CPNI

Centre for the Protection of National Infrastructure

RAIL CODE OF PRACTICE FOR SECURITY-INFORMED SAFETY

A guide to good practice

CONTENTS

OVERVIEW

The document comprises a Code of Practice (CoP) for security-informed safety in the rail sector and provides guidance on security issues for railway safety engineers and managers. It is outcome-focused and intended to help all organisations in the rail ecosystem ensure that security threats to their products, services or activities do not pose unacceptable risks to the safety of rail users and wider society.

The CoP considers interactions between safety and security and provides guidance on how to resolve conflicts between them. Security concerns that are not directly safety-related, such as confidentiality, privacy and theft, fall outside the scope of the CoP. Other risks to the railway system, for example, financial or reputational risks, are also considered to be out of scope.

The code applies to risks that can affect a single system or a few systems and gives recommendations for managing systemic risks – wider risks which might appear small, but which become more significant when interdependencies are considered and where the failure of a single or a few entities could result in more widespread failure.

The CoP covers the entire rail ecosystem, including light rail as well as heavy rail, and is intended to be used by suppliers, duty holders, and maintainers of systems used in a connected railway system. Specifically, it is applicable to organisations that are responsible for commissioning, designing, supplying, operating or maintaining systems and services that support the proper operation of rail transport, including systems for railway signalling, traffic management, rail communications, timetabling, passenger information, operation and maintenance. This includes manufacturers and suppliers of railway equipment or services, rolling stock owners, train operators, rail infrastructure providers, maintenance organisations, and digital service providers. It recognises that everyone in the ecosystem has a role to play.

Although this CoP is primarily concerned with cyber security, it also considers physical security and personnel security because the best way to provide effective security is to use a combination of security measures from all three disciplines.

The document is organised as a set of recommendations grouped into six sections:

SECTION 1
The impact of security considerations on safety policy and organisational culture

SECTION 2
A high-level overview of security requirements throughout the system lifecycle

SECTION 3
Detailed guidance on ensuring that security is maintained during operation

SECTION 4
Detailed guidance on managing security incidents

SECTION 5
Detailed guidance on building security into the design of the system

SECTION 6
Cooperation and collaboration with other organisations to improve the security of the rail ecosystem

OVERVIEW

The appendices provide detailed technical guidance on specific topics such as risk assessment, assurance cases, network security, and secure coding guidelines, concluding with an analysis of the relationship between the CoP and other rail industry guidance.

GUIDANCE FOR READERS

The CoP is primarily aimed at people with a safety background who need to know how security issues impact on their existing safety practice, but it might also be of use to people with a security background who need to know something about how the rail industry manages safety.

Readers who are not familiar with how the rail industry manages safety may find it helpful to read 'Taking Safe Decisions' [12], a Rail Safety and Standards Board (RSSB) guidance document that explains how Britain's railways take decisions that affect safety. Readers with a railway background who are not familiar with cyber security may find the Department for Transport (DfT) guidance on Rail Cyber Security [2] helpful as a starting point.

The CoP builds on both of these documents by suggesting a set of principles and specific actions for security-informed safety that conform to best practice and address the requirements of the DfT guidance on Rail Cyber Security, while complying with the RSSB guidance on "Taking Safe Decisions".

Each railway stakeholder in the rail ecosystem will have their own perspective on the CoP and will find some sections more relevant than others. Detailed guidance for the intended readership can be found in Appendix H, which identifies a broad set of individual and organisational roles that are representative of various stakeholders in the railway industry and suggests which sections of the CoP might be most relevant. The roles are intended to be illustrative and the guidance is indicative rather than definitive. In practice, individuals and organisations should take the relevant guidance from the CoP and adapt it to their circumstances.

USE OF THIS DOCUMENT

This CoP takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this CoP is expected to be able to justify any course of action that deviates from its recommendations.

It has been assumed in the preparation of this CoP that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a code of practice cannot confer immunity from legal obligations.

