ISO/IEC 27002 is referred to as BS 7799 part 1 and sometimes it refers to part 1 and part 2. BS 7799 part 1 provides an outline for cyber security policy; whereas BS 7799 part 2 provides a certification. The certification once obtained lasts three years and is periodically checked by the BSI to ensure an organization continues to be compliant throughout that three year period. The ISO/IEC 27002 standard is arranged into eleven control areas; security policy, organizing information security, asset management, human resources security, physical and environmental security, communication and operations, access controls, information systems acquisition/development/maintenance, incident handling, business continuity management, compliance
ISO 27003:2010 – focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005. It describes the process of ISMS specification and design from inception to the production of implementation plans
ISO 27004:2009 provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.
ISO 27005:2008 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

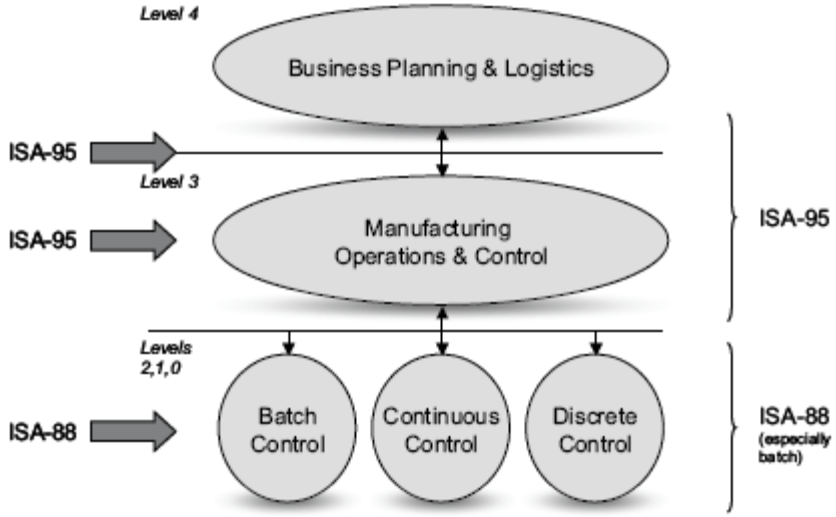
ISO 27006:2007 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.
ISO 27007 (Under development) Guidelines for information security management systems auditing
ISO 27008 (Under development) Guidance for auditors on ISMS controls

9.2 IEC62433 Industrial Communication Networks – Network & System Security

IEC 62443-1-1:2009defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security.
IEC 62443-2-1:2010 defines the elements necessary to establish a cyber-security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements
IEC 62443-3-1:2009 provides a current assessment of various cyber security tools, mitigation counter-measures, and technologies, including authentication methods, access control techniques, encryption, VPNs, protection and detection tools, and web technology

9.3 ISA88 and ISA95

These standards are used to represent template models of a plant although they differ in terms of their purpose, which means manufacturing companies will often make use of both standards. Typically, ISA-88 is used for automating the control of machines and devices, and ISA-95 for the exchange of information between ERP and MES systems.



From the point of cyber security these standards provide a useful reference for modelling the plant as a series of components with different capabilities and vulnerabilities, such as the one proposed in ISA standard 88.01 section 4.2.

- The lowest level of control is the Control Module Level. This level describes basic input and output (I/O) devices such as sensors (e.g. pressure, flow rate, temperature, turbidity, etc.) and control devices (e.g. valves, motors, solenoids, burner controls, etc.) fundamental to the power generation process in the field. The amount of intelligence is typically very limited at this level, though some new smart devices are changing this trend.
- Above the Control Module Level is the Equipment Module Level which performs basic monitoring and control functions with input from and feedback to the Control Module Level equipment. The equipment at this level can detect and respond to emergencies within its area of control, usually by monitoring for conditions outside of the normal ranges of operation. A programmable logic controller (PLC) or distributed control system (DCS) is usually found at this level. Occasionally, a single loop controller (SLC) can be found within this level.

