SECURITY INFORMED SAFETY

WHY ITS EASY, WHY ITS HARD

Professor Robin E Bloomfield FREng

Adelard LLP
City, University of London

reb@adelard.com
r.e.bloomfield@city.ac.uk

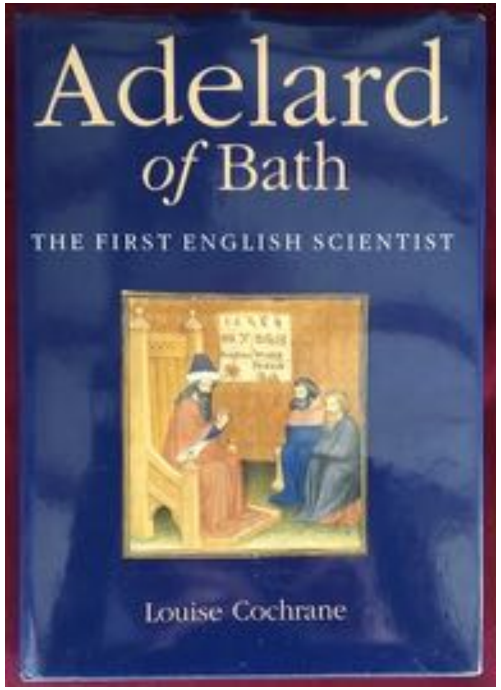
January 2019

PT/632/309/81

Adelard LLP, 24 Waterside, 44-48 Wharf Road, London N1 7UX
T +44 20 7832 5850 E office@adelard.com W www.adelard.com

ADELARD

- Adelard is a specialized, influential product and services company working on safety, security and resilience since 1987
- Wide-ranging experience of assessing computer-based systems and components
- Work across different industrial sectors, including nuclear, rail, defence, aviation, financial, medical
  - Policy, methodology, technology
  - Product for managing safety and assurance cases (ASCE)
  - Security-informed safety and dependability
- Consultants PhD level, international team
- Partner in UK Research Institute on Trustworthy ICS (RiTICS)



ASSURANCE

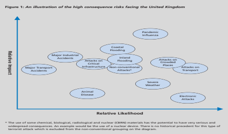
- trust and trustworthiness are of enormous societal value
- assurance is an enabler of innovation
- security requires innovation

OUTLINE

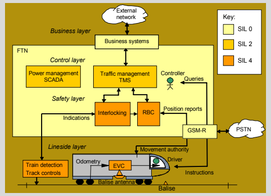
- Background
- Assessing impact of security on safety
  - Projects and policies
- Outcomes and ongoing work
  - Security informed safety case
  - Codes of Practice (PAS and CoP)
  - research projects
- Discussion and conclusion
  - Why easier than feared, why hard

SECURITY-INFORMED SAFETY AND RESILIENCE

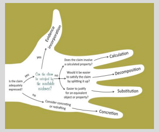
Systems of systems



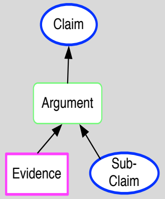
Risk assessment



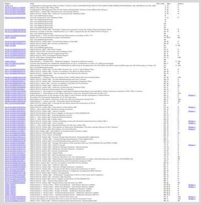
Training



Assurance and policy Framework

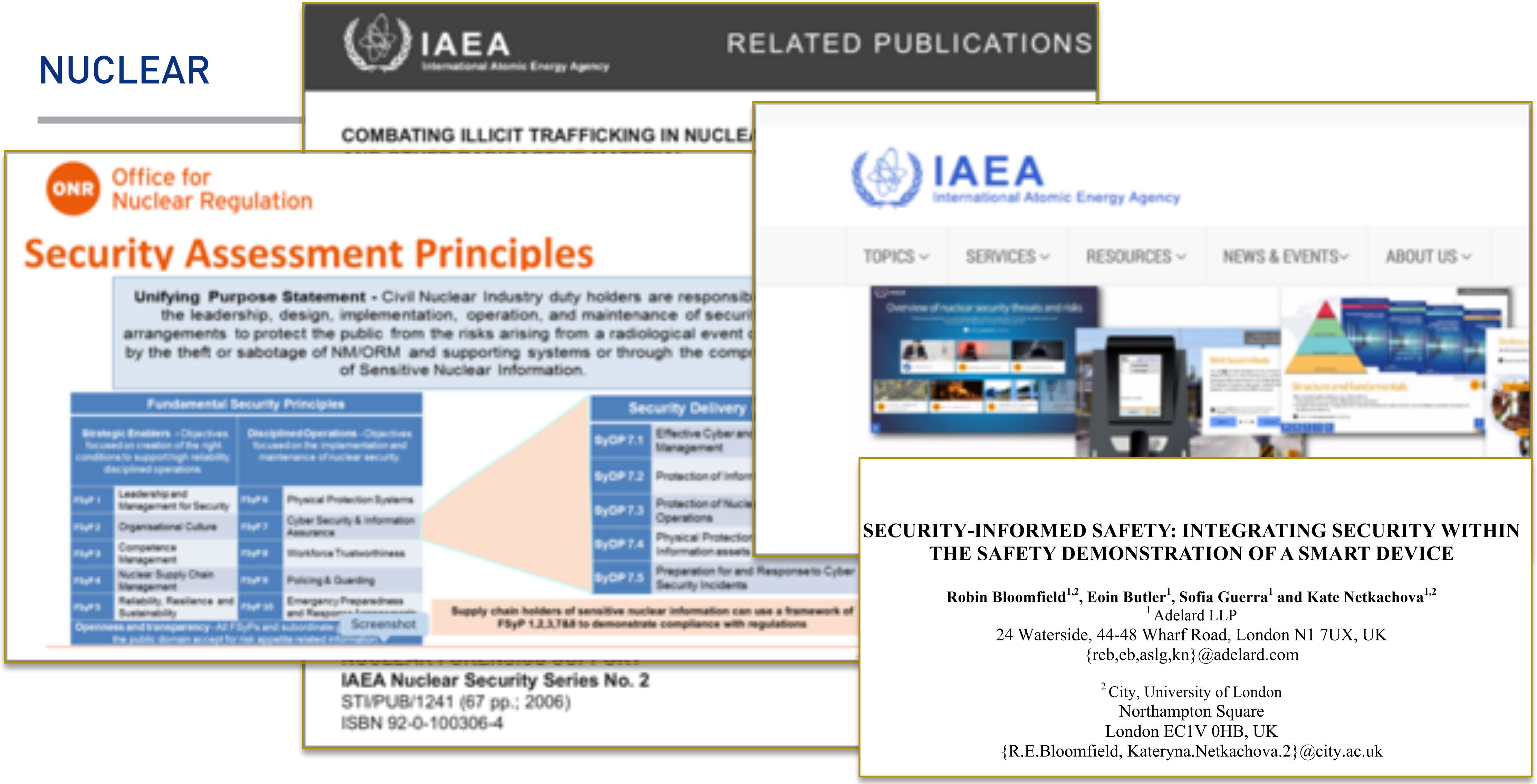


Standards and policy



Many projects: Ritics, Sesamo, Aquas, CPNI, IEC, BSI, IET …

NUCLEAR



IAEA International Atomic Energy Agency RELATED PUBLICATIONS

COMBATING ILLICIT TRAFFICKING IN NUCLEA

IAEA Nuclear Security Series No. 2
STI/PUB/1241 (67 pp.; 2006)
ISBN 92-0-100306-4

ONR Office for Nuclear Regulation

Security Assessment Principles

Unifying Purpose Statement - Civil Nuclear Industry duty holders are responsib the leadership, design, implementation, operation, and maintenance of securi arrangements to protect the public from the risks arising from a radiological event by the theft or sabotage of NM/ORM and supporting systems or through the comp of Sensitive Nuclear Information.

Fundamental Security Principles			
Strategic Enablers - Objectives focused on creation of the right conditions to support high reliability, disciplined operations.		**Disciplined Operations** - Objectives focused on the implementation and maintenance of nuclear security.	
FSyP 1	Leadership and Management for Security	FSyP 6	Physical Protection Systems
FSyP 2	Organisational Culture	FSyP 7	Cyber Security & Information Assurance
FSyP 3	Competence Management	FSyP 8	Workforce Trustworthiness
FSyP 4	Nuclear Supply Chain Management	FSyP 9	Policing & Guarding
FSyP 5	Reliability, Resilience and Sustainability	FSyP 10	Emergency Preparedness and Respo

Openness and transparency - All FSyPs and subordinate the public domain accept for risk appetite related information.

Screenshot

Security Delivery	
SyDP 7.1	Effective Cyber an Management
SyDP 7.2	Protection of Inform
SyDP 7.3	Protection of Nucle Operations
SyDP 7.4	Physical Protection Information assets
SyDP 7.5	Preparation for and Response to Cyber Security Incidents

Supply chain holders of sensitive nuclear information can use a framework of FSyP 1,2,3,7&8 to demonstrate compliance with regulations

IAEA International Atomic Energy Agency

TOPICS
SERVICES
RESOURCES
NEWS & EVENTS
ABOUT US
Overview of nuclear security threats and risks
Structure and fundamentals

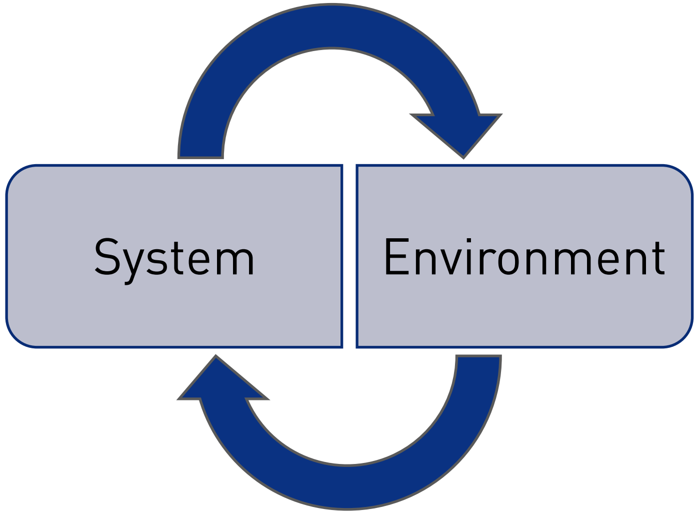
SECURITY-INFORMED SAFETY: INTEGRATING SECURITY WITHIN THE SAFETY DEMONSTRATION OF A SMART DEVICE

