An Introduction to Cyber Security for Safety-Related Systems

The Association would welcome any comments on this publication, see: http://www.61508.org/contact. Whilst every effort has been made to ensure the accuracy of the information contained in this document, neither The 61508 Association nor any of its members will assume liability for any use made thereof.

This document has been created by the 61508 Association as an introduction to the topic of cyber security for safety-related systems with the aim of providing some basic information while the UK industry waits for relevant international standards to be published. It should be noted that Cyber Security is a fast moving landscape and relying on slow changing international standards is not sufficient.

1 - The State of Industry 2016

Cyber security issues are becoming more common in the modern world due to the fact more and more devices are designed with high levels of technology. Devices, systems and networks are becoming increasingly more open and integrated and therefore accessible providing an ever increasing attack surface for cyber security threats. Many safety-related systems were designed and developed at a time when the issue of cyber security was not envisaged. That leaves many of today's current systems potentially vulnerable to new and emerging threats.

Whilst the IT industry is further ahead in relation to cyber security the priorities for Information Technology (IT) are different from those of Operational Technology (OT) and the solutions and mechanisms used are not necessarily applicable to industry and industrial control systems. There are many threat vectors and it is important to bear in mind that not all cyber security incidents are the result of deliberate actions. Many cyber security incidents are triggered accidently or by inadvertent actions. The security threat landscape is constantly changing, however there are some general classifications as described in IEC 62443 of potential threats that an organization should consider:

- Malicious hackers – an individual whose objective is to penetrate the security defences of a third party computer system or network. [ISO/IEC 27002]
- Professional Hackers – an organization funded by a government or other organization specifically aimed at penetrating security defences.
- Disgruntled Employee - an individual who works for the organization who may be inclined to do harm resulting from their state of mind regards the organization.
- Well-meaning employee – an individual who works for the organization, who, during the course of their work, circumvents a security countermeasure in order to "get the job done".
- Third-party contractor – an individual or organization that may have privileged access to the Basic Process Control System (BPCS), Safety Instrumented System (SIS) and/or other control-related systems through an agreement to operate or maintain those systems.
- Automated systems (device-to-device) – automated portions of the BPCS, SIS and/or other control-related systems that have privileged access.

As cyber security is a relatively modern discipline some organisations currently produce guidance and / or standards, most of which are still to be fully developed. Some of this guidance is for the IT industry, some is specifically for industrial control systems and some addresses, at least in part, the requirements for safety-related systems. The most recent versions of the functional safety standards for the Process Industries (IEC 61508 and IEC 61511) have added a mandatory requirement to consider cyber security threats and, if any are identified, take the necessary steps to protect against them. It should also be considered good practice to apply this mandatory cyber security requirement to functional safety in all other industries, for example machinery (IEC 62061 / ISO 13849).

It is important to note, just as in functional safety, cyber security must consider the entire safety function.

The level of risk reduction a system is designed to achieve is commensurate with the effectiveness of, and effort applied to, the cyber security measures and systems. This is particularly relevant to SIS because of the high level of risk reduction attributed to the SIS and the potential for multiple failures and failures that are common across Industrial Automation and Control Systems (IACS) and Safety Reliability Systems (SRS).

In response to the increased cyber security threat, many product manufacturers have developed security concepts and have hardened their devices against attack. However, these improvements are often currently overlooked, and should be included in users' detailed specifications for the cyber security aspects in the procurement phase of a new IACS system. As many security concepts as practicable should be designed into the overall solution including IACS and safety-related system. The consideration of cyber security for functional safety should be a key element of the overall Instrumented Control System (ICS) cyber security procedures.

2 - What is required for IACS / what are we concerned about?

The term Cyber Security is used in many different market sectors. In many of them the main area of concern is Information Security, for example in banking, online retail, and health care. This Information Security requirement is normally managed by an organisation's IT section. The ISO/IEC 2700x family of standards cover Information Security.

The IT industries view of cyber security is related to the control of data and is often referred to as CIA or:

Confidentiality of Data
Integrity of Data
Availability of Data

Confidentiality, integrity and availability (also known as the "CIA triad", as it is often displayed in this form) is a model designed to guide policies for information security within an organisation.

Whilst these are still pertinent for industry and IACS it can be argued that the priority is changed so that we consider them in the order of:

Availability of Data
Integrity of Data
Confidentiality of Data

Sometimes this is also known as the AIC triad, but this is mainly used to avoid misunderstandings associated with the Central Intelligence Agency of the United States of America. The IEC 62443 family of standards cover cyber security for Industrial Automation and Control Systems (IACS) however work is still ongoing in this area.

Safety-related control systems are just a small part of the IACS world but a cyber security management system that covers IACS can also cover the safety-related controls.
When we move into the functional safety arena we adjust our concerns to PEAR:

People
Environment
Asset
Reputation

3 - What is required by the functional safety standards?

IEC 61511-1:2016 states the following:

8.2.4 - A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

- a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);
- a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);
- a description of the potential consequences resulting from the security events and the likelihood of these events occurring;
- consideration of various phases such as design, implementation, commissioning, operation, and maintenance;
- the determination of requirements for additional risk reduction;
- a description of, or references to information on, the measures taken to reduce or remove the threats.

