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

Dr Richard Piggin

16 November 2017 - © Atkins Limited

Introduction

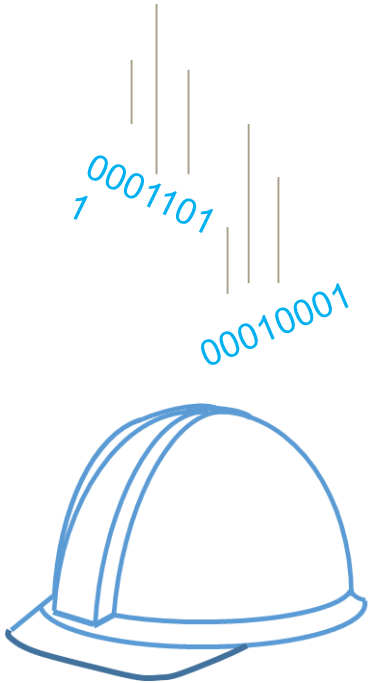
- Background
- Motivation
- Safety Engineering ↔ Cyber Engineering
- Safety-related Secure System - Working Definition
- Proposal & approach
- Next steps

Who is involved

Andrew Cooney - IET Standards Portfolio Development Manager

Andy German - Functional Safety TPN

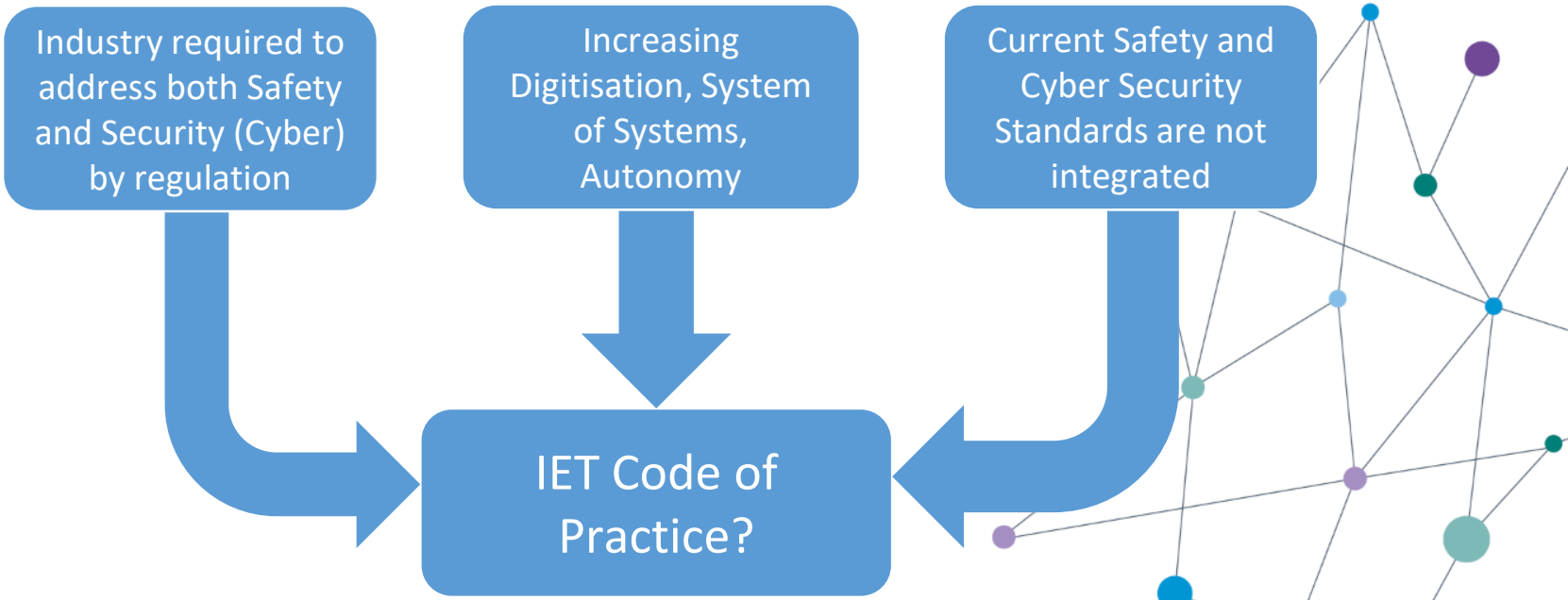
Richard Piggin – Cyber TPN



ATKINS

Motivation for this Safe and Secure Activity

ATKINS



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

ATKINS

"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

ATKINS

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

IET Safety and Security Code of Practice Brief

Authors: Richard Piggin (Cyber TPN) Andy German (Functional Safety TPN)

Dated: 2nd March 2017
Issue: 1

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.

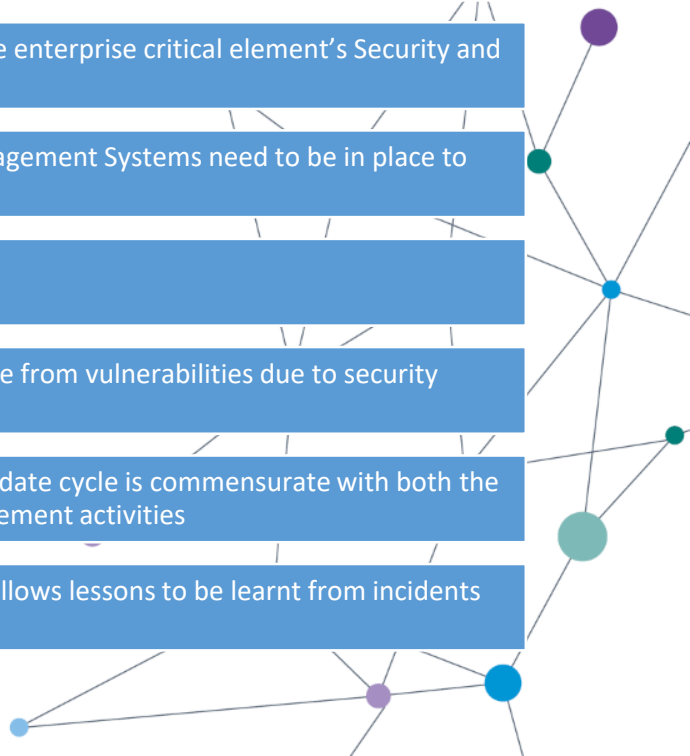
1

Working Groups

ATKINS

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

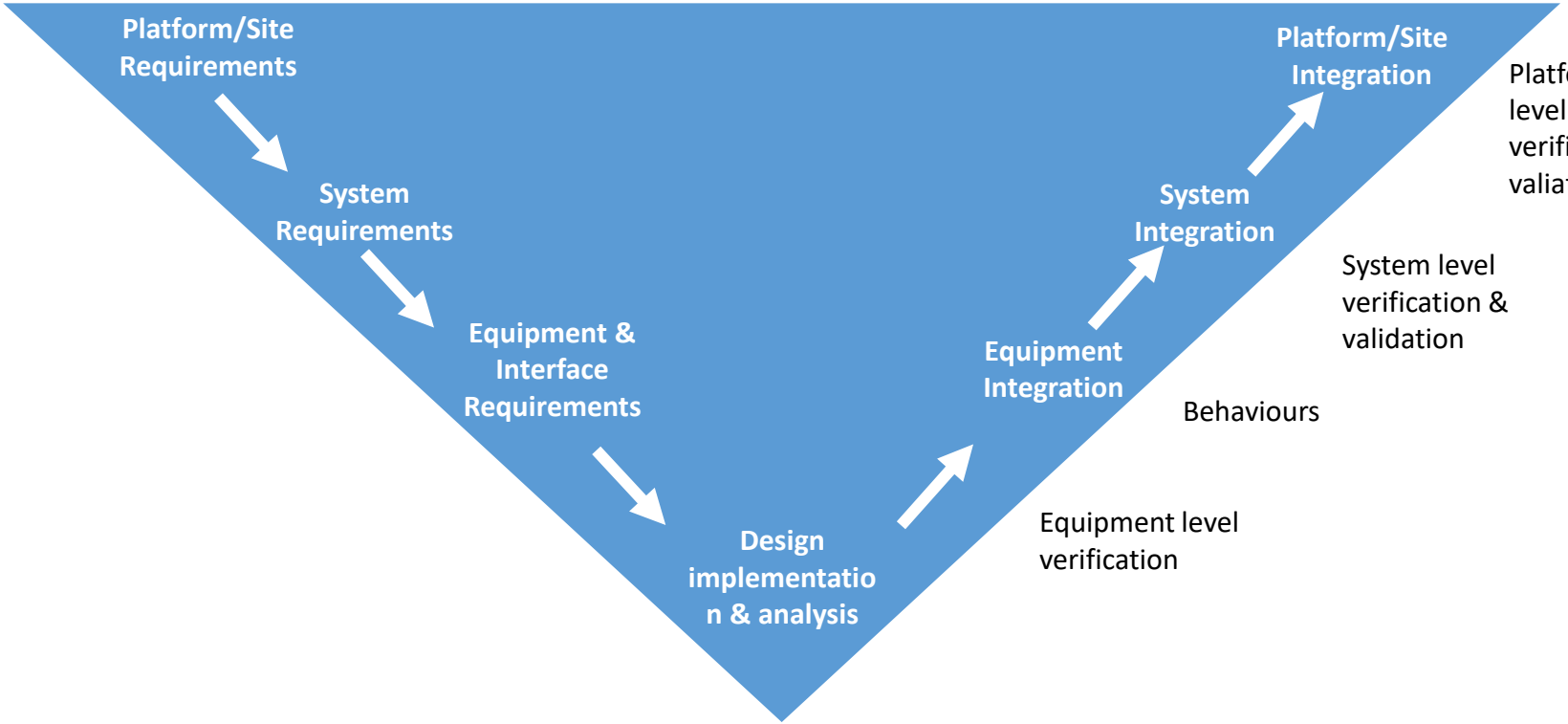


Language

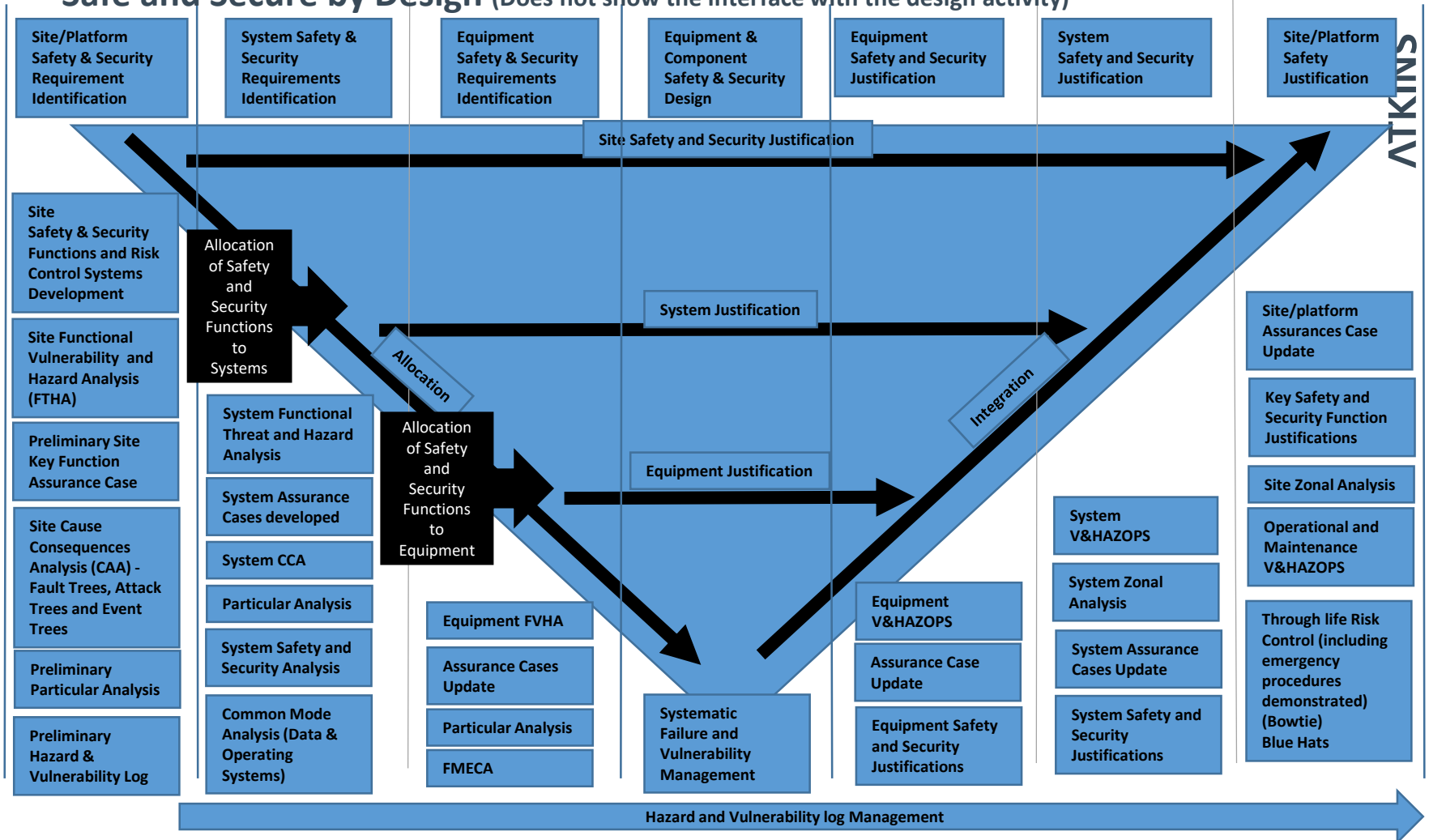
Cyber Effects	Safety-related Functional Effect
Degradation	Partial loss of safety function (less)
Interruption	Loss of function (no, not)
Modification	Incorrect function - not as designed (as well as, part of, reverse, other than, early, late, before after)
Fabrication	Erroneous data (as well as, other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

Safe and Secure by Design

Functional Requirement	Safety	Security	Child Requirements	Metric	Test & Acceptance

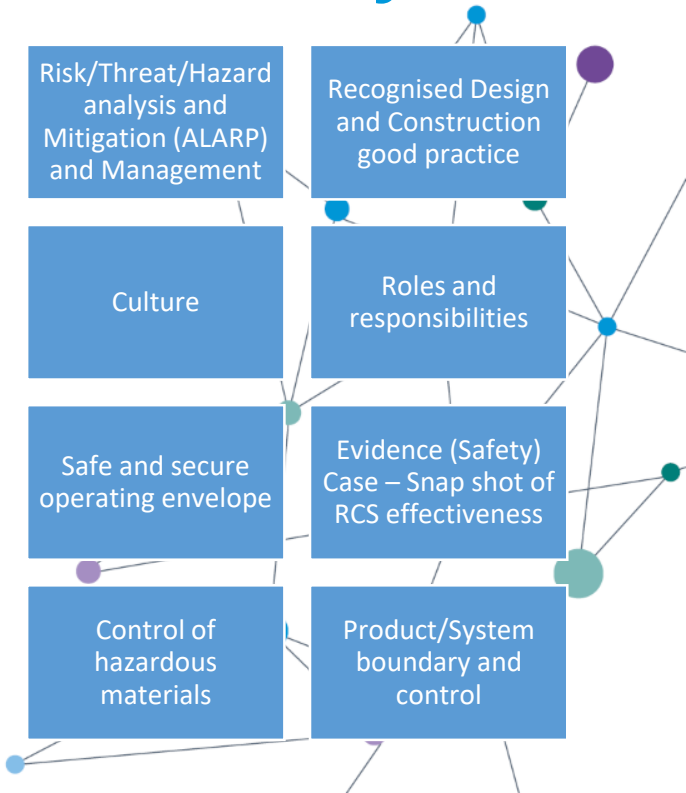


Safe and Secure by Design (Does not show the interface with the design activity)



Combined risk assessments, risk controls including ALARP for security

Governance and Management Systems	System, Equipment, Service Safety and Security Plans	Requirements Management	Risk/Threat/Hazard identification	Risk/Threat/Hazard analysis and Mitigation (ALARP) and Management	Recognised Design and Construction good practice
Certification and permissioning	Maintenance of condition	Configuration and Change Management	Documentation and evidence	Culture	Roles and responsibilities
Competency and training	Organisational competency	Incident and accident reporting	Emergency preparedness	Safe and secure operating envelope	Evidence (Safety) Case – Snap shot of RCS effectiveness
Test and evaluation	Quality Assurance and Audit	Independent verification and validation (ITE, ISAs etc.)	Technology specific risk mitigations and limitations	Control of hazardous materials	Product/System boundary and control

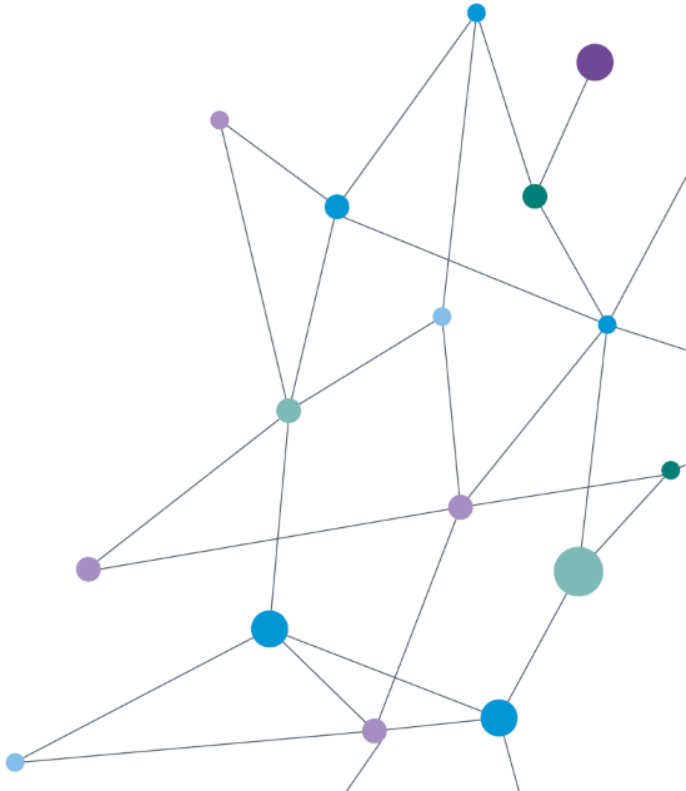


Supply chain and contracting

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

ATKINS

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