Robin Bloomfield[1,2], **Eoin Butler**[1], **Sofia Guerra**[1] **and Kate Netkachova**[1,2]
[1] Adelard LLP
24 Waterside, 44-48 Wharf Road, London N1 7UX, UK
{reb,eb,aslg,kn}@adelard.com

[2] City, University of London
Northampton Square
London EC1V 0HB, UK
{R.E.Bloomfield, Kateryna.Netkachova.2}@city.ac.uk

SAFETY AND SECURITY

- Safety –the damage the system can do to the environment

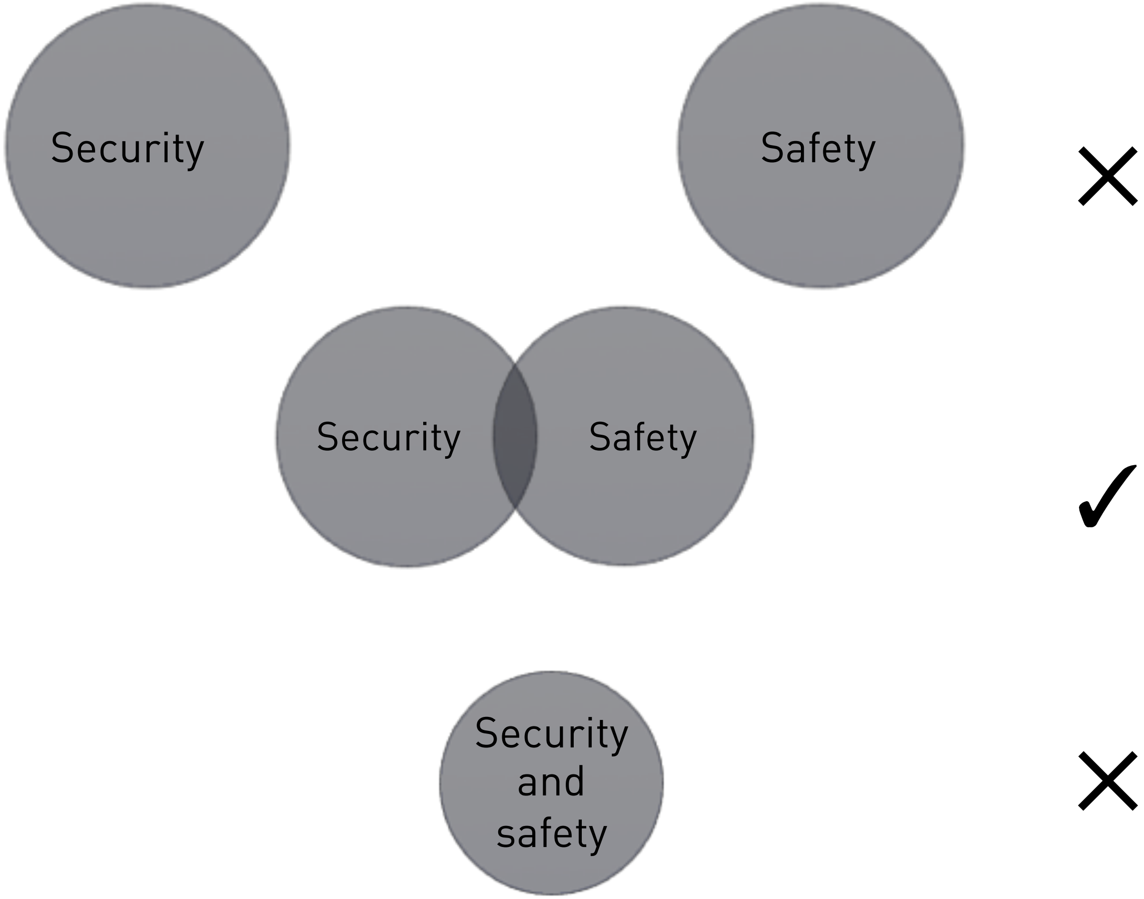


- Security – the damage the environment (in a broad sense) does to the system

SLOGAN

“If it’s not secure, it’s not safe”

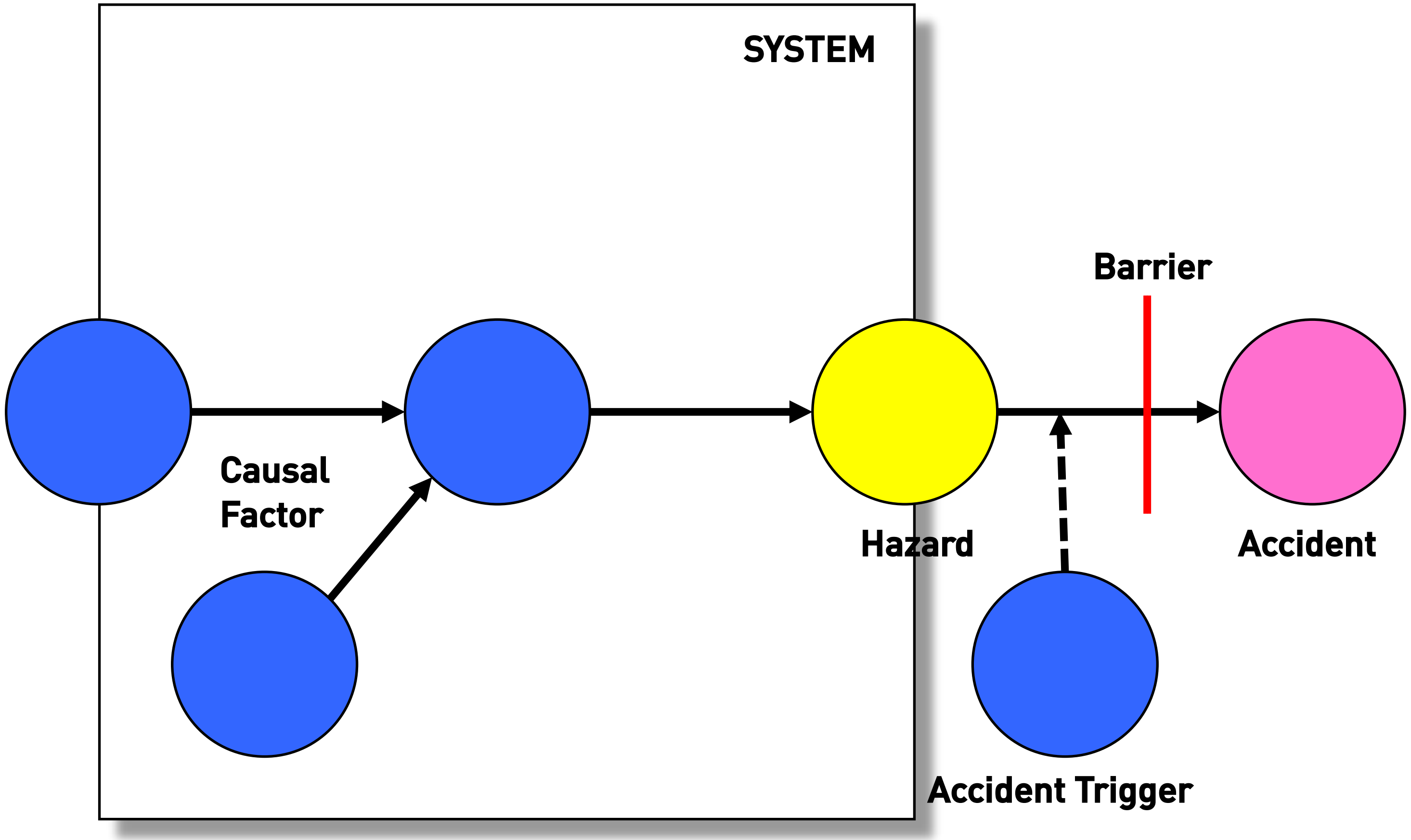
HOW MUCH SHOULD SAFETY AND SECURITY BE INTEGRATED?



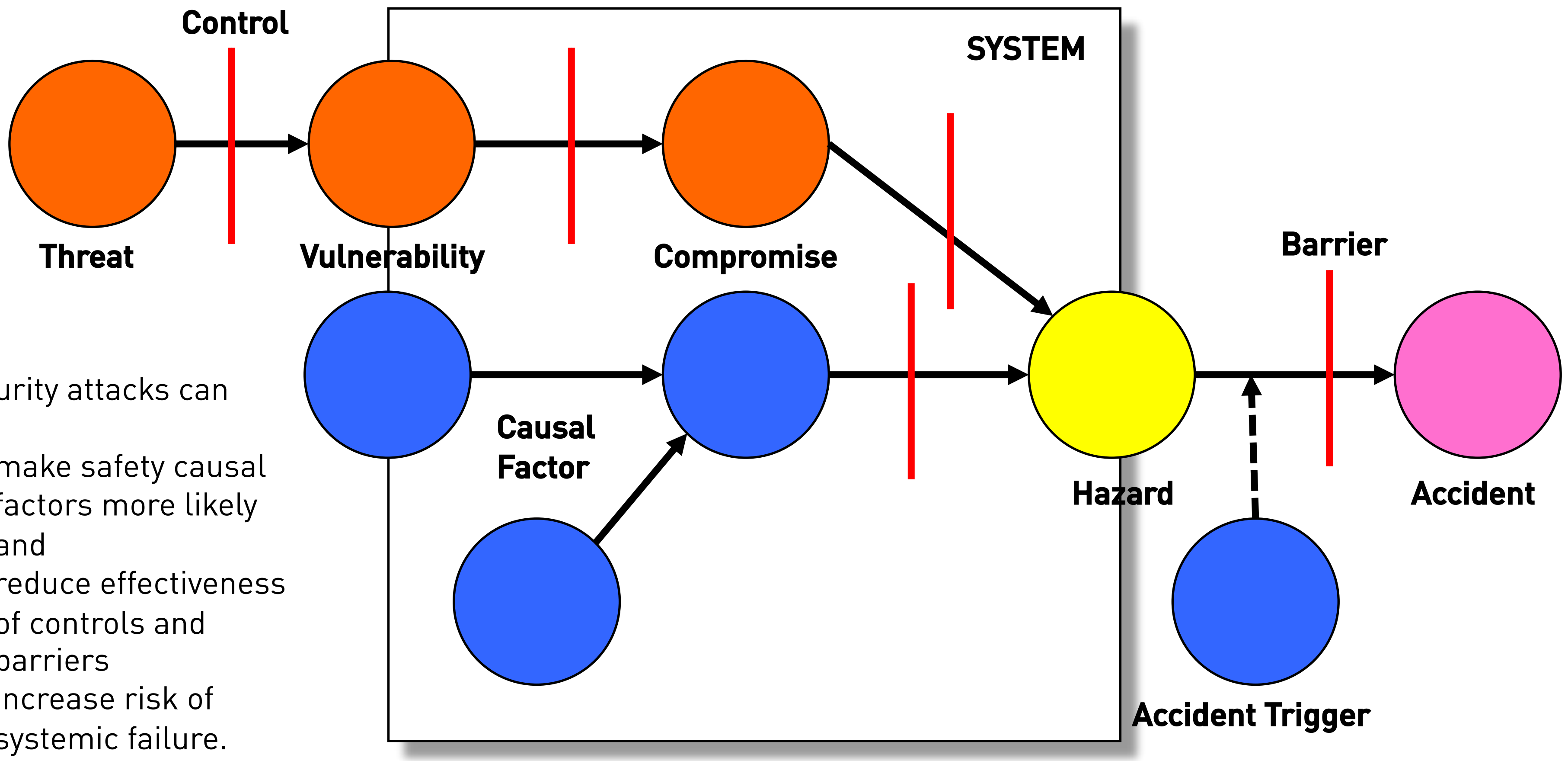
IS THE SECURITY OF INDUSTRIAL SYSTEMS A REAL SAFETY CONCERN?

- Examples
- Late 2014, German steel mill attack
  - Initial breach via “spear fishing”
  - Safety controls overridden
  - Extensive damage to blast furnace
  - Probably a nation state attack (advanced persistent threat – APT)
- December 2015, Cyber attack on Ukraine Power grid
  - Cut off 103 towns and cities in Ukraine
  - Russia blamed
- December 2017 malware detected in Middle Eastern petrochemical facility
  - Safety system shutdown as the result of a Triton malware attack.
  - System had been penetrated over a 2 years before detection
  - Tampering with the process control AND safety systems
  - Russia blamed

SAFETY ANALYSIS



COMBINED SAFETY AND SECURITY ANALYSIS



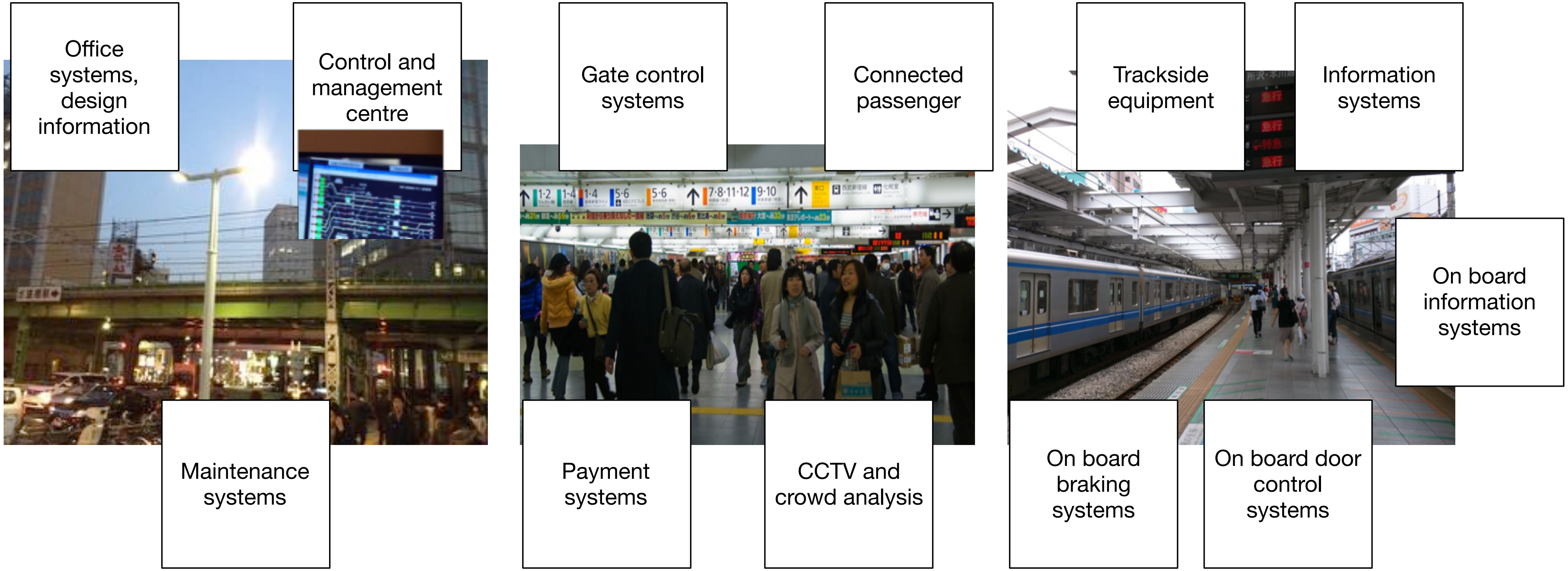
Security attacks can also

- make safety causal factors more likely and
- reduce effectiveness of controls and barriers
- increase risk of systemic failure.

TYPICAL URBAN TRANSPORT SYSTEM

Images http://jpninfo.com/57046

SYSTEMS OF SYSTEMS



Office systems, design information

Control and management centre

Maintenance systems

Gate control systems

Connected passenger

Payment systems

CCTV and crowd analysis

Trackside equipment

Information systems

On board information systems

On board braking systems

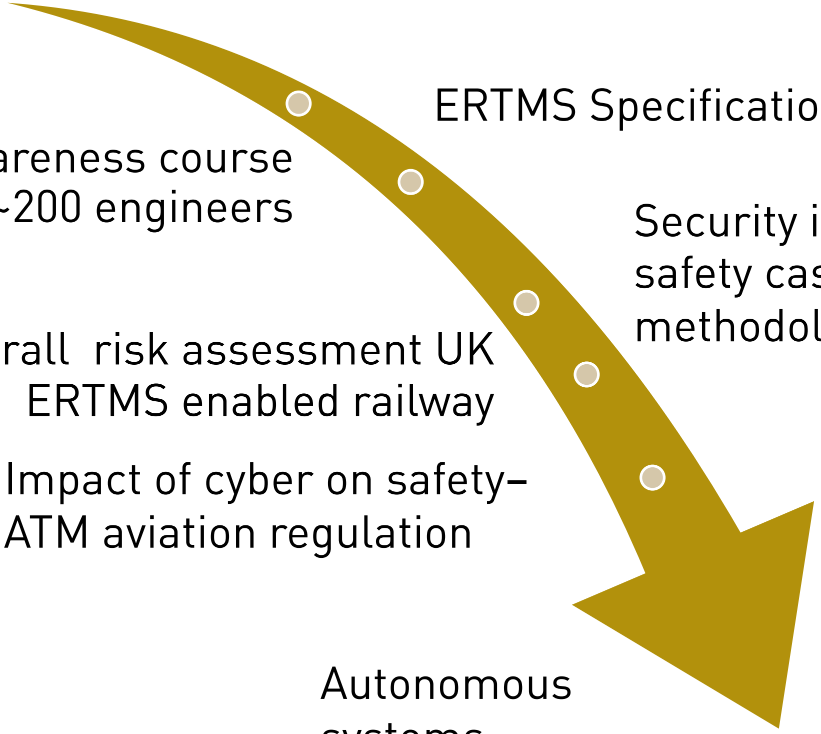
On board door control systems

SAFETY AND SECURITY SYSTEMS

- Plant/Systems with an overall mission, part of which is safety and security
  - Main mission is to deliver a service
- Safety systems with one mission
  - Shut down, stop
- Security systems with one mission
  - Access control, CCTV
- Security systems that can directly impact safety
  - Crowd control, PA and communications
- Systems that can be used in different stages of an attack
  - e.g for phishing, gaining information
- Architectures that integrate all types of systems
- Complex incidents - enabled, amplified by systems interactions

ASSESSING IMPACT OF SECURITY ON SAFETY

Security, resilience and safety



Security and safety

ERTMS Specification analysis

Awareness course
~200 engineers

Security informed
safety case
methodology

Overall risk assessment UK
ERTMS enabled railway

Specific train ETCS
assessments

Impact of cyber on safety–
ATM aviation regulation

Impact on automotive

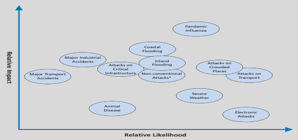
Autonomous
systems

Security, resilience and
safety

SECURITY-INFORMED SAFETY AND RESILIENCE - OVERVIEW

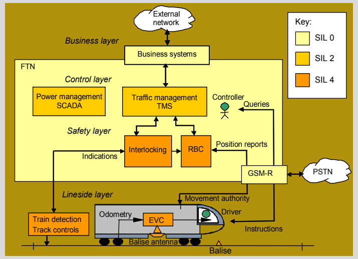
Systems of systems

Figure 1: *An illustration of the high consequence risks facing the United Kingdom*

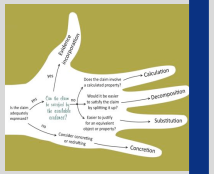


* The use of some chemical, biological, radiological and nuclear (CBRN) materials has the potential to have very serious and widespread consequences. An example would be the use of a nuclear device. There is no historical precedent for this type of terrorist attack which is excluded from the non-conventional grouping on the diagram.

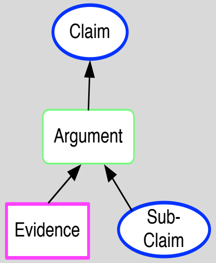
Risk assessment



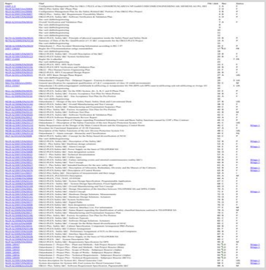
Training


Evidence incorporation
yes
Is the claim adequately expressed?
yes
Can the claim be satisfied by the available evidence?
no
Does the claim involve a calculated property?
Calculation
Would it be easier to satisfy the claim by splitting it up?
Decomposition
Easier to justify for an equivalent object or property?
Substitution
no
Consider concreting or redrafting
Concretion

Assurance and policy Framework

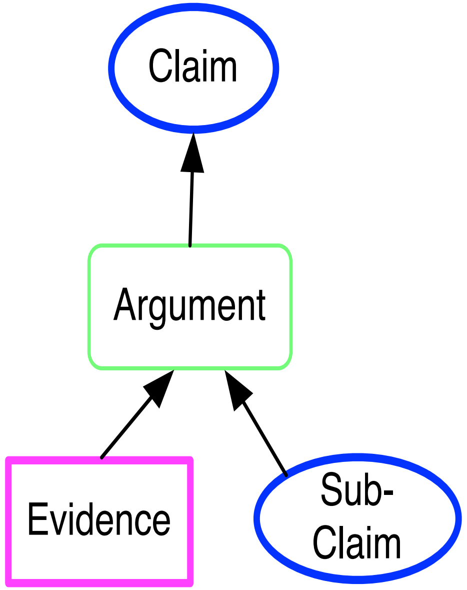


Standards and policy



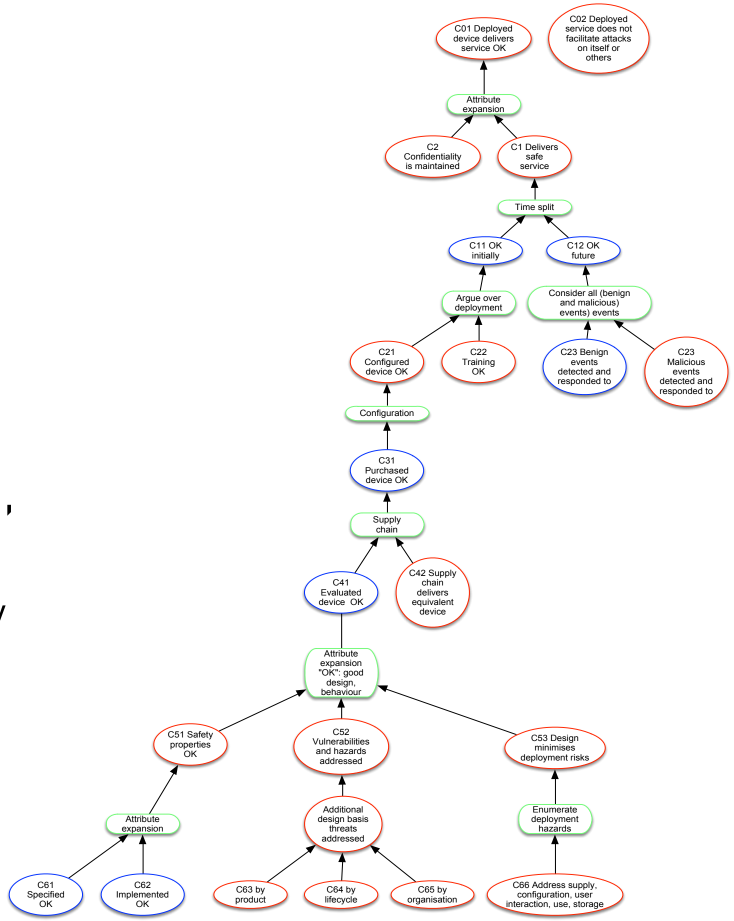
SECURITY-INFORMED ASSURANCE CASES

- Methodology
  - Express safety case about system behavior in terms of Claims-Arguments-Evidence
  - Review how the claims might be impacted by security
  - Review security controls to see if these can be used to provide an argument and evidence for satisfying the claim
  - Review impact of deploying controls on architecture and implementation
- Iterative layered approach informed by strategy triangle
  - Properties, standards, vulnerabilities



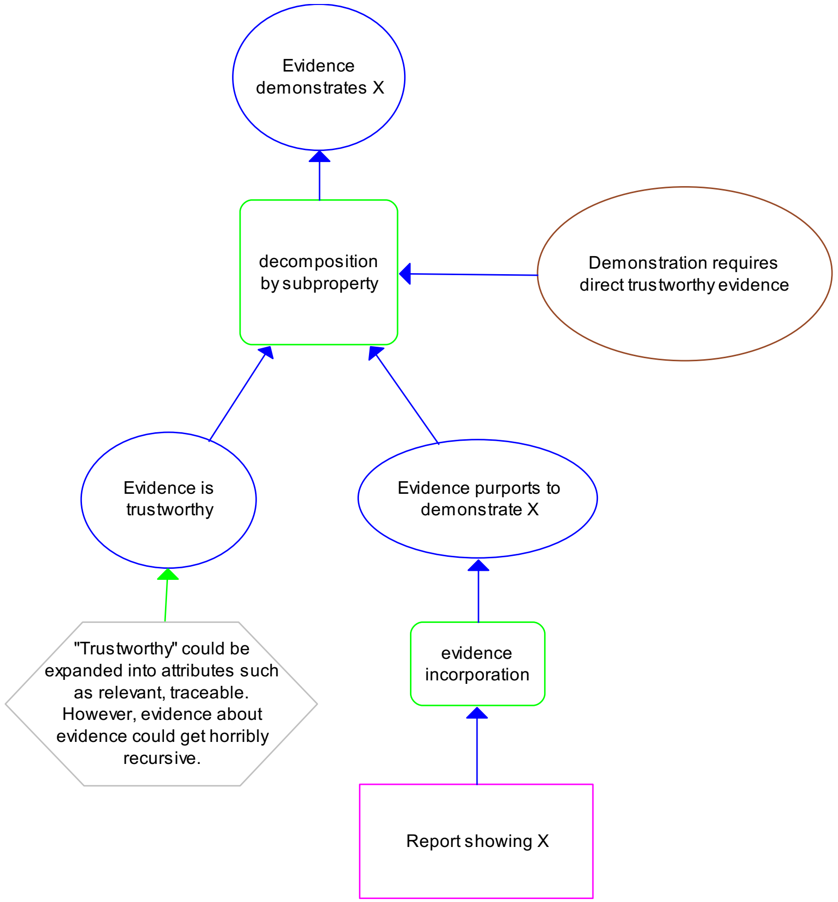
IMPACT OF SECURITY ON ASSURANCE CASE

- Some observations:
  - Integration of requirements
  - Possible exploitation of the device/service to attack itself or others
    - Failstop, role of CIA
  - Malicious events post deployment
  - Supply chain integrity
  - Design changes to address user interactions, training, configuration, vulnerabilities
  - Additional functional requirements - security controls
  - Reduced lifetime of installed equipment
- With supporting process and analysis techniques


C01 Deployed device delivers service OK
C02 Deployed service does not facilitate attacks on itself or others
Attribute expansion
C2 Confidentiality is maintained
C1 Delivers safe service
Time split
C11 OK initially
C12 OK future
Argue over deployment
Consider all (benign and malicious) events) events
C21 Configured device OK
C22 Training OK
C23 Benign events detected and responded to
C23 Malicious events detected and responded to
Configuration
C31 Purchased device OK
Supply chain
C41 Evaluated device OK
C42 Supply chain delivers equivalent device
Attribute expansion "OK": good design, behaviour
C51 Safety properties OK
C52 Vulnerabilities and hazards addressed
C53 Design minimises deployment risks
Attribute expansion
Additional design basis threats addressed
Enumerate deployment hazards
C61 Specified OK
C62 Implemented OK
C63 by product
C64 by lifecycle
C65 by organisation
C66 Address supply, configuration, user interaction, use, storage

EXPLICIT DISCUSSION OF TRUSTWORTHINESS OF EVIDENCE

- Changing the threat assumptions impact how we address evidence that is fundamental to the safety case.
- Need an explicit claim that the evidence is trustworthy and we may need to factor this by the different organisations that provide it.
  - risks from the deliberate tampering with evidence
  - non-reporting or falsification of findings
- Safety standards already require the trustworthiness of tools to be justified,
  - inclusion of security concerns means that the different threats become credible e.g. malicious inclusion of code by tools needs consideration.


Evidence demonstrates X
decomposition by subproperty
Demonstration requires direct trustworthy evidence
Evidence is trustworthy
Evidence purports to demonstrate X
"Trustworthy" could be expanded into attributes such as relevant, traceable. However, evidence about evidence could get horribly recursive.
evidence incorporation
Report showing X

ERTMS-BASED RAILWAY SYSTEMS

Systems of systems

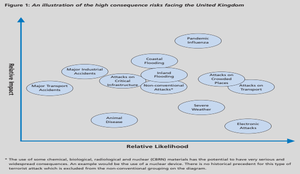
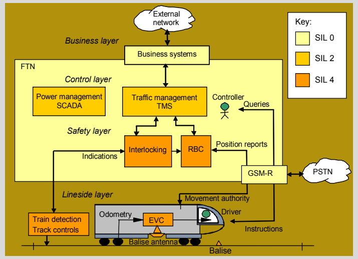


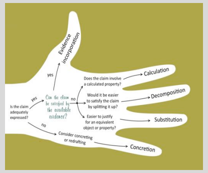
Figure 1: *An illustration of the high consequence risks facing the United Kingdom*

* The use of some chemical, biological, radiological and nuclear (CBRN) materials has the potential to have very serious and widespread consequences. An example would be the use of a nuclear device. There is no historical precedent for this type of terrorist attack which is excluded from the non-conventional grouping on the diagram.

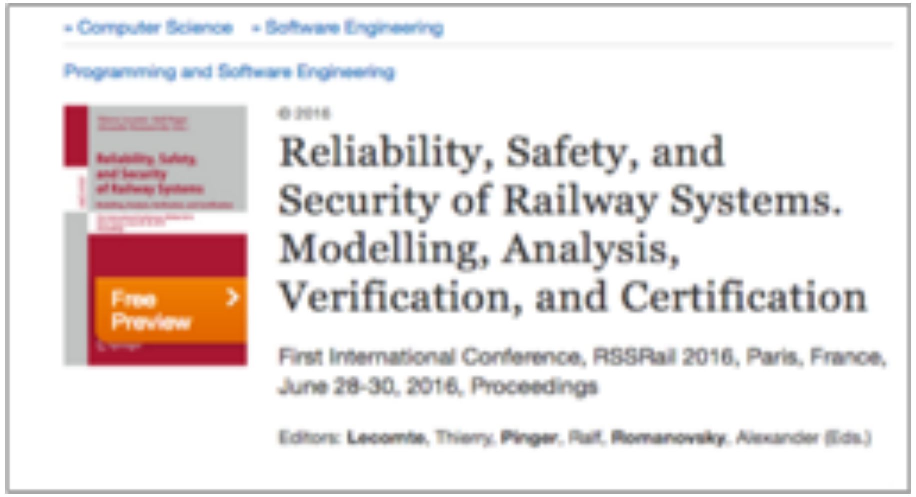
Risk assessment



Training



Evidence incorporation
yes
Does the claim involve a calculated property?
Calculation
Is the claim adequately expressed?
yes
Can the claim be satisfied by the available evidence?
no
Would it be easier to satisfy the claim by splitting it up?
Decomposition
Easier to justify for an equivalent object or property?
Substitution
no
Consider concreting or redrafting
Concretion



› Computer Science › Software Engineering

Programming and Software Engineering

© 2016

Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification

First International Conference, RSSRail 2016, Paris, France, June 28-30, 2016, Proceedings

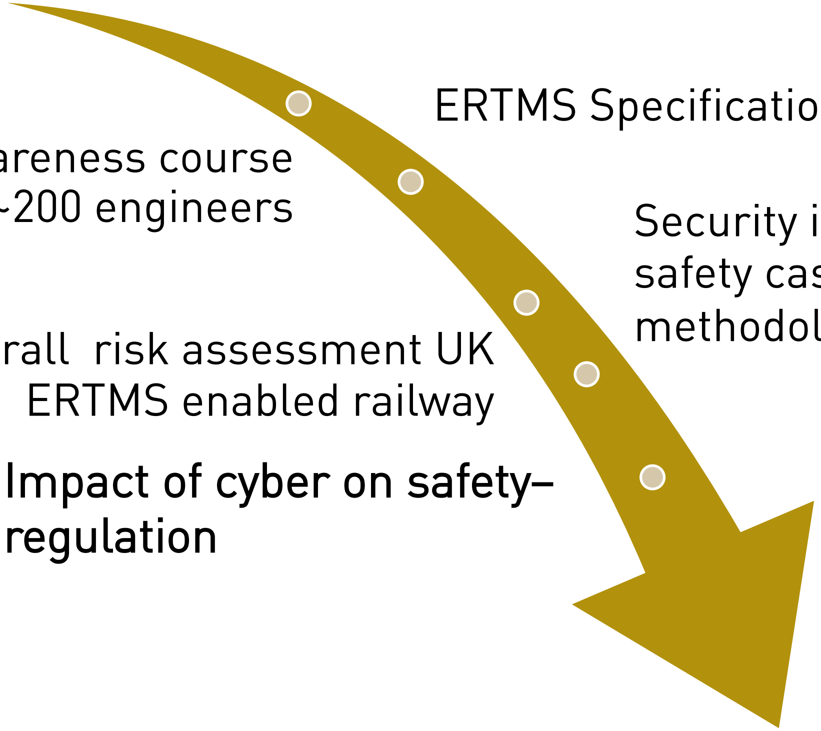
Editors: Lecomte, Thierry, Pinger, Ralf, Romanovsky, Alexander (Eds.)

Bloomfield, R. E., Bendele, M., Bishop, P. G., Stroud, R. & Tonks, S. (2016). The risk assessment of ERTMS-based railway systems from a cyber security perspective: Methodology and lessons learned. Paper presented at the First International Conference, RSSRail 2016, 28-30 Jun 2016, Paris, France.

LESSONS LEARNED

1. Start security considerations as early in the lifecycle as possible.
2. Early on, assess the implications of security for the project - low safety criticality can have high security.
3. Define the security and safety engineering and assurance processes and their interaction.
4. Integrate security into safety analysis (e.g., by performing a security-informed Hazop).
5. Develop, validate and update the hazard analysis in light of penetration testing.
6. Require evidence for the service providers' non-functional requirements (integrity, availability) rather than just relying on SLAs.
7. Provide greater emphasis on resilience and incident recovery.
8. Maintain a "living" safety case. Address changes to threats and strengths of security controls.
9. Be aware of the need for security controls in addition to safety controls in end-users and service providers.

Security, resilience and safety



Security and safety

Awareness course
~200 engineers

ERTMS Specification analysis

Security informed
safety case
methodology

Overall risk assessment UK
ERTMS enabled railway

Specific train ETCS
assessments

**Impact of cyber on safety–
regulation**

Impact on automotive

Security, resilience and
safety

FROM VISION TO OBJECTIVES

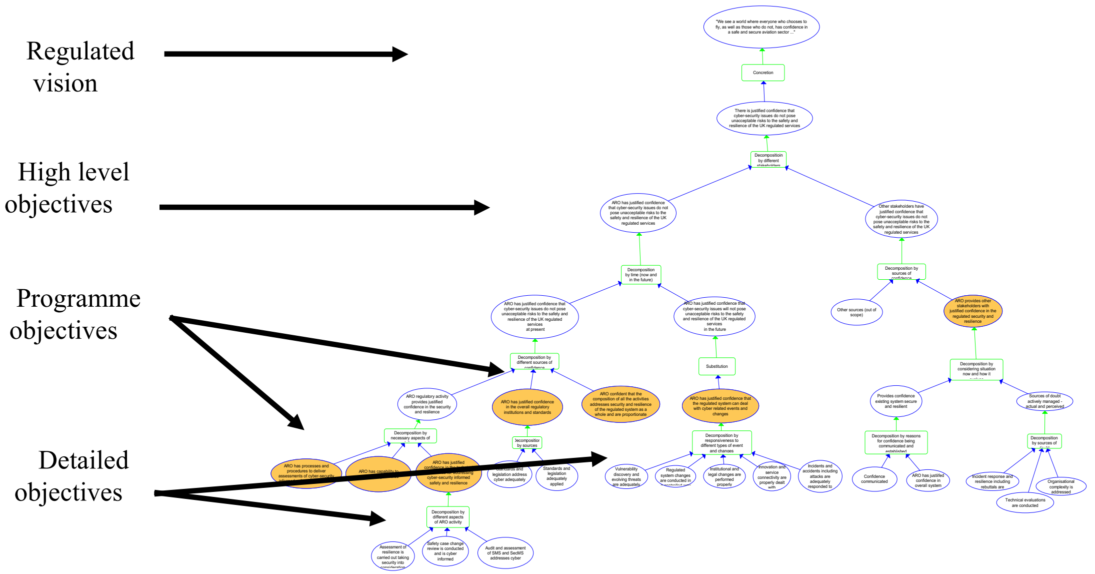
Goal

- *"We see a world where there is justified confidence that (cyber) security issues do not pose unacceptable risks to the safety and resilience of…"*

Consider this from the viewpoint of different stakeholders,

- *the ARO has justified confidence in its products*
- *the ARO provides other stakeholders with justified confidence*

This second point is unusual - example of the "good citizen" principles



Regulated vision

High level objectives

Programme objectives

Detailed objectives

"We see a world where everyone who chooses to fly, as well as those who do not, has confidence in a safe and secure aviation sector ..."
Concretion
There is justified confidence that cyber-security issues do not pose unacceptable risks to the safety and resilience of the UK regulated services
Decompositioin by different stakeholders
ARO has justified confidence that cyber-security issues do not pose unacceptable risks to the safety and resilience of the UK regulated services
Other stakeholders have justified confidence that cyber-security issues do not pose unacceptable risks to the safety and resilience of the UK regulated services
Decomposition by time (now and in the future)
Decomposition by sources of confidence
ARO has justified confidence that cyber-security issues do not pose unacceptable risks to the safety and resilience of the UK regulated services at present
ARO has justified confidence that cyber-security issues will not pose unacceptable risks to the safety and resilience of the UK regulated services in the future
Other sources (out of scope)
ARO provides other stakeholders with justified confidence in the regulated security and resilience
Decomposition by different sources of confidence
Substitution
Decomposition by considering situation now and how it evolves
ARO regulatory activity provides justified confidence in the security and reslience
ARO has justified confidence in the overall regulatory institutions and standards
ARO confident that the composition of all the activities addresses security and resilience of the regulated system as a whole and are proportionate
ARO has justified confidence that the regulated system can deal with cyber related events and changes
Provides confidence existing system secure and resilient
Sources of doubt actively managed - actual and perceived
Decomposition by necessary aspects of
Decomposition by sources
Decomposition by responsiveness to different types of event and changes
Decomposition by reasons for confidence being communicated and established
Decomposition by sources of doubt
ARO has processes and procedures to deliver assessments of cyber-security
ARO has capability to
ARO has justified confidence in the
cyber-security informed safety and resilience
Standards and legislation address cyber adequately
Standards and legislation adequately applied
Vulnerability discovery and evolving threats are adequately
Regulated system changes are conducted in
Institutional and legal changes are performed properly
Innovation and service connectivity are properly dealt with
Incidents and accidents including attacks are adequately responded to
Confidence communicated
ARO has justifed confidence in overall system
Incident response and resilience including rebuttals are
Organisational complexity is addressed
Technical evaluations are conducted
Decomposition by different aspects of ARO activity
Assessment of resilience is carried out taking security into consideration
Safety case change review is conducted and is cyber informed
Audit and assessment of SMS and SecMS addresses cyber

IMPACT ON REGULATOR

A CAE-based analysis led to a structured set of objectives for the Cyber Strategy

To support the ARO provided an analysis of some of the challenges :

- cyber-informed safety assurance
- resilience
- vulnerabilities
- systemic risks and interdependencies
- awareness, training and education
- incident response and organisational learning

From this we developed

- recommendations to address these issues, and related them to the programme objectives.
- a preliminary regulatory maturity model to explain and structure the programme of work and to put into context the challenge: achieving these seven objectives.
- programme objectives with links to levels of our maturity model to define an indicative high-level plan.