OVERVIEW

ACKNOWLEDGEMENTS

Acknowledgement is given to the technical authors, Robin Bloomfield, Eoin Butler, Peter Bishop and Robert Stroud of Adelard (now part of NCC Group), and to the following organisations that were involved in the development of the CoP as reviewers:

- Alstom Group
- DB Cargo (UK) Ltd
- Department for Transport
- National Cyber Security Centre (NCSC)
- Network Rail
- Rail Safety and Standards Board (RSSB)
- Ricardo Rail
- Siemens Rail
- Transport for London

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this CoP.

INTRODUCTION

RAILWAY SAFETY AND SECURITY

Under UK domestic law, rail operators are obliged to protect the safety of their operations. In this context, 'rail operators' has a specific meaning, as defined by the Railways and Other Guided Transport Systems (Safety) Regulations (ROGS) [1], which applies to:

- transport undertakings
- infrastructure managers
- maintenance organisations

ROGS requires all rail operators to establish safety management systems and put in place a change management process to identify and control new risks. Mainline rail operators are required to follow the Common Safety Method for Risk Evaluation and Assessment [5]; changes to non-mainline railway systems need to go through a safety verification process if they could create significant new or different safety risks. There is also a Common Safety Method for Monitoring [6] that requires rail operators to monitor the effectiveness of their safety management system and risk control measures.

Although ROGS is concerned with safety rather than security, a security vulnerability could result in a safety hazard. This is recognised by the DfT guidance on rail cyber security [2], which explains that claims about safety must be informed by security considerations and that failure to make systems secure might contravene regulatory safety requirements.

In practice, although rail suppliers fall outside the scope of ROGS, it is not possible for a rail operator to guarantee the safety of their operations without assurance from their suppliers. For this reason, the CoP is intended to be applicable to both rail operators and rail suppliers, in other words, people and organisations that supply equipment or services to rail operators.

SECURITY-INFORMED SAFETY

'Security-informed safety' is the term used to describe the inclusion of security considerations when managing safety risks. There is a growing realisation that security and safety are closely interconnected: it is no longer acceptable to assume that a safety system is immune from attack because it is built using bespoke hardware and software, or because it is separated from the outside world by an 'air gap'. A safety justification, or safety case, is incomplete and unconvincing without a consideration of security issues. IET have published a code of practice on cyber security and safety [7], which observes that

"Historically, it has been acceptable for safety assurance documents to make assumptions about security or exclude security from their scope. It is increasingly recognised that security has to be considered and justified in a more integrated manner."

The latest editions of safety standards such as EN 61508 [8] and EN 50129 [3] require security threats to be considered during hazard and risk analysis, and details of specific security measures to be included in the safety case.

INTRODUCTION

For example, EN 61508-1:2010 [8] requires *'malevolent and unauthorised actions to be considered during hazard and risk analysis'* (clause 1.2k) and states that the safety manual should include *'details of any security measures that may have been implemented against listed threats and vulnerabilities'* (clause D.2.4m). References are provided to other ISO/IEC standards that address this subject in depth, including ISO/IEC TR 19791 [9] and the IEC 62443 series [10].

Similarly, EN 50129:2018 [3] requires the safety case to describe how the system has been protected from unauthorised access. In particular, the safety case should describe how *'IT security threats that have the potential to have the potential to affect safety-related functions have been evaluated and how protection against them has been achieved'.*

More generally, PD CLC/TS 50701:2021 [4], a new cybersecurity standard for railway cybersecurity, *'aims to ensure that the RAMS characteristics of railway systems / subsystems / equipment cannot be reduced, lost or compromised in the case of intentional attacks'.*

The CoP is intended to support the rail industry in implementing these new standards and help organisations in the rail ecosystem ensure that security threats to their products, services or activities do not pose unacceptable risks to safety.

While in many situations, security and safety measures can comfortably be integrated together, there are other cases where there may be tension or conflict between safety and security needs. In some areas, such as risk estimation, the techniques traditionally used in safety analysis may be inadequate. In addition, the pace at which threats change in the security domain requires more dynamic solutions than those that are often seen when only safety is taken into account.

More information about challenges at the intersection of safety and security can be found in the IET Code of Practice on Cyber Security and Safety [7].