11.2.12 - The design of the SIS shall be such that it provides the necessary resilience against the identified security risks (see 8.2.4).

12.4.2 - The following information shall be contained in the application program or related documentation:

k) If required by the SRS, the means by which:

- communications are made secure (e.g., cyber security measures);

ISA-TR84.00.09-2013 states the following:

The SRS should have a section dedicated to security countermeasures addressing, as a minimum, the following:

- The impact of the security countermeasures should not impact the performance of the SIS.
- If a security countermeasure has the potential to impact the overall response time of the SIF, then the response time impact of the security countermeasure should be incorporated in the calculation of the overall response time of the SIF (e.g., the time from process deviation detection through the process response to final element action).
- Selection of the security countermeasures should consider its ability to support interoperability of different manufacturer's devices without degrading the safety integrity, the safety integrity level (SIL), the reliability (spurious trip rate), and the communication speed.

4 - Other cyber security guidance

In the UK, the Centre for the Protection of National Infrastructure (CPNI) offers specific advice in a series of process control and SCADA good practice guidelines. These have 3 guiding principles, namely:

- **Protect, detect and respond** - It is important to be able to detect possible attacks and respond in an appropriate and timely manner to minimise the impacts.
- **Defence in depth** - No single security measure is fool proof as vulnerabilities and weaknesses can be identified at any time. To reduce these risks, implementing multiple protection measures in series avoids single point failures.
- **Technical, procedural and managerial protection measures** - Technology is insufficient on its own to provide robust levels of protection.

ISA-TR84.00.09-2013, Security Countermeasures Related to Safety Instrumented Systems

Regardless of the cyber security standard, guidance or process that is selected, the main aspects to be considered for cyber security are:

- **Assess and Define Security Threat** – The extent of the threat and potential consequences on site should be considered when deciding how much resource needs to be applied to ensure a proportionate approach is implemented
- **Security Safety Management Systems** – A system of policies and procedures is required to manage and maintain the cyber security aspects for the defined system under consideration.
- **Defining the System under Consideration (SUC)** – The SUC must include all IACS assets including any Safety-Related Systems.
- **Simplified Risk Assessment** – For security threats, it is more difficult to determine the potential consequence of each threat or its likelihood without detailed analysis on an on-going basis as threats, and vulnerabilities to threats, change over time and history is no indication of future likelihood. Therefore, a simplified approach is proposed to identify reasonably practicable risk reduction measures.
- **Implement Risk Reduction Measures** - There is no single method for securing an IACS. Each IACS presents different potential consequences depending upon the threats it is exposed to and its inherent vulnerabilities.

5 - Health & Safety Executive Guidance

The UK Health and Safety Executive have created some operational guidance for Cyber Security in relation to Industrial Automation and Control Systems (IACS). This guidance is not designed to replace any particular standards but, however, is created to facilitate the implementation of cyber security control measures. The guidance is aimed at HSE inspectors but will also be useful for duty holders. This HSE guidance confirms that cyber security of a safety-related system is just one specific aspect of the broader Industrial Automation and Control Systems cyber security topic. The safety-related system however, and especially a SIS, may require additional cyber safeguards for the safety-related zone. Here is a link to the guidance:
http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

6 - The Cyber Security Responsible Person

The responsible person(s) for cyber security of the safety-related systems should come from a process or automation background and must have competence in E, C & I and functional safety together with an understanding of IT technology and cyber security. The responsible person(s) must understand the safety requirements and how they can be impacted by cyber security. All personnel involved with SIS and Cyber Security should participate in on-going skill development and training. As skill requirements change due to new equipment or procedures senior technical and management personnel should provide training to ensure the best outcome for their facility's SIS installations. Cyber security hazards and risk are fast changing therefore the skill sets of the cyber security responsible person must be reviewed frequently.

7 - Detect & Respond

Consideration must be given to how a cyber security issue can be detected and then what response can be taken by responsible and competent personnel. This may require, for a safety-related system, a method of bringing equipment to a safe state or may also require a method to isolate the IACS and / or the safety-related system in the event of a cyber security incident such as a denial of service attack.

Audit, change control and disaster recovery are also required as they are essential elements of any cyber security / safety-related management system, however these are very similar across all IACS. All IACS require investigation of unusual issues, simply re-starting the plant/equipment could mean resumption of operation with a defective IACS, e.g. with malicious code installed.

Once a cyber security incident on a safety-related system has been recognized and dealt with the correct functioning of the safety-related system shall be checked before the system / equipment / process is restarted. Where appropriate, a 'forensic' analysis should be undertaken to identify the nature of the attack, and preventative measures should be implemented to protect against further attacks of that nature. The cyber security threat landscape is forever changing.

8 - References

ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements
ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security controls
ISO/IEC 27003 – Information technology – Security techniques – Information security management system implementation guidance
ISO/IEC 27004 – Information technology – Security techniques – Information security management - Measurement
ISO/IEC 27005 – Information technology – Security techniques – Information security risk management
ISO/IEC 27006 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007 – Information technology – Security techniques – Guidelines for information security management systems auditing
IEC 62443-2-4 – Security for industrial automation control systems – Part 2-4: Security program requirements for IACS service providers
IEC 62443-3-3 – Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels