Integrating Cyber Security and Safety Systems Engineering Disciplines with a common Code of Practice

Dr Richard Piggin
Introduction

• Background
• Motivation
• Safety Engineering ↔ Cyber Engineering
• Safety-related Secure System - Working Definition
• Proposal & approach
• Next steps
Who is involved

Andrew Cooney - IET Standards Portfolio Development Manager
Andy German - Functional Safety TPN
Richard Piggin – Cyber TPN
Motivation for this Safe and Secure Activity

Industry required to address both Safety and Security (Cyber) by regulation

Increasing Digitisation, System of Systems, Autonomy

Current Safety and Cyber Security Standards are not integrated

IET Code of Practice?
Safety Engineering ↔ Cyber Engineering

Safety engineering is a discipline that ensures the development, operation and disposal of products, services or systems are safe. This is informed by hazard identification, hazard analysis, risk analysis, safety analysis. The application of risk control systems including recognised good engineering practice. Knowledge of failure modes that can contribute to an accident.

Cyber engineering is a discipline that ensures the development, operation and disposal of products, services or systems are secure. This is informed by threat identification, threat analysis, risk analysis, vulnerability analysis. The application of risk control systems including recognised good engineering practice. Knowledge of attack modes that can contribute to loss.
Safety-related Secure System - Working Definition

“A system that when subject to failure and/or a hostile act can ensure and maintain system safety so far as reasonably practicable”

Expectations

All complex safety involved systems have residual design faults and vulnerabilities

Safety involved systems will be subject to hostile acts during their life

Safety and Security considered at the system and functional level to support

Proportional risk management

Defence in-depth always required to prevent failure and vulnerability condition propagation to a harmful condition
Proposal

The IET should develop a Safety and Security Code of Practice

A practical how to guide

Focus on safety involved systems for critical infrastructure

Not a standard but a road map identifying good practice

Support combined skills and competency identification and development

Expected to develop over the next few years
The briefing paper
Working Groups

- Principles
- Language
- Safe & Secure by design through life
- Supply chain and contracting
- Combined risk assessments, risk controls including ALARP for security
Principles

- The enterprise as a minimum meet the jurisdiction’s legislative and regulatory requirements for both safety and security
- Individuals, teams and organisations must be demonstrably competent to undertake the enterprise critical element’s Security and Safety activities
- The enterprise has demonstrably effective Systems Engineering, Quality and Asset Management Systems need to be in place to facilitate effective application of the CoP
- An explicit combined safe and secure enterprise critical design is coevolved
- The enterprise assurance case must demonstrate that the potential harm including those from vulnerabilities due to security threats, are reduced “SFARP”
- The enterprise assurance case is maintained throughout the life of the enterprise, its update cycle is commensurate with both the technologies refresh rates, and is justified by the continuing ageing system’s risk management activities
- The enterprise critical element management enables a learning culture and the design allows lessons to be learnt from incidents and accidents
# Language

<table>
<thead>
<tr>
<th>Cyber Effects</th>
<th>Safety-related Functional Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degradation</td>
<td>Partial loss of safety function (less)</td>
</tr>
<tr>
<td>Interruption</td>
<td>Loss of function (no, not)</td>
</tr>
<tr>
<td>Modification</td>
<td>Incorrect function - not as designed (as well as, part of, reverse, other than, early, late, before after)</td>
</tr>
<tr>
<td>Fabrication</td>
<td>Erroneous data (as well as, other than)</td>
</tr>
<tr>
<td>Unauthorised use</td>
<td>Erroneous operation (other than)</td>
</tr>
<tr>
<td>Interception</td>
<td>Loss of data (other than)</td>
</tr>
</tbody>
</table>
Safe and Secure by Design (Does not show the interface with the design activity)
Combined risk assessments, risk controls including ALARP for security

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification and permissioning</td>
<td>Maintenance of condition</td>
<td>Configuration and Change Management</td>
<td>Documentation and evidence</td>
<td>Culture</td>
<td>Roles and responsibilities</td>
</tr>
<tr>
<td>Competency and training</td>
<td>Organisational competency</td>
<td>Incident and accident reporting</td>
<td>Emergency preparedness</td>
<td>Safe and secure operating envelope</td>
<td>Evidence (Safety) Case – Snap shot of RCS effectiveness</td>
</tr>
<tr>
<td>Test and evaluation</td>
<td>Quality Assurance and Audit</td>
<td>Independent verification and validation (ITE, ISAs etc.)</td>
<td>Technology specific risk mitigations and limitations</td>
<td>Control of hazardous materials</td>
<td>Product/System boundary and control</td>
</tr>
</tbody>
</table>
Supply chain and contracting

ISO/IEC 27001:2013 international standard that describes best practice for an information security management system

Cyber Essentials

Open source data management – suppliers of systems, equipment and services for critical infrastructure projects and their employees are not to publish information (including social media) that has the potential to create cyber vulnerabilities
Next Steps

Notes from this working group

Set up share working space to support remote collaboration

Cyber and Functional Safety TPNs to Publish the development programme

Request participation from wider IET, other Institutes, Industry, Regulators, etc
For more information:

Richard.Piggin@atkinsglobal.com

www.atkinsglobal.com/cyber