01.
POLICY, ORGANISATION AND CULTURE

Organisations responsible for safety-related products or services in the rail sector will have a safety policy that describes the organisation's approach to the safety of their products, services or activities. The safety policy will typically provide a statement of the organisation's general policy on health and safety, and the quality and safety of its products and services, and will also set out the organisation's commitments to managing safety effectively.

In particular, rail operators have legal responsibilities to manage their safety risks, both on an ongoing basis and whenever a change is made to the railway system. To support this, rail suppliers are expected to provide a safety case to demonstrate that their product or service is adequately safe.

The NIS Regulations 2018 [13] require 'operators of essential services' (including some rail operators) to take 'appropriate and proportionate security measures to manage risks posed to the security of the network and information systems on which their essential service relies'.

DfT is the security regulator for the domestic railway network. Under Section 119 of the UK Railways Act 1993 the Secretary of State is empowered to give appropriate instructions regarding security for the purpose of ensuring that relevant assets within Great Britain are protected against acts of violence. These instructions can be given to any person who is the owner or operator of a relevant asset or to any person who provides railway services.

Consideration of security issues, whether in their own right or integrated with a safety policy, will necessitate significant departures from existing approaches. The impact of security threats on safety risks needs to be considered and products and services need to be engineered so that security threats and vulnerabilities are addressed throughout the lifecycle. Information about the security threats and countermeasures identified by an organisation might enable an attacker to identify residual vulnerabilities in the system, so a security-informed safety analysis needs to be handled with a greater degree of confidentiality than is customary in safety. Personnel with responsibility for overseeing safety activities might not be competent in the security area, so additional roles and responsibilities may need to be defined.

Security concerns that are not directly safety-related, such as confidentiality and privacy requirements arising from the UK General Data Protection Regulation (UK GDPR) [14], falls outside the scope of the CoP, although they could indirectly lead to safety issues (for example, theft of design documentation might enable an attack, or information on the movement of sensitive rail traffic might identify a high-value target).

Further guidance can be found in PAS 555 [15], which specifies a framework for the governance and management of cyber security risk. Detailed guidance on security policy, organisation and culture can be found in BS 10754-1:2018 [16], which deals with the governance and management of systems trustworthiness, and sets out a series of processes and controls for developing trustworthy systems.

1.1 POLICIES AND PROCESSES

1.1.1
Organisations should formulate a policy on security-informed safety that sets out their overall stance and aims with respect to ensuring that security is considered as part of their approach to managing safety risks.

1.1.2
The policy should recognise that the organisation has a responsibility to ensure that security threats do not pose unacceptable risks to safety.

1.1.3
The policy should ensure that the impact of security on safety is addressed by the organisation and its partners and suppliers, throughout all phases of the product and service lifecycle.

NOTE: The policy should cover how to manage security incidents that arise during operation. Further guidance on incident management can be found in Section 4.

1.1.4
Organisations should define and implement processes to support their policy on security-informed safety.

NOTE: In general, processes should be flexible rather than prescriptive and organisations should only prescribe particular methods if there is a sound business case for doing so.

Keeping processes flexible makes organisations more agile and able to adapt to emerging best practice. However, in some cases, there may be a compelling reason to adopt a particular method (e.g., regulatory compliance, industry standards).

01. POLICY, ORGANISATION AND CULTURE

1.1.5
Policies and processes on security-informed safety should consider technical, procedural and managerial measures for mitigating security threats.

NOTE: Security is not purely a technological problem. In order to ensure robust protection, it is important to consider procedural and managerial aspects of security as well.

1.1.6
Organisations should take steps to ensure that their policies and processes for ensuring security-informed safety are described, communicated, and implemented effectively.

NOTE: Guidance on developing policies and processes can be found in the NCSC CAF guidance [17], specifically, Objective B.1: Service protection polices and processes.

1.1.7
Organisations should have mechanisms in place to validate the implementation and effectiveness of their policies and processes for ensuring security-informed safety.

NOTE: The Common Safety Method for Monitoring [6] requires organisations to monitor the effectiveness of their safety management systems.

1.1.8
Sufficient documentary evidence should be produced to enable decisions relating to security and safety to be reviewed and justified in the future.

NOTE: An important consideration is the ability, following an incident, to justify the organisation's approach to security and safety and relevant decisions.

1.1.9
Records of decisions relating to security and safety should be preserved for a sufficient period of time to allow for the occurrence, detection and investigation of safety and security incidents.

NOTE: The retention period might be different for different types of evidence. The organisation might wish to consider the expected lifetime of its products, systems and services to inform this decision.

1.2 RESPONSIBILITY AND ACCOUNTABILITY

1.2.1
Accountability for security and safety issues that might affect the organisation's products and services should be clearly defined, and traceable to board level.

NOTE: The board can delegate responsibility for decisions about security and safety issues but must remain accountable for the organisation's overall approach to security and safety.

1.2.2
A member of the board or equivalent senior person should be responsible for defining the organisation's overall programme of work on security-informed safety.

1.2.3
A senior manager should be responsible for implementing the security-informed safety programme in the organisation.

NOTE: Responsibility for implementing particular aspects of the security-informed safety programme can be delegated to clearly identified individuals with specific job descriptions and responsibilities. Individuals can be identified by role or by name.

1.3 RISK MANAGEMENT

NOTE: This section is concerned with managing the impact of security threats on safety risks associated with the organisation's products and services. Typically, organisations consider all risks to their business, including commercial, financial and reputational risks, as well as safety and security risks, but here we focus on safety risk management, specifically the management of safety risks that result from security threats.

1.3.1
Organisations should adopt a formal, holistic, approach to identifying, assessing and managing the impact of security threats on the safety risks associated with their products and services.

NOTE: For some products and services, it may also be appropriate to consider the impact of security threats on reliability and availability, particularly in situations where the reliability or availability of the system may have safety implications.

1.3.2
The safety policy should document the organisation's overall approach to addressing the impact of security threats on safety risks, setting out its commitment to manage such risks effectively and defining responsibilities accordingly.

1.3.3
The safety policy should articulate the organisation's appetite towards safety risks caused by security threats, so that decision-makers at all levels of the organisation can make informed decisions about risk acceptance.

NOTE 1: Under the Health and Safety at Work Act [18], organisations must ensure the safety of people affected by their undertaking so far as is reasonably practicable (SFAIRP). Organisations may, voluntarily, reduce risk beyond what is legally required (e.g., for reputational reasons).

NOTE 2: Cyber attack poses a growing threat to the security and therefore the safety of critical infrastructure, including the railway networks. Rail operators have obligations under UK law to protect the safety of their operations. Failure to take reasonable care to do so may make them liable for some of the resulting losses [2].

1.3.4
The safety policy should document the organisation's approach to resolving conflicts between safety and security, which can occur at any stage of the product/service lifecycle.

1.3.5
The safety policy should require any conflicts between safety and security that are identified to be recorded, together with the decision and rationale for resolving the conflict.

NOTE: Further guidance on managing conflicts between safety and security can be found in Appendix D.

1.3.6
Organisations should identify, assess and understand the impact of any assumptions they make regarding the prevalence, capabilities and motivations of threat agents on their demonstration that risks are tolerable.

1.3.7
The risk management process should consider risks to the safety and security of products, services and activities arising from threats to physical security.

NOTE: Guidance on physical security is available from CPNI [19].

1.3.8
The risk management process should consider risks to the safety and security of products, services and activities arising from threats from people who have access to systems, including contractors and maintenance personnel, as well as the organisation's own staff.

NOTE: Guidance on personnel security is available from CPNI [20].

1.3.9
The risk management process should consider risks to the safety and security of products, services and activities arising from cyber threats.

NOTE: Guidance on cyber security is available from NCSC [21].

1.3.10
The safety case for products, services and activities should provide assurance that security threats to safety have been adequately managed.

1.4 ASSET MANAGEMENT

1.4.1
Assets that are used to deliver, maintain or support the security and safety of an organisation's products and services should be identified and recorded. The information that is recorded should include an indication of the importance of the asset to achieving safety and security.

NOTE: 'Assets' includes data, people and systems as well as any supporting infrastructure, and can be tangible or intangible.