- Supervisory control and coordination functions between the various Equipment Module Level hardware is performed by the Unit Level. The Unit Level is usually made up of modules that together perform a specific task within the overall process. Supervisory control and data acquisition (SCADA) systems are often found at this level, though more and more the distinction between a DCS and a SCADA system has become blurred and they are used nearly interchangeably.
- The top level which spans the entire process is called the Process Cell Level which is comprised of all the Unit Level hardware. The Process Cell Level is particularly important in the coordination of an emergency, including one potentially caused by a hostile attack, as it would coordinate the emergency action plan of all the levels below it.

The remaining 3 levels, Area Level, Site Level and Enterprise Level, are part of the business network, which is split by organizational requirements. A Demilitarized Zone, separating these levels from the plant control levels is perhaps one of the most important security precautions as usage and security within these levels is more relaxed then it is within the lower levels of control
http://www.defcon.org/images/defcon-18/dc-18-presentations/Polk-Malkewicz-Novak/DEFCON-18-Polk-Malkewicz-Novak-Industrial-Cyber.pdf

9.4 ISO17799

This standard has now been superseded by ISO27002:2005

9.5 ISO24760

This standard covers the following:
ISO24760-1 - IT Security – Identity management: A Framework for Identity Management
ISO24760-2 - IT Security – Identity management: Reference architecture and requirements
ISO24760-3 - IT Security Techniques – Identity management: Practice

9.6 Other ISO Standards

There are numerous ISO standards covering the detail of encryption and authentication techniques; however at this time it is believed that these are outside the scope of this document.

9.7 National Initiatives

The US is leading the way and has already mandated minimum Critical Infrastructure Protection (CIP) standards in the electrical power industry. The Department of Homeland Security- National Cyber Security Division's Control Systems Security Program (CSSP) coordinates efforts among federal, state, local, and tribal governments, as well as industrial control systems owners, operators and vendors, to reduce the likelihood of success and severity of impact of a cyber-attack against critical infrastructure control systems. It publishes regular threat updates and its assessment of the current cyber security threat level here http://www.us-cert.gov/control_systems/index.html
This site is a prime source of up to date information regarding control systems security.

In Europe the European Network and Information Security Agency (ENISA), represents the EU Institutions and Member States. However it lacks focus and deals in generalities rather than specifics. It can be found here http://www.enisa.europa.eu/

In the UK the Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides protective security advice to the national infrastructure. http://www.cpni.gov.uk/

10 Annexe B : ISO 27001 – Policy Headings

The following represents a template for a set of policies aligned with the standard. Note that these are headings, to assist with policy creation, rather than policy statements.

10.1 Chapter 1 INFORMATION SECURITY ORGANIZATION

10.1.1 Information Security policy

Senior Management Support
Information Security Policy Review
Inter-departmental collaboration

10.1.2 Information Security Organization

Independent Review of Information Security Policy
Sharing Information with other Organizations

10.2 Chapter 2 CLASSIFYING INFORMATION AND DATA

10.2.1 Setting Classification Standards

Defining Information
Classifying Information
Accepting Ownership for Classified Information
Labelling Classified Information
Storing and Handling Classified Information
Isolating Top Secret Information
Managing Network Security

10.3 Chapter 3 CONTROLLING ACCESS TO INFORMATION AND SYSTEMS

10.3.1 Controlling Access to Information and Systems

Managing Access Control Standards
Managing User Access
Securing Unattended Workstations
Management Duties
Third Party Service Management
Managing Network Access Controls
Controlling Access to Operating System Software
Managing Passwords
Securing Against Unauthorized Physical Access
Access Control Framework
Access Policy
Restricting Access
Monitoring System Access and Use
Giving Access to Files and Documents
Managing Higher Risk System Access
Controlling Remote User Access
Types of Access Granted to Third Parties
Why access is granted to third parties
Controlled pathway
Node authentication
Diagnostic and Configuration Port Controls
Granting Access to Customers
Acceptable Usage of Information Assets
Monitoring Third Party Services
Third Party Service Changes

10.4 Chapter 4 PROCESSING INFORMATION AND DOCUMENTS

10.4.1 Networks

Configuring Networks

Managing the Network
Network Segregation
Controlling Shared Networks
Routing Controls
Network Security
Accessing your Network Remotely
Defending your Network Information from Malicious Attack
Time-out Facility
Exploitation of Covert Channels
Authentication of Network Connecting Equipment

10.4.2 System Operations and Administration

Appointing System Administrators
Administrating Systems
Controlling Data Distribution
System Utilities
System Use Procedures
Internal Processing Controls
Permitting Third Party Access
Managing Electronic Keys
Managing System Operations and System Administration
Managing System Documentation
Synchronizing System Clocks
Monitoring Error Logs
Scheduling Systems Operations
Scheduling Changes to Routine Systems Operations
Monitoring Operational Audit Logs
Responding to System Faults
Managing or Using Transaction / Processing Reports
Commissioning Facilities Management - FM
Third Party Service Delivery
Log-on Procedures
Corruption of Data
Corrupt Data Controls
Controlling On-Line Transactions

10.4.3 E-mail and the Worldwide Web

Downloading Files and Information from the Internet
Electronic Business Communications
Policy on Electronic Business Communications
Using and Receiving Digital Signatures
Sending Electronic Mail (E-mail)
Receiving Electronic Mail (E-mail)
Retaining or Deleting Electronic Mail
Developing a Web Site
Receiving Misdirected Information by E-mail
Forwarding E-mail
Using Internet for Work Purposes
Giving Information when Ordering Goods on Internet
Setting up Intranet Access
Setting up Extranet Access
Setting up Internet Access
'Out of the Box' Web Browser Issues
Using Internet 'Search Engines'
Maintaining your Web Site
Filtering Inappropriate Material from the Internet
Certainty of File Origin
Cryptographic Keys
Key Management Procedures
Controlling Mobile Code

10.4.4 Telephones & Fax

Making Conference Calls

Recording of Telephone Conversations
Receiving Misdirected Information by Fax
Giving Information when Ordering Goods on Telephone
Persons Giving Instructions over the Telephone
Using Video Conferencing Facilities
Persons Requesting Information over the Telephone
Receiving Unsolicited Faxes

10.4.5 Data Management

Transferring and Exchanging Data
Permitting Emergency Data Amendment
Receiving Information on Disks
Setting up a New Folder / Directory
Amending Directory Structures
Sharing Data on Project Management Systems
Archiving Documents
Information Retention Policy
Setting up New Spreadsheets
Setting up New Databases
Linking Information between Documents and Files
Updating Draft Reports
Deleting Draft Reports
Using Version Control Systems
Updating Customer Information
Using Meaningful File Names
Managing Data Storage
Managing Databases
Using Headers and Footers
Using and Deleting 'Temp' Files
Using Customer and Other Third Party Data Files
Saving Data / Information by Individual Users

10.4.6 Backup, Recovery and Archiving

Restarting or Recovering your System
Archiving Information
Backing up Data on Portable Computers
Managing Backup and Recovery Procedures
Archiving Electronic Files
Recovery and Restoring of Data Files

10.4.7 Document Handling

Managing Hard Copy Printouts
The Countersigning of Documents
Checking Document Correctness
Approving Documents
Verifying Signatures
Receiving Unsolicited Mail
Style and Presentation of Reports
Photocopying Confidential Information
Filing of Documents and Information
Transporting Sensitive Documents
Shredding of Unwanted Hardcopy
Using Good Document Management Practice

10.4.8 Securing Data

Using Encryption Techniques
Sending Information to Third Parties
Maintaining Customer Information Confidentiality
Handling of Customer Credit Card Details
Fire Risks to Your Information
Sending Out Reports
Sharing Information
Dealing with Sensitive Financial Information
Deleting Data Created / Owned by Others

Protecting Documents with Passwords
Printing of Classified Documents

10.4.9 Other Information Handling and Processing

Using Dual Input Controls
Loading Personal Screen Savers
Speaking to the Media
Speaking to Customers
Need for Dual Control / Segregation of Duties
Using Clear Desk Policy
Misaddressing Communications to Third Parties
Using External Disposal Firms
Using Photocopier for Personal Use
Verifying Correctness of Information
Traveling on Business
Checking Customer Credit Limits

