IET Safety and Security Code of Practice Brief

Dated: 28th February 2017
Issue: 1
Authors: Richard Piggin (Cyber TPN) Andy German (Functional Safety TPN)

1 INTRODUCTION

The IET Cyber and Functional Safety Technical and Professional Networks (TPN) are in place to inspire and promote the continuing professional development of Safety and Cyber Security Engineers and enable their professional registration. Part of the support provided includes publishing Codes of Practice (CoP).

The Safety and Cyber Security TPNs have been working closely together and believe that the provision of a Code of Practice that addresses the through life, design and management essentials for safety and cyber security would help promote and improve good practice.

2 WORKING DEFINITIONS

A safety-related system is defined as a system that, subject to correct operation, is necessary for ensuring and maintaining system safety so far as reasonably practicable.

A safety-related secure system is defined as a system that when subject to hostile acts can ensure and maintain system safety so far as reasonably practicable.

A risk control system is a formal management process in which specific risk areas are considered in order to ensure, so far as is reasonably practicable, that harm is minimised. Regulators tend to use the same risk control systems to promote safe activities.

3 BRIEFING PAPER PURPOSE

The purpose of this briefing paper is to provide potential working group participants with an outline of the Code of Practice's, scope, links with existing standards, target market, benefits and proposed structure.

4 SCOPE

Safety and security disciplines are often independent domains, but with little interaction to date. There is increasing convergence driven through common technologies, platforms and networking, where safe operation of complex systems requires appropriate security. The two disciplines may also conflict, creating new functionality, vulnerabilities and hazards that may require additional mitigations to reduce risk.

New technologies and programmes that include interconnected safety-related programmable electronic (digitisation) systems, including the increasing numbers of complex autonomous systems result in the need for engineers engaged in the design, development, maintenance and use to ensure that these systems are both safe and secure. These systems include but are not limited to:

- Distributed Control Systems;
- Supervisory Control Data Acquisition systems;
- Real-time Position Systems;
- Collision Avoidance Systems;
- Health Monitoring Systems;
- Safety Instrumented Systems;
- Plant Information Systems; and
- Programmable switchgear, governors, drives, sensors & actuators.

5 LINKS WITH STANDARDS & GOOD PRACTICE

The aim of the Code of Practice is to identify current good practice and existing standards (not repeat them) whenever practicable. The following table identifies some of these key standards and good practice.

Reference	Title
DHS ICS-CERT	Cyber security procurement language for control systems
CPNI & DHS - Good practice guide	Cyber security assessments of Industrial control systems
DHS Recommended practice	Developing an Industrial Control Systems Cybersecurity Incident Response Capability
IEC 62061	Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems.
IEC 61511	Functional safety – Safety instrumented systems for the process industry sector
IEC 61513	Nuclear power plants. Instrumentation and control important to safety. General requirements for systems
IEC 15288	Systems and software engineering. System life cycle processes
IEC 61784-3-n	Industrial communication networks-Profiles-Functional safety field buses
IEC 62443-4-2	Security for industrial automation and control systems - Technical security requirements for IACS components
IEC 62443	Industrial communication networks. Network and system security. System security requirements and security levels
IEC TS 63069 ED1 Publication target date: 06/2018	Industrial-process measurement, control and automation- Framework to bridge the requirements for safety and security

ISA TR84.00.09-2013	Security Countermeasures Related to Safety Instrumented Systems (SIS) & Associated IACS
NIST CSF	Framework for improving critical infrastructure cyber security
NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security R2
NIST SP 800-160	Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
NCSC interim guidance CPNI	Security Architecture Principles for OT (to replace Security for Industrial Control Systems in the future).
PAS 555:2013	Cyber Security Risk. Governance and Management
VDI 2182	IT-security for industrial automation

Table 1 - Key Standards (Richard Piggin and Andy German)

6 TARGET MARKET

The guidance provided by this code of practice should be equally applicable for any engineer engaged in the design, development, maintenance and use of safety-related programmable electronic systems. Although the code of practice would have a UK perspective, it should be generally applicable regardless of geographic region.

7 BENEFITS OF THE CODE

The key benefit of the code is to provide current good practice for Engineers and Organisations to ensure that their Cyber Safety risks are managed so far as is reasonably practicable, meeting regulations and hence legislation.

The Health and Safety Executive (HSE) and Office for Nuclear Regulation (ONR) are developing guidance for their inspectors which provides an “interpretation of current standards on industrial communication network and system security, and functional safety in so far as they relate to the control of major hazards for safety to people and the environment.” This code should help in the provision of adequate evidence of Cyber and Safety risk management for such inspections.

8 PROPOSED STRUCTURE

8.1 APPLICABILITY

The guidance would apply to all industrial sectors that work with safety-related systems that can potentially cause harm.

8.2 UNCOMMON LANGUAGE

The domains of Cyber Security and Safety use differing language to descibe the same issues and the Code of Practice would include a simple translator for common terms. Table 2 below provides some examples.

Cyber Effects[1]	Safety-related Functional Effect
Degradation	Partial loss of safety function (less)
Interruption	Loss of function (no, not)
Modification	Incorrect function - not as designed (as well as, part of, reverse, other than, early, late, before after)
Fabrication	Erroneous data (as well as, other than)
Unauthorised use	Erroneous operation (other than)
Interception	Loss of data (other than)

Table 2 - Safe and Secure translator (Andy German)

8.3 SAFE AND SECURE PRINCIPLES

All codes of practice benefit from principles that then drive the detailed codes. These principles would need to be developed and agreed but could include the following:

1. Potential for safety (including Cyber) harm must be demonstrated to be "As low as Reasonably Practicable" (ALARP).
2. Fault and vulnerability (see figure Figure 3 - Common Fault and Vulnerability Principles (Andy German)) avoidance, detection, removal and warning techniques are proportionate to the potential harm (including common causes) and required integrity level.
3. No single point of failure or vulnerability (e.g. zero-day and systematic design faults always assumed to exist) for potentially catastrophic hazards/threats.
4. No hidden failure or vulnerability that could result in the majority of the system integrity being lost for high integrity systems.
5. Security functional (e.g. loss of privacy) threat analysis conducted as part of the functional failure analysis.
6. Minimal rights to access (whitelisting) safety-related data or services.
7. Air gaps are not considered as viable mitigation.

[1] Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder. Paperback – 3 Aug 2014 by Don Murdoch

8.4 LIFECYCLE MANAGEMENT

Lifecycle management section would provide an outline of the requirements to manage safety and cyber security through life; these also provide Regulated required Risk Control Systems. Suggested topics include:

- Governance
- Roles & Responsibilities including duty holding
- Competency and training
- Safety and security programme and management system
- Competency
- Training and Skills
- Process planning
- Design basis
- Requirements specification
- Architecture, functional and item integrity allocation
- Selection of pre-developed items
- Detailed design and implementation
- System integration
- System validation
- Installation, integration and commissioning
- Operation and maintenance
- Configuration management
- Modification
- Incident and accident management
- Emergency procedures
- Decommissioning/Retirement

8.5 SAFE AND SECURE BY DESIGN

This section would provide guidance on selecting an appropriate systems engineering approach including life cycle and safe and secure requirement decomposition methodology to ensure that safety and security features are identified and embodied in the design and build (see Figure 1 below). In addition, it should cover potential faults and vulnerabilities that are discovered using

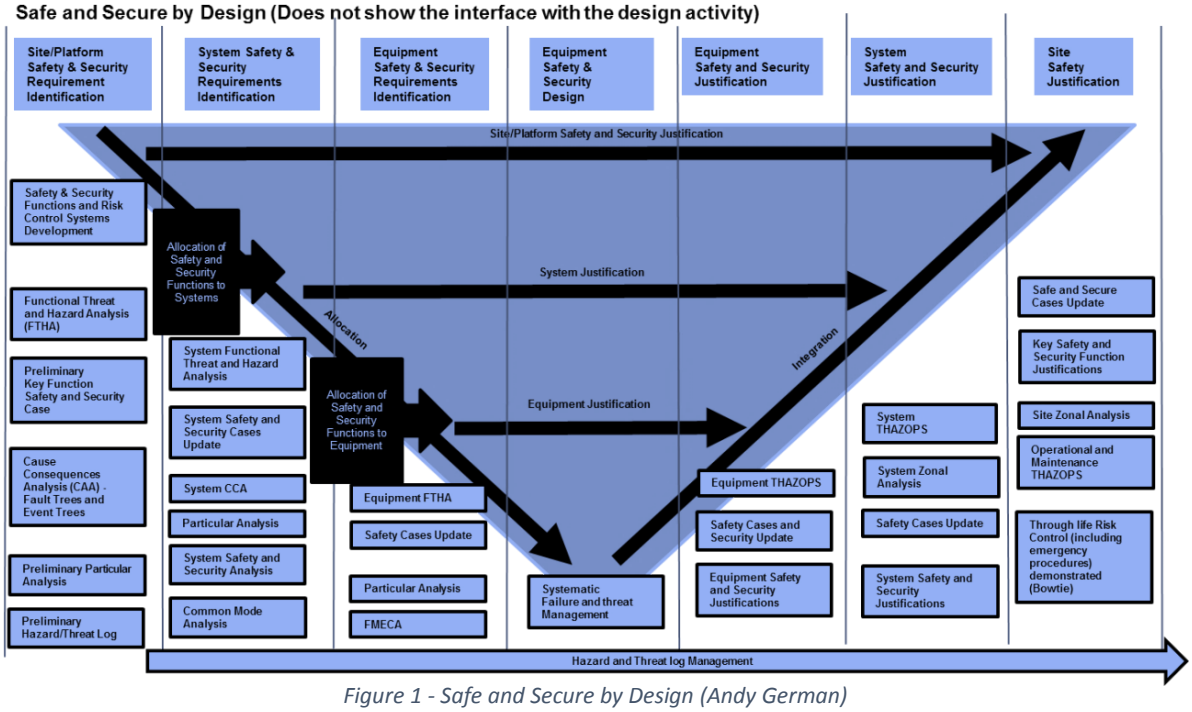

Figure 1 - Safe and Secure by Design (Andy German)

combined techniques (e.g. Functional Failure Analysis, System Threat and Hazard Analysis, Common Cause Analysis) and mitigations designed into the site/platform, systems, equipment and components. These features and mitigations should be verified and validated throughout the build,

test and acceptance activities. In particular, the Aerospace ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment methodology can be considered.

A variety of secure development lifecycles (SDLC) good practices are available. This CoP can outline security engineering good practice to complement the safety engineering lifecycle, such as new National Institute of Standards and Technology (NIST) guidance. Cybersecurity assurance programmes can utilise good practice developed in IEC 62443-4-1 Product Development Requirements and IEC 62443-4-2 Technical Security Requirements for industrial control system components. These standards focus upon secure product development good practice, (including IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems), verification and testing, and lifecycle management (see **Error! Reference source not found.**).

Figure 2- Security lifecycle defence in depth philosophy (Richard Piggin)

The US NIST recently published the Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (SP 800-160). It provides an engineering perspective and describes the actions necessary to develop more defensible and survivable systems, in light of the growing adverse consequences of cyber-attacks, disruptions and hazards, where the need for trustworthy secure systems is paramount.

Security topics are addressed in the context of the system life cycle processes contained in ISO IEC IEEE 15288 and the security-related activities and tasks that are described in SP 800-160, which is designed as complementary guidance. It is intended to be flexible in application acting as a handbook for achieving identified security outcomes in an engineering perspective on system life cycle processes. Further publications in the SP 800-160 series are planned to cover other security engineering topics in the lifecycle context of ISO/IEC/IEEE 15288.

8.6 RISK ASSESSMENT

Approaches to bridge safety and security risk assessment will be described to provide comprehensive methodologies and address the use of the ALARP principle.

8.7 MODELS

The basic models (see Figure 3 - Common Fault and Vulnerability Principles (Andy German)) for managing faults and vulnerabilities are coincident at the highest levels and the code of practice

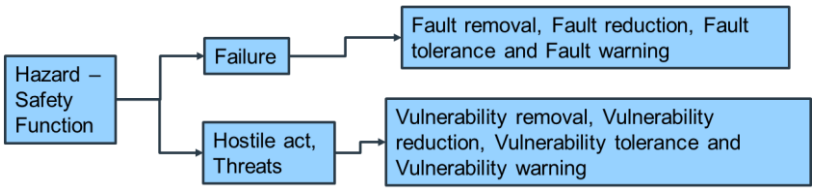

Figure 3 - Common Fault and Vulnerability Principles (Andy German)

would explore these further and be clear about similarities and differences.

8.8 REGULATOR REQUIRED RISK CONTROL SYSTEMS

Both Safety (Regulation defined) and Cyber Security[2] use common risk control systems to manage safety and security risks. It is contended that combining these risk control systems would provide both:

- synergy and therefore greater understanding of the risks and their management; and
- ensure that cyber security effort is proportional to the safety hazards being managed.

8.9 MANAGING HAZARDS AND VULNERABILITIES THROUGH LIFE

Although this section would include continuing management of hazards and vulnerabilities through life using appropriate secure lifecycle processes (including procurement for instance) and Risk Control Systems it would also include guidance about existing safety-related systems and their security assessment and vulnerability mitigation.

[2] PAS 555:2013 Cyber Security Risk. Governance and Management.