1.4.2
This record of assets should be updated whenever such assets are added, removed or changed, and should be periodically reviewed to ensure that it remains up-to-date and relevant.

NOTE: The frequency of review may depend on the nature of the asset and how often its importance to safety and security might be expected to change.

01.
POLICY, ORGANISATION AND CULTURE

1.5 LEGACY SYSTEMS

1.5.1
Organisations should assess the impact of security-related risks on the safety of legacy systems and update their risk assessments for legacy systems accordingly.

NOTE: Legacy systems may not have been designed with security in mind and therefore need additional security measures to ensure adequate protection against attack.

1.5.2
The risk assessment of legacy systems should cover their current state through to decommissioning and disposal.

1.6 SUPPLY CHAIN AND OTHER EXTERNAL DEPENDENCIES

1.6.1
Organisations should assess and manage security risks arising from external dependencies on suppliers, sub-contractors, and service providers.

NOTE 1: This includes ensuring that appropriate measures are employed where third-party services are used.

NOTE 2: ISO 28000 provides a means of implementing a security management system for supply chains.

1.6.2
Organisations should integrate the management of supply chain risks into their lifecycle processes, including specification, design, procurement, implementation and testing.

1.6.3
Organisations should have a process for managing the disclosure of potentially sensitive information to the supply chain in order to mitigate the risk of such information being misused.

NOTE: Section 1.9 discusses the protection of information assets in more detail.

1.6.4
Organisations should assess, and periodically re-assess, the security of their suppliers. The frequency of re-assessment should be determined by the organisation's security policy.

1.6.5
Organisations should ensure that suppliers have an appropriate policy and programme in place to manage risks to the safety and security of their products and services.

NOTE: Possible means of ensuring this include audits and external accreditation. Consider requiring all suppliers to be accredited to a standard such as Cyber Essentials [22],EN ISO/IEC 27001 [23] or IEC 62443-2-4 [24].

1.6.6
Organisations should include security requirements and requirements for good security engineering practice in procurement contracts with suppliers, and ensure that such requirements are cascaded down the supply chain as necessary.

NOTE 1: One way to comply with this clause is to require suppliers to comply with all or part of this CoP.

NOTE 2: Further guidance on supply chain security is available from CPNI [25] and NCSC [26].

1.7 SECURITY AWARENESS AND COMPETENCY

1.7.1
All personnel should be aware of security issues relevant to their role and should receive training to ensure they have the necessary knowledge and competence.

NOTE 1: The level of training needed will vary depending on the role, but it is likely that all personnel will need at least a basic level of security awareness training.

NOTE 2: The NCSC Certified Training scheme [27] certifies two levels of cyber security skills training:

- **Awareness level** — giving newcomers a thorough foundation in cyber security
- **Application level** — in-depth courses for professional development

1.7.2
Personnel that are responsible for the design, development, manufacture, delivery, operation or maintenance of safety-related products and services should have the information, knowledge, and skills they need to perform their roles securely.

1.7.3
Organisations should assess the need for specialist security expertise, and develop or contract such expertise as needed.

NOTE: This might include roles such as security architect, security risk assessor, penetration tester.

1.8 CULTURE AND COMMUNICATION

1.8.1
Organisations should promote a healthy security culture among those responsible for the safety of their product and services.

1.8.2
Communication channels for security matters relating to the organisation and its services and products should be established.

1.8.3
Where responsibilities for safety and security have been separated within an organisation, the organisation should promote cooperation and collaboration between the two groups.

NOTE: An example of such a measure would be a joint review of a product or service for security-related safety issues at an appropriate point in the design and development process.

1.9 PROTECTION OF INFORMATION

1.9.1
Organisations should ensure that the security of information, documentation and data whose compromise could affect the safety of their systems is maintained.

NOTE 1: Unauthorised disclosure of such information can significantly increase safety and security risks, as it can assist in identifying vulnerabilities. For example, detailed information about the security controls in the system design might help an attacker to successfully compromise a system.

NOTE 2: Information in both electronic and physical form should be protected (e.g. laptops, mobile devices, USB sticks, cloud storage, paper copies).