10.5 Chapter 5 PURCHASING AND MAINTAINING COMMERCIAL SOFTWARE

10.5.1 Purchasing and Installing Software

Specifying User Requirements for Software
Implementing New / Upgraded Software
Selecting Business Software Packages
Selecting Office Software Packages
Using Licensed Software
Technical Vulnerability Management

10.5.2 Software Maintenance & Upgrade

Applying 'Patches' to Software
Responding to Vendor Recommended Upgrades to Software
Interfacing Applications Software / Systems
Supporting Application Software
Operating System Software Upgrades
Upgrading Software
Support for Operating Systems
Recording and Reporting Software Faults

10.5.3 Other Software Issues

Disposing of Software

10.6 Chapter 6 SECURING HARDWARE, PERIPHERALS AND OTHER EQUIPMENT

10.6.1 Purchasing and Installing Hardware

Specifying Information Security Requirements for New Hardware
Specifying Detailed Functional Needs for New Hardware
Installing New Hardware
Testing Systems and Equipment

10.6.2 Cabling, UPS, Printers and Modems

Supplying Continuous Power to Critical Equipment
Using Centralized, Networked or Stand-Alone Printers
Managing and Maintaining Backup Power Generators
Using Fax Machines / Fax Modems
Using Modems / ISDN / DSL connections
Installing and Maintaining Network Cabling

10.6.3 Consumables

Controlling IT Consumables
Using Removable Storage Media including Diskettes and CDs

10.6.4 Working Off Premises or Using Outsourced Processing

Contracting or Using Outsourced Processing
Using Mobile Phones
Using Business Centre Facilities

Issuing Laptop / Portable Computers to Personnel
Using Laptop/Portable Computers
Working from Home or Other Off-Site Location (Tele-working)
Moving Hardware from One Location to Another
Day to Day Use of Laptop / Portable Computers

10.6.5 Using Secure Storage

Using Lockable Storage Cupboards
Using Lockable Filing Cabinets
Using Fire Protected Storage Cabinets
Using a Safe

10.6.6 Documenting Hardware

Managing and Using Hardware Documentation
Maintaining a Hardware Inventory or Register

10.6.7 Other Hardware Issues

Disposing of Obsolete Equipment
Recording and Reporting Hardware Faults
Clear Screen Policy
Logon and Logoff from your Computer
Dealing with Answering Machines / Voice Mail
Taking Equipment off the Premises
Maintaining Hardware (On-site or Off-site Support)
Using Speed Dialling Telephone Options
Cleaning of Keyboards and Screens
Damage to Equipment
Insuring Hardware
Insuring Laptops / Portables for use domestically or abroad

10.7 Chapter 7 COMBATING CYBER CRIME

10.7.1 Combating Cyber Crime

Defending Against Premeditated Cyber Crime Attacks
Minimizing the Impact of Cyber Attacks
Collecting Evidence for Cyber Crime Prosecution
Defending Against Premeditated Internal Attacks
Defending Against Opportunistic Cyber Crime Attacks
Safeguarding Against Malicious Denial of Service Attack
Defending Against Hackers, Stealth-and Techno-Vandalism
Handling Hoax Virus Warnings
Defending Against Virus Attacks
Responding to Virus Incidents
Collecting Evidence for Cyber Crime Prosecution
Installing Virus Scanning Software

10.8 Chapter 8 CONTROLLING E-COMMERCE INFORMATION SECURITY

10.8.1 E-Commerce Issues

Structuring E-Commerce Systems including Web Sites
Securing E-Commerce Networks
Configuring E-Commerce Web Sites
Using External Service Providers for E-Commerce

10.9 Chapter 9 DEVELOPING AND MAINTAINING IN-HOUSE SOFTWARE

10.9.1 Controlling Software Code

Managing Operational Program Libraries
Controlling Software Code during Software Development
Controlling Program Listings
Controlling Program Source Libraries
Controlling Old Versions of Programs

Managing Program Source Libraries

10.9.2 Software Development

Software Development
Establishing ownership for System Enhancements
Justifying New System Development
Managing Change Control Procedures
Making Emergency Amendments to Software
Separating Systems Development and Operations

10.9.3 Testing & Training

Controlling Test Environments
Using Live Data for Testing
Testing Software before Transferring to a Live Environment
Capacity Planning and Testing of New Systems
Parallel Running
Training in New Systems

10.9.4 Documentation

Documenting New and Enhanced Systems

10.9.5 Other Software Development

Acquiring Vendor Developed Software

10.10 Chapter 10 DEALING WITH PREMISES RELATED CONSIDERATIONS

10.10.1 Premises Security

Preparing Premises to Site Computers
Securing Physical Protection of Computer Premises
Challenging Strangers on the Premises
High Security Locations
Delivery and loading areas
Duress Alarm
Ensuring Suitable Environmental Conditions
Physical Access Control to Secure Areas
Environmental and other external threats

10.10.2 Data Stores

Managing On-Site Data Stores
Managing Remote Data Stores

10.10.3 Other Premises Issues

Electronic Eavesdropping
Cabling Security
Disaster Recovery Plan

10.11 Chapter 11 ADDRESSING PERSONNEL ISSUES RELATING TO SECURITY

10.11.1 Contractual Documentation

Preparing Terms and Conditions of Employment
Using Non-Disclosure Agreements (Staff and Third Party)
Misuse of Organization Stationery
Lending Keys to Secure Areas to Others
Lending Money to Work Colleagues
Complying with Information Security Policy
Establishing Ownership of Intellectual Property Rights
Employing / Contracting New Staff
Contracting with External Suppliers / other Service Providers
Employees' Responsibility to Protect Confidentiality of Data

10.11.2 Confidential Personnel Data

Respecting Privacy in the Workplace
Handling Confidential Employee Information
Giving References on Staff
Checking Staff Security Clearance

Sharing Employee Information with Other Employees
Sharing Personal Salary Information

10.11.3 Personnel Information Security Responsibilities

Using the Internet in an Acceptable Way
Keeping Passwords / PIN Numbers Confidential
Sharing Organization Information with Other Employees
Signing for the Delivery of Goods
Signing for Work done by Third Parties
Ordering Goods and Services
Verifying Financial Claims and Invoices
Approving and Authorization of Expenditure
Responding to Telephone Enquiries
Sharing Confidential Information with Family Members
Gossiping and Disclosing Information
Spreading Information through the Office 'Grape Vine'
Using E-Mail and Postal Mail Facilities for Personal Reasons
Using Telephone Systems for Personal Reasons
Using the Organization's Mobile Phones for Personal Use
Using Organization Credit Cards
Playing Games on Office Computers
Using Office Computers for Personal Use

10.11.4 HR Management

Dealing with Disaffected Staff
Taking Official Notes of Employee Meetings

10.11.5 Staff Leaving Employment

Handling Staff Resignations
Completing Procedures for Terminating Staff or Contractors
Obligations of Staff Transferring to Competitors

10.11.6 HR Issues Other

Recommending Professional Advisors

10.12 Chapter 12 DELIVERING TRAINING AND STAFF AWARENESS

10.12.1 Awareness

Delivering Awareness Programmes to Permanent Staff
Drafting Top Management Security Communications to Staff
Third Party Contractor : Awareness Programmes
Delivering Awareness Programmes to Temporary Staff
Providing Regular Information Updates to Staff

10.12.2 Training

Information Security Training on New Systems
Information Security Officer : Training
User : Information Security Training
Technical Staff : Information Security Training
Training New Recruits in Information Security

10.13 Chapter 13 COMPLYING WITH LEGAL AND POLICY REQUIREMENTS

10.13.1 Complying with Legal Obligations

Being Aware of Legal Obligations
Complying with Copyright and Software Licensing Legislation
Complying with the Data Protection Act or Equivalent
Complying with General Copyright Legislation
Complying with Database Copyright Legislation
Legal Safeguards against Computer Misuse