Bloomfield, R. E., Bishop, P. G., Butler, E. and Netkachova, K. (2017). Using an assurance case framework to develop security strategy and policies. Lecture Notes in Computer Science, 10489, pp. 27-38. doi: 10.1007/978-3-319-66284-8_3T

ROYAL
ACADEMY OF
ENGINEERING

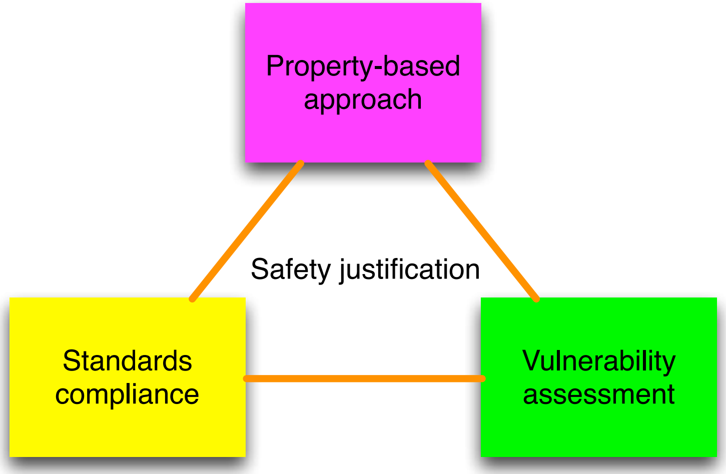
Cyber safety and resilience

strengthening the digital systems that support the modern economy

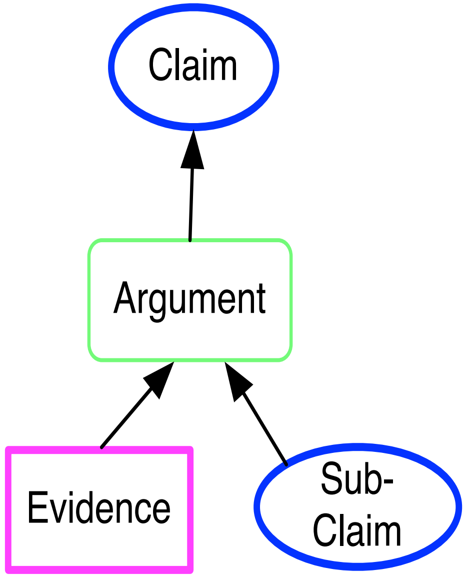
CURRENT PROJECTS

SECURITY INFORMED SAFETY CASES – COMMUNICATION AND REASONING

- Safety justification triangle



- CAE framework
  - Concepts
  - CAE Blocks
  - Guidance

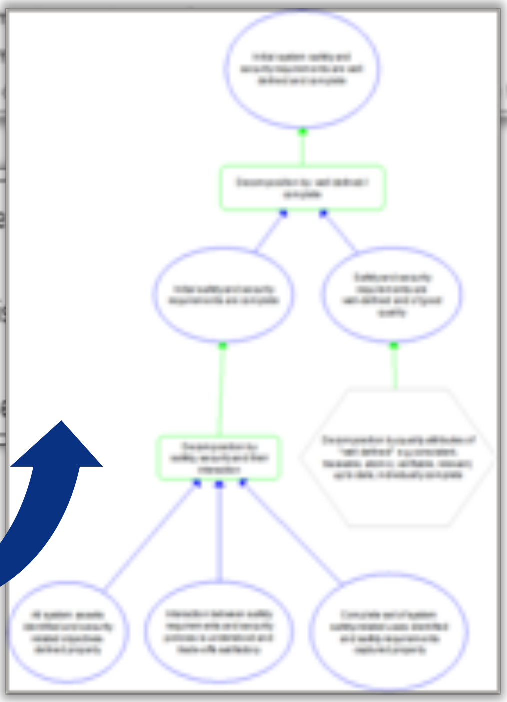


7 STEPS – SECURITY INFORMED SAFETY CASES

Case study	Risk assessment	Development lifecycle	Assur artefa
Phase 1	Step 1 – Establish system context and scope of assessment	Requirements and specification	Re and Assur case
	Step 2 – Configure risk assessme		
	Step 3 – Analyse policies and requirements		
Phase 2	Step 4 – Preliminary risk analysis		
	Step 5 – Identify specific attack scenarios		
	Step 6 – Focused risk analysis		
	Step 7 – Finalise risk assessment		

Policy issue	Activities
Risk, responsibility and regulation	Add explicit threat models and scenarios to environment description. Define capability levels of attackers and design basis threats. Introduce policy on design basis threats, not just in operational environment but in development infrastructure, organisation and supply chain. Make risk and safety statement conditional on these assumptions, discuss with regulators and overall duty holders. Agree how to demonstrate that the risks are ALARP with respect to security-initiated events. This may be problematic. Recognise that a duty-holder cannot outsource risk to a cyber department or through SLAs (although specialist advice will be needed). The holder still has a responsibility to understand safety hazards and mitigations. Augm Augm Map for them.

Step 3 – Analyse policies and requirements	Undertake an analysis of policy issues considering inte safety requirements and security policies. Resolve any conflicts, show that the trade-offs are satis document the decisions made. Document the requirements and policy assurance case



SECURITY AND SAFETY - CODE OF PRACTICE AND PAS

What we are doing:

- Developed a fast track British Standard (PAS Code of Practice) on automotive eco-system security and safety
- Developing a Code of Practice for railways security informed safety
- Sponsored by the UK CPNI with close involvement of industry
- Principle based approach in keeping with UK outcome focused regulation

TOP-LEVEL PRINCIPLES (COMMON)

Security policy, organization and culture

Security-aware lifecycle

Maintaining effective defences

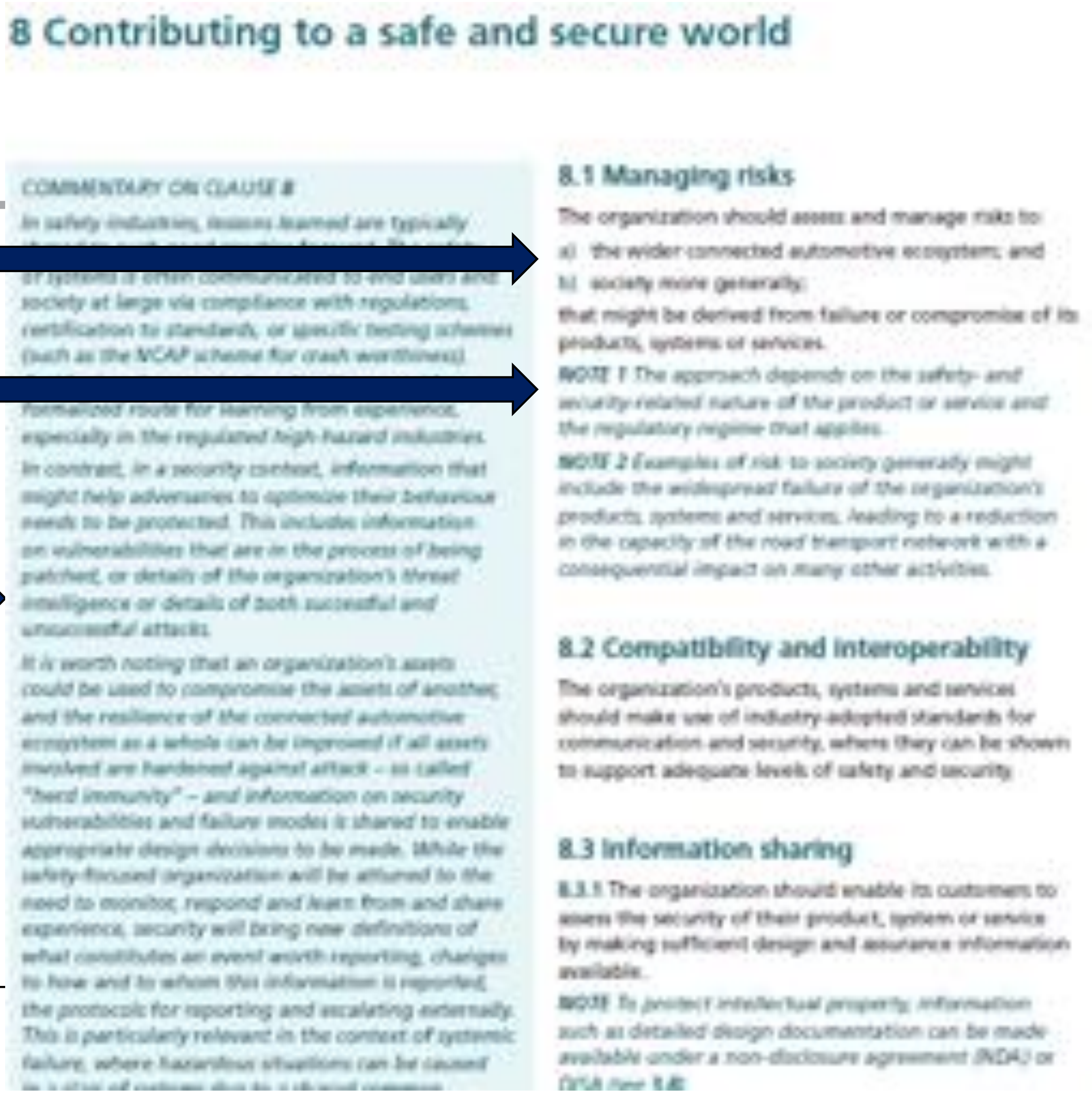
Incident management

Secure and safe design

Contributing to a safe and secure world

“GOOD CITIZEN” PRINCIPLE

- Detailed recommendations (automotive guidance)
- Explanatory notes
- Supporting rationale



8 Contributing to a safe and secure world

COMMENTARY ON CLAUSE 8

In safety industries, lessons learned are typically [illegible] *of systems is often communicated to end users and society at large via compliance with regulations, certification to standards, or specific testing schemes (such as the NCAP scheme for crash worthiness).* [illegible] *formalized route for learning from experience, especially in the regulated high-hazard industries.*

In contrast, in a security context, information that might help adversaries to optimize their behaviour needs to be protected. This includes information on vulnerabilities that are in the process of being patched, or details of the organization's threat intelligence or details of both successful and unsuccessful attacks.

It is worth noting that an organization's assets could be used to compromise the assets of another, and the resilience of the connected automotive ecosystem as a whole can be improved if all assets involved are hardened against attack – so called "herd immunity" – and information on security vulnerabilities and failure modes is shared to enable appropriate design decisions to be made. While the safety-focused organization will be attuned to the need to monitor, respond and learn from and share experience, security will bring new definitions of what constitutes an event worth reporting, changes to how and to whom this information is reported, the protocols for reporting and escalating externally. This is particularly relevant in the context of systemic failure, where hazardous situations can be caused [illegible]

8.1 Managing risks

The organization should assess and manage risks to:

a) the wider connected automotive ecosystem; and

b) society more generally;

that might be derived from failure or compromise of its products, systems or services.

NOTE 1 *The approach depends on the safety- and security-related nature of the product or service and the regulatory regime that applies.*

NOTE 2 *Examples of risk to society generally might include the widespread failure of the organization's products, systems and services, leading to a reduction in the capacity of the road transport network with a consequential impact on many other activities.*

8.2 Compatibility and interoperability

The organization's products, systems and services should make use of industry-adopted standards for communication and security, where they can be shown to support adequate levels of safety and security.

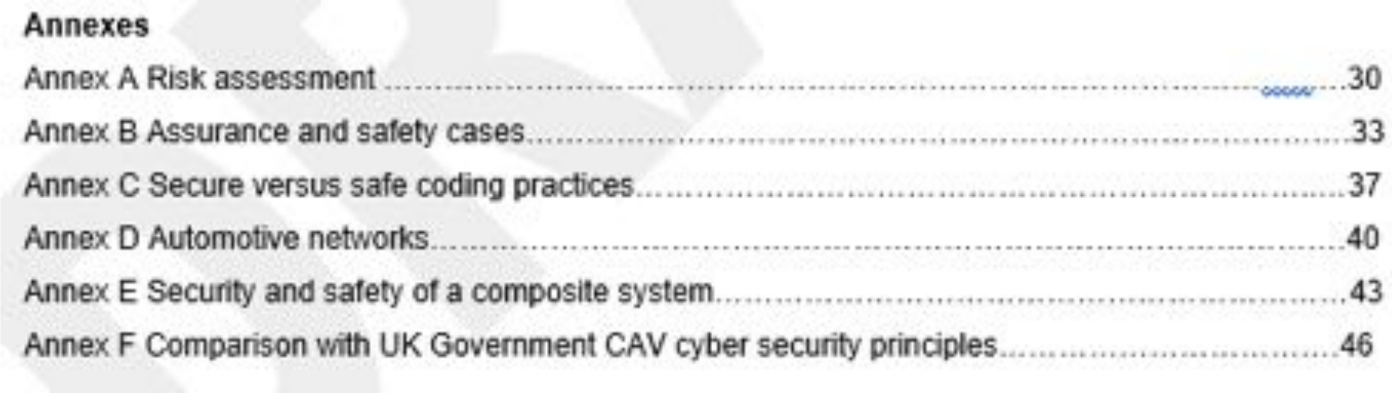
8.3 Information sharing

8.3.1 The organization should enable its customers to assess the security of their product, system or service by making sufficient design and assurance information available.

NOTE *To protect intellectual property, information such as detailed design documentation can be made available under a non-disclosure agreement (NDA) or* [illegible]

© 2017 ADELARD LLP

SUPPORTING ANNEXES



Annexes

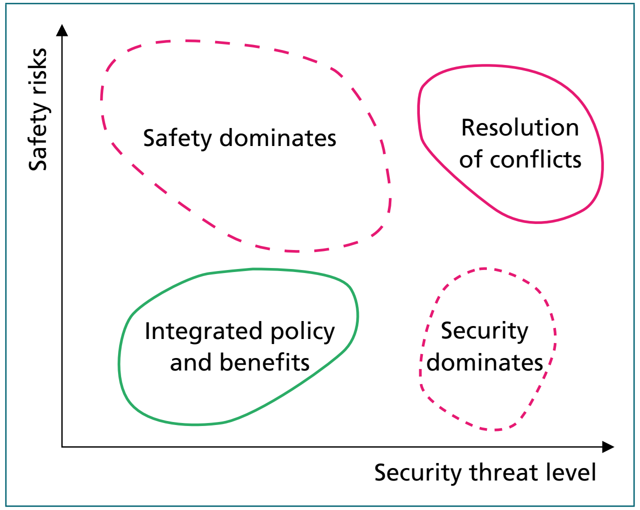
- Examples from the Rail CoP
- The annexes are informative and are designed to support the recommendations in the main body of the CoP

Appendix E Interactions between safety and security

E.1 Introduction

This CoP deals with many different aspects of considering security in the context of the safety of an integrated rail system. One of the most challenging areas is where safety and security interact, particularly in cases where their aims contradict or where there are unintended consequences. Interactions can stem from

- overlapping requirements
- overlapp
- the use c
- informat
- misuse o



In general, t to make decisions
that could r ould result in direct
conflicts bet e, consider an access
system that t an attacker cannot
gain access, fire. The interactions
between a s any trade-offs
identified. I essential to consider
the trade-of

For safety, t the required
functionalit ecurity perspective is
included, co nded measures to
protect the identify
vulnerabiliti ope of the CoP, but
there might ck, or where the
disclosure of sensitive data leads to non-physical harm.

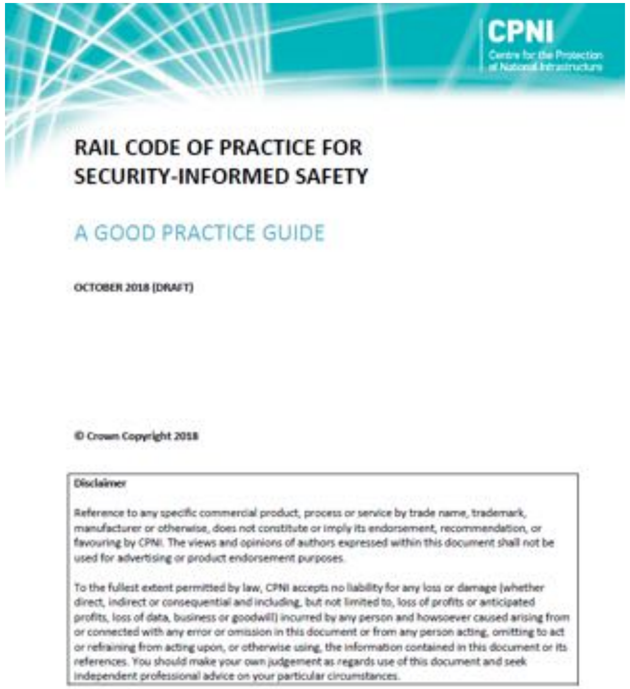
Figure 6, which is taken and generalized from [1], shows four different scenarios where security and safety interact:

- **bottom left corner** – this is an area of maximum operational benefit, where there are low levels of threat and no significant safety challenge, so it is relatively straightforward to satisfy both aspects.
- **bottom right corner** – this is an area where security concerns might dominate due to the threat level, for example, a need to restrict access to the device. In this case, the safety analysis must

AVAILABILITY

- Rail
  - Draft for industry consultation
  - Currently under review
  - Plan to release guidance Q1 2019

- Automotive
  - BSI publication December 2018
  - BSI PAS 11281



CPNI
Centre for the Protection of National Infrastructure

RAIL CODE OF PRACTICE FOR SECURITY-INFORMED SAFETY

A GOOD PRACTICE GUIDE

OCTOBER 2018 (DRAFT)

© Crown Copyright 2018

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

PAS 11281:2018

Connected automotive ecosystems – Impact of security on safety – Code of practice

CPNI.
Centre for the Protection of National Infrastructure

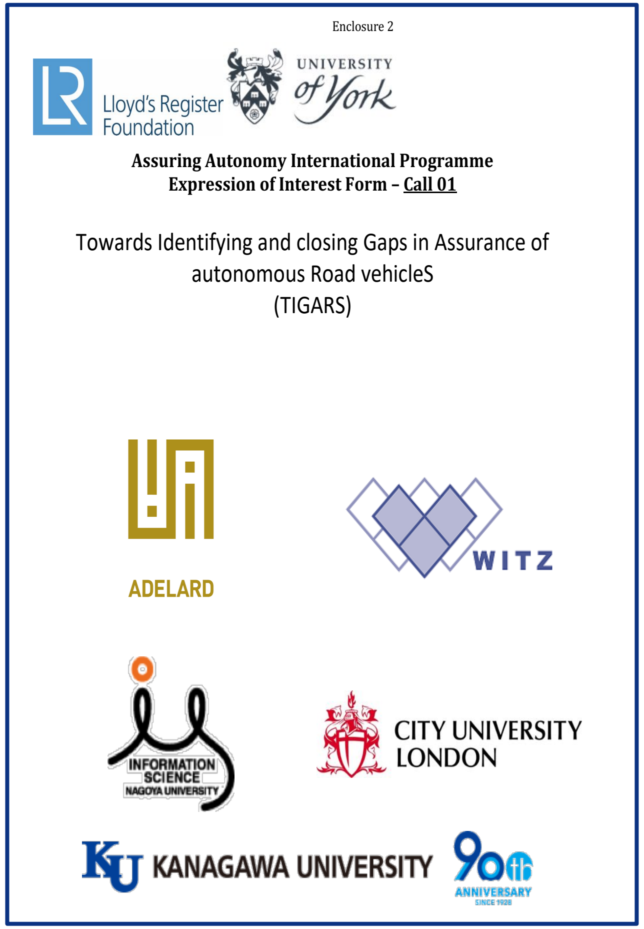
bsi.

RESEARCH PROJECTS

“Towards Identifying and closing Gaps in Assurance of autonomous Road vehicleS”

(TIGARS)

ASSURED AUTONOMY



Enclosure 2

Lloyd's Register Foundation
UNIVERSITY of York

Assuring Autonomy International Programme
Expression of Interest Form – Call 01

Towards Identifying and closing Gaps in Assurance of autonomous Road vehicleS
(TIGARS)

ADELARD
WITZ
INFORMATION SCIENCE NAGOYA UNIVERSITY
CITY UNIVERSITY LONDON
KU KANAGAWA UNIVERSITY
90th ANNIVERSARY SINCE 1928

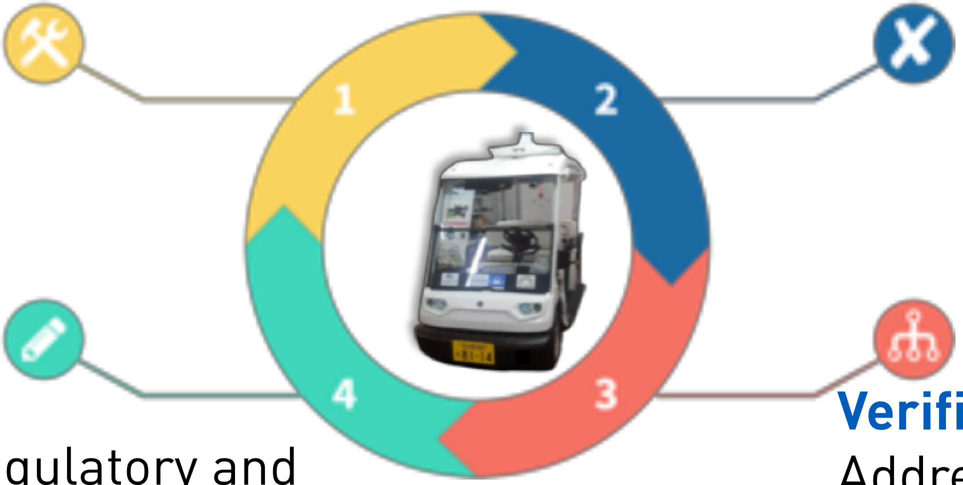
Tigars - Aims & Challenges

Engineering Practices

Identify current autonomous systems engineering approaches and assess the current state of software engineering development practice.

Assurance Gaps

Assess the feasibility of deploying current state-of-the-art static analysis, verification, and testing techniques.



Standards & Policies

Recommendations to regulatory and policy organisations

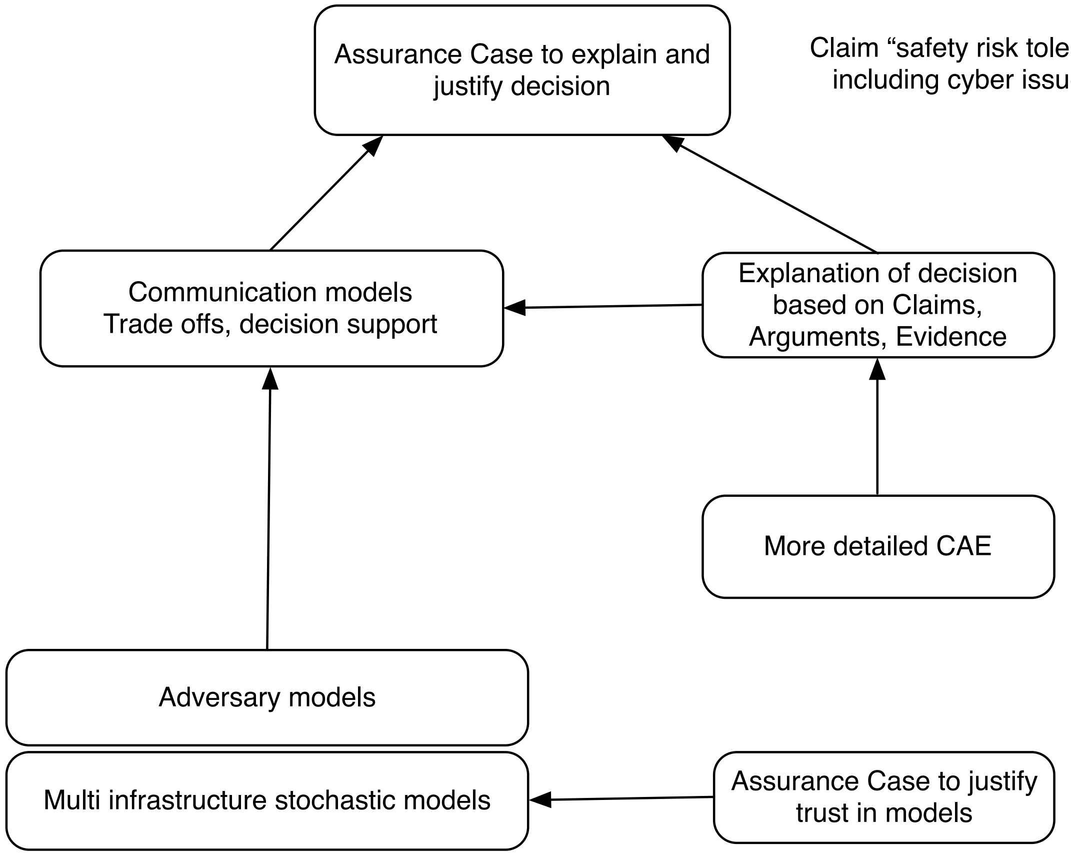
- principles-based framework to address autonomy
- near-term interpretation of existing standards.

Verification & Validation

Address assurance gaps with new approaches

- static analysis of machine learning,
- simulation and test strategies
- defence in depth.

OVERVIEW



Assurance Case to explain and justify decision

Communication models
Trade offs, decision support

Explanation of decision based on Claims, Arguments, Evidence

More detailed CAE

Adversary models

Multi infrastructure stochastic models

Assurance Case to justify trust in models

Claim “safety risk tolerable including cyber issues”

PIA FARA

RITICS ROADMAPPING – SHORT TERM

- With Dr Peter Popov
- Landscape and road mapping
  - Identify issues with practitioners
    - Transport, Nuclear,
    - Resilience community
  - Develop issues
    - Breadth and selective depth
  - Combine
    - Technology and threat awareness
  - Develop short R&D roadmap
- Help and interest welcome!

- Structure of issues from
  - RAEng Cyber Safety + PAS + IAEA
  - Autonomy from Tigars and AAIP
  - Resilienceshift (Arup) and NIC

DISCUSSION – THE YES BUT…

WHY IT MIGHT BE EASIER THAN FEARED

- Success of dependability engineering
  - Automotive engineering
  - Air and rail transportation
  - Finance system
  - Nuclear power
  - Consumer products

Succeed through initial high quality, fault tolerance, failure management and recovery

Already address

- Safety cases and myriad sources of risk
- Competency and culture
- Incident response and organisational learning
- Updates to system and recertification
- Defence in depth and systemic risk
- Supply chains already managed
- Dependability built in

BUT ACHIEVING DEPENDABLE SYSTEMS IS HARD

- Automotive engineering
  - Yet Toyota, VW
- Air and rail transportation
  - Yet Spanish crash, Nimrod
- Finance system
  - Yet crashes, $400M bug
- Nuclear power
  - Yet Fukushima, QA fraud
- Consumer products
  - Yet recalls and data loss
- Medical systems
  - Yet avoidable deaths

"Normal business", achieving dependable conventional digital systems is hard

DISCUSSION – THE YES BUT…

- The impact of security on safety now *known* in general and have techniques for identifying this and detailing it further:
  - Security policy, organization and culture
  - Security-aware lifecycle
  - Maintaining effective defences
  - Incident management
  - Secure and safe design
  - Contributing to a safe and secure world
- Known and very significant impact

YES BUT…

- Security will have a major impact on all aspects of organisation, governance, requirements, architecture, development, assurance
  - Management of institutional and regulatory change
  - Legacy and long lived systems
  - Systems engineering and systems thinking
  - Technologies and architectures
  - Assurance strategies
- Security, like quality, intrinsic to everything – need to address security mindedness
- Political, social and threat context is changing
- Technology and systems are changing
  - AI,ML, IoT

CONCLUSIONS

- Security will impact on all aspects of organisation, governance, requirements, architecture, development, assurance
  - Security policy, organization and culture
  - Security-aware lifecycle
  - Maintaining effective defences
  - Incident management
  - Secure and safe design
  - Contributing to a safe and secure world
- "Normal business" achieving dependable conventional digital systems is hard

- A way forward
  - Industry implement objectives of PAS
  - Government and NGO address RAEng and social policy issues
  - Research needed to support this
- Awareness of
  - Political, social and threat context is changing
  - Technology and systems are changing
  - Need for holistic approach
- Provides opportunities not just problems
- Innovate and integrate!!

FURTHER READING

CYBERTRUST

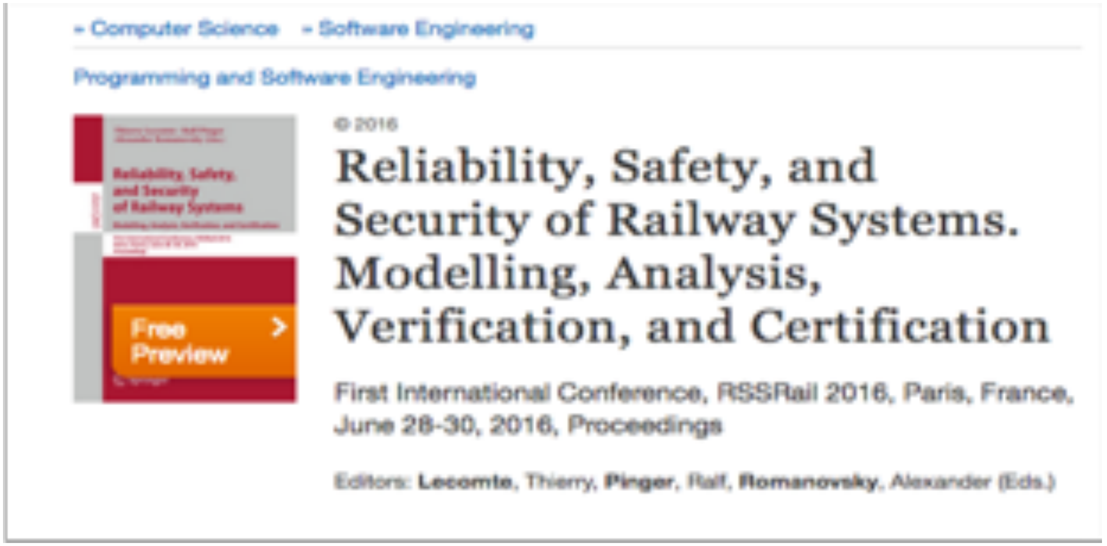
Security-Informed Safety

Kate Netkachova and Robin E. Bloomfield, Adelard LLP and City University London

For safety-critical systems, if it isn't secure, it isn't safe.

which a system malfunction could lead to accidents with marginal or negligible severity, to high criticality, in which a system failure or malfunction could result in death and

IEEE Computer June 2016



› Computer Science › Software Engineering

Programming and Software Engineering

© 2016

Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification

First International Conference, RSSRail 2016, Paris, France, June 28-30, 2016, Proceedings

Editors: **Lecomte**, Thierry, **Pinger**, Ralf, **Romanovsky**, Alexander (Eds.)

Bloomfield, R. E., Bendele, M., Bishop, P. G., Stroud, R. & Tonks, S. (2016). The risk assessment of ERTMS-based railway systems from a cyber security perspective: Methodology and lessons learned. Paper presented at the First International Conference, RSSRail 2016, 28-30 Jun 2016, Paris, France.

ADELARD