1.9.2
Organisations should formulate a procedure for classifying, labelling and handling security-related information and documents.

NOTE: Guidance on information classification, labelling and handling can be found in clause 8.2 of EN ISO/IEC 27002 [28].

1.9.3
Information with an HMG security classification should be handled in accordance with HMG security policy [29].

1.9.4
Information released to third parties (e.g. contractors, suppliers, maintainers) that could be used to compromise an organisation's security or the security of its systems should be appropriately classified and labelled, and the receiving party should be required to handle the information in accordance with its security classification.

NOTE: Examples of requirements for information handling could be the length of retention, the process to be followed for release and the measures to be taken to protect the information.

1.9.5
Information and documents received from other organisations should be handled in accordance with any security-related classification or labelling.

02.
LIFECYCLE CONSIDERATIONS

Safety-focused lifecycles aim to reduce the number and impact of faults in the product or service that supplies the required functionality. Typically, safe operating envelopes and hazards are identified using some form of risk assessment, and requirements are introduced to remove hazards, prevent their occurrence or mitigate their effects. In addition, requirements for safe operation, maintenance, and decommissioning are documented. Quality management and safety management processes are used to reduce the incidence of human errors at each stage of the lifecycle and thus reduce the risk of systematic faults in the system.

A security-aware approach will mirror a safety approach but will aim to reduce the number and impact of security vulnerabilities or weaknesses in the product or service. Many steps of the process will be very similar at a high level. However, it is important to note that it may be necessary to consider the security of products or components that do not have a direct safety impact. This is because systems that do not have direct safety relevance (e.g. passenger wi-fi and infotainment) might be used by attackers as an initial means of compromise to gain a foothold in the system before going on to attack further parts of the system.

This section includes a minimal set of measures to be incorporated into the product/service lifecycle. The measures are not to be regarded as complete, and do not exclude the incorporation of any other measures indicated (e.g. by standards or risk assessment).

In the railway context, PD CLC/TS 50701:2021 [4] provides guidance on the management of cybersecurity for railway applications within the framework of the lifecycle described in EN 50126-1 [30], but the guidance is applicable to other lifecycles too, depending on the system under consideration.

Further details about the relationship between the CoP and PD CLC/TS 50701 can be found in Appendix G.

General guidance on shared engineering principles and recommended practices for safety and security can be found in the IET Code of Practice on Cyber Security and Safety [7].

More generally, BS 10754-1:2018 [16] provides guidance on the governance and management of systems trustworthiness, and sets out a series of processes and controls for developing trustworthy systems.

2.1 GENERAL REQUIREMENTS

2.1.1

For all products and services, each phase of the lifecycle should be analysed to:

a. establish its role in delivering a safe and secure system

b. identify opportunities in the lifecycle to consider the security of the service or product

c. identify opportunities to introduce security measures in the lifecycle

NOTE 1: Some publications offer guidance on incorporating security into a safety lifecycle. For some cases, it may be sufficient to follow the guidance. Examples of such publications include IEC TS 62443-1-1 [31] and BS 10754-1:2018 [16].

NOTE 2: In the railway context, PD CLC/TR 50701 [4] identifies specific cybersecurity activities to be carried out during the lifecycle of a railway application, together with synchronisation points to ensure coordination with other stakeholders.

2.1.2

The lifecycle and supporting processes should be modified as needed to ensure that adequate consideration has been given to security issues and that a set of measures are implemented to ensure that a safe and secure product or service is produced.

NOTE 1: The measures to be deployed will depend on the specific situation. Examples include:

- *aligning security and safety activities with project management gateways*
- *including iterative security assurance activities*
- *aligning safety and security approval and sign-off activities*

NOTE 2: The production of a complicated system such as a railway signalling system requires a number of interlocking and integrated lifecycle processes. ISO/IEC/IEEE 15288 [32] identifies 30 system lifecycle processes, which are divided into four groups:

a. *agreement processes,*

b. *organisational project-enabling processes,*

c. *technical management processes; and*

d. *technical processes.*

2.2 RISK ASSESSMENT AND REQUIREMENTS DEFINITION

NOTE: PD CLC/TS 50701 describes an approach to cyber security risk assessment and requirements definition based on the IEC 62443 series of standards. More general guidance on risk assessment is given in Appendix A.