10.13.2 Complying with Policies

Managing Media Storage and Record Retention
Complying with Information Security Policy

10.13.3 Avoiding Litigation

Safeguarding against Libel and Slander

Using Copyrighted Information from the Internet
Sending Copyrighted Information Electronically
Using Text directly from Reports, Books or Documents
Infringement of Copyright

10.13.4 Other Legal Issues

Recording Evidence of Incidents (Information Security)
Reviewing System Compliance Levels
Renewing Domain Name Licenses – Web Sites
Insuring Risks
Recording Telephone Conversations
Admissibility of Evidence
Adequacy of Evidence
Collection of Evidence

10.14 Chapter 14 DETECTING AND RESPONDING TO IS INCIDENTS

10.14.1 Reporting Information Security Incidents

Reporting Information Security Incidents
Reporting IS Incidents to Outside Authorities
Reporting Information Security Breaches
Software Errors and Weaknesses
Notifying Information Security Weaknesses
Witnessing an Information Security Breach
Being Alert for Fraudulent Activities
When and How to Notify Authorities

10.14.2 Investigating Information Security Incidents

Investigating the Cause and Impact of IS Incidents
Collecting Evidence of an Information Security Breach
Recording Information Security Breaches
Responding to Information Security Incidents

10.14.3 Corrective Activity

Establishing Remedies to Information Security Breaches

10.14.4 Other Information Security Incident Issues

Ensuring the Integrity of IS Incident Investigations
Analysing IS Incidents Resulting from System Failures
Monitoring Confidentiality of Information Security Incidents
Breaching Confidentiality
Establishing Dual Control / Segregation of Duties
Using Information Security Incident Check Lists
Detecting Electronic Eavesdropping and Espionage Activities
Risks in System Usage
Reviewing System Usage

10.15 Chapter 15 PLANNING FOR BUSINESS CONTINUITY

10.15.1 Business Continuity Management

Initiating the Business Continuity Project
Assessing the Business Continuity Security Risk
Developing the Business Continuity Plan
Testing the Business Continuity Plan
Training and Staff Awareness on Business Continuity
Maintaining and Updating the Business Continuity Plan
Realistic Testing Environment for Business Continuity Plans
Impact of the Pace of change on the Business Continuity Plan

11 Annexe C - References

Good General reference site for standards
http://www.us-cert.gov/control_systems/csstandards.html

List of NIST publications for cyber security – excellent source
http://csrc.nist.gov/publications/PubsSPs.html

NIST Security Bulletins – in-depth discussions of SCADA topics
http://csrc.nist.gov/publications/PubsITLSB.html

ISA certification for ISA99
http://www.isasecure.org/Home.aspx

ISO27001 (ISO/IEC 27001:2005)
This is the international standard for an Information Security Management System (ISMS).
http://www.iso27001security.com/html/27001.html
http://www.27001-online.com/secpols.htm

ISO27002 (ISO/IEC 27001:2005)
The ISO 27002 is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001
http://www.iso27001security.com/html/27002.html

ISO27003 (ISO/IEC 27003:2010)
ISO/IEC 27003 provides implementation guidance to help those implementing the ISO27k standards.
http://www.iso27001security.com/html/27003.html

ISO27004 (ISO/IEC 27004:2009)
ISO/IEC 27004 covers information security management measurements, generally known as security metrics. http://www.iso27001security.com/html/27004.html

ISO27005 (ISO/IEC 27005:2008)
Provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach so may be a good approach for The 61508 Association http://www.iso27001security.com/html/27005.html
The BSI's standard for Information Security Risk Management is BS7799-3 but this is complementary to ISO2005

ISO27006 (ISO/IEC 27006:2007)
Specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), http://www.iso27001security.com/html/27006.html

Industrial security from the perspective of the power industry – very good overview which overlaps into process
http://www.defcon.org/images/defcon-18/dc-18-presentations/Polk-Malkewicz-Novak/DEFCON-18-Polk-Malkewicz-Novak-Industrial-Cyber.pdf

Description of Buffer overflow
http://www.watchguard.com/infocenter/editorial/135136.asp