2.2.1

A detailed risk assessment should be performed on the proposed architecture of any new product or service (or modifications thereof) to identify any potential vulnerabilities or security risks that might affect the safety of the overall railway system.

NOTE: Established techniques for performing risk assessments can be found in NCSC's Risk Management Collection [33].

2.2.2

If the product or service depends on components or services procured from third parties, the risk assessment should consider the potential impact of contamination, faults or vulnerabilities in those components or services on the safety and security of the overall product or service.

NOTE: Contamination of computer-based components can take the form of malicious code or unauthorised modification to data, for example changes to configuration and reference data. In both cases, the outcome could be that the component operates in an unsafe manner.

2.2.3

The risk assessment should consider the potential effect of security incidents on the safety of the product or service.

NOTE: Although security incidents can be causal factors leading to hazards, the impact of a security incident on functional safety can be extremely difficult to predict. An alternative approach is to consider security incidents as hazardous events that can lead to multiple outcomes and potentially affect reliability and availability as well as safety.

2.2.4

The risk assessment should consider the risks posed by the following classes of attacks:

a. technical (e.g. hacking)

b. socio-technical (e.g. social engineering)

c. supply chain (e.g. substitution of components)

d. physical attacks (e.g. destruction of equipment)

NOTE: Although security incidents can be causal factors leading to hazards, the impact of a security incident on functional safety can be extremely difficult to predict. An alternative approach is to consider security incidents as hazardous events that can lead to multiple outcomes and potentially affect reliability and availability as well as safety.

2.2.5

The risk assessment should consider interactions, conflicts and trade-offs between security and safety. In general, safety should take precedence over security, unless the risks of an insecure system are considered to be too great.

NOTE 1: Safety is reliant on integrity, so preserving integrity should generally take precedence over preserving availability and confidentiality. Depending on the context, it may also be important to preserve availability.

NOTE 2: Further guidance on trade-offs between safety and security can be found in Appendix D.

2.2.6

The risk assessment should take interdependencies between systems and services into account and consider the potential impact of simultaneous failures and their consequences.

NOTE: This includes the possibility of cascade failures.

2.2.7

The risk assessment should allow for the possibility that changes to network connectivity (whether introduced maliciously or as a side-effect of another activity) could circumvent security measures.

NOTE: Air gaps merit particular attention in this context. An 'air gap' is a security measure where a computer system is physically isolated from other systems. The 'air gap' can be bypassed if a network connection is added.

2.2.8
To allow for the possibility of unknown network connectivity, the risk assessment should consider the entire system to be accessible to cyber attack unless network isolation can be guaranteed.

NOTE: This implies that the network should be treated as open by default (see Appendix E for more information on network security). Based on experience, network isolation is very difficult to maintain in the long-term, so erring on the side of caution is a sensible strategy.

2.2.9
The risk assessment should include risks posed by malicious actors who aim to cause deliberate harm, as well as risks posed by malicious actors who may incidentally cause harm as an unintended consequence of other activities.

NOTE: Examples of activities that might cause incidental harm as an unintended consequence are espionage, ransomware and cryptocurrency mining.

2.2.10
The risk assessment should include risks posed by non-malicious actors who might inadvertently cause harm as an unintended consequence of their actions.

NOTE: Examples of actions that might inadvertently cause harm include introducing an infected USB drive or choosing a weak password.

2.2.11
The risk assessment should be periodically reviewed throughout the lifetime of the product or service to allow for the potential impact of evolving security threats and the discovery of exploitable vulnerabilities on the safety of the system.

NOTE: The capabilities required for a successful attack are likely to decrease during the lifetime of the system, as attacks that are currently only within the capabilities of nation states become commoditised, so the system or service needs to be able to respond to changes to the threat profile.

2.2.12
The risk assessment should be used to derive appropriate requirements to mitigate the effect of the identified risks on safety and security.

2.2.13
The requirements derived from the risk assessment should include security requirements to mitigate the safety risks posed by threat agents to an acceptable level.

NOTE: See clause 1.3.3 for guidance on how to determine what is acceptable.

2.2.14
When a system (or service) is composed of subsystems (or other services), security requirements should be propagated to the specification of each subsystem (or service).

2.3 DESIGN

2.3.1
The product or service should be designed to be fail-safe and secure by default.

2.3.2
The design should address security and safety throughout the lifetime of the product or service.

2.3.3
The design should consider the potential impact of component vulnerabilities on the product or service, and include appropriate mitigations.

NOTE: Further guidance on secure design principles can be found in Section 5.

2.4 MANUFACTURING

2.4.1
The product should be manufactured in such a way as to prevent its safety or security being compromised by threats during the manufacturing process.

NOTE: Guidance on securing manufacturing systems can be found in PAS 1085 [34].

2.5 SUPPLY CHAIN

NOTE: This section provides recommendations for managing risks associated with procuring components from third parties. Recommendations for managing supply chain risks in general can be found in section 1.6.

2.5.1
Reasonable steps should be taken to ensure that all components received from suppliers are authentic and trustworthy.

2.5.2
All new hardware and software should be scanned for malware.

NOTE: Cyber security standards in other countries may not be equivalent to those in the UK. Furthermore, some countries may harbour malicious intent towards the UK and its industries. Further advice on supply chain risk is available from CPNI [25] and NCSC [26].

2.5.3
Suppliers should be required to disclose any functionality in their equipment or software that might be capable of compromising the safety or security of the device.

NOTE: Examples of such functionality include the ability for the supplier to transmit or receive data from the device or reprogram the device remotely.

2.5.4
Organisations should decide on a risk basis whether such functionality should be enabled or disabled, and this should be specified as part of the contract.

2.5.5
Suppliers should be contractually obliged to adhere to relevant security standards.

2.5.6
Organisations should include security requirements and requirements for good security engineering practices in procurement contracts and ask for evidence of security features and known vulnerabilities in the procured products.

2.5.7
Organisations should assert the right to audit the development environment and the security of the development, testing, chain of custody and shipping process.

2.5.8
Organisations should ensure that procurement staff are sufficiently knowledgeable in security to be able to articulate requirements correctly.

2.5.9
Organisations that use third-party products and services should ensure that their suppliers check for vulnerabilities and are prepared to issue security patches or updates throughout the lifetime of the product or service, or else state clearly that security patches are no longer provided, in which case the product or service can no longer be considered secure.

2.5.10
Organisations should identify who is responsible for the supply and installation of security patches to third-party products and services that they use in their own products or services.

NOTE: Further guidance on managing product and service updates can be found in clause 3.5.

2.5.11
Organisations should manage risks to the safety and security of their products or services caused by dependencies on third-party products or services that might be discontinued or cease to be maintained.

NOTE 1: If an organisation depends on a third-party product or service that is no longer maintained, there is a risk that future security vulnerabilities discovered in the third-party product or service might provide a means of attacking the organisation's own products or services.

NOTE 2: Possible steps to mitigate this risk include requiring advance notice of discontinuation, sourcing alternative products and services, and isolating/eliminating the dependency.

2.6 INSTALLATION

2.6.1
Installation of a product in the field should be carried out so that the safety and security of the overall railway system is maintained.

NOTE: It is common for special arrangements to be put in place while installation is carried out, and it is important that these do not offer opportunities to attackers, even if they are temporary in nature.

2.6.2
Equipment suppliers and installation contractors should only be granted access to the system for as long as is contractually necessary.

02. LIFECYCLE CONSIDERATIONS

NOTE: Consider deleting or changing all authentication keys used during installation and acceptance testing before the system is put into operation.

2.7 DEMONSTRATION OF SECURITY

2.7.1
There should be a documented plan for demonstrating that the safety and security of the product or service is adequate, and that security weaknesses do not cause unacceptable risks to the safety of the system.

2.7.2
The product or service should be subject to security analysis and testing, including:

a. system, attacker and threat modelling

b. an analysis for common known weaknesses or vulnerabilities

c. an analysis of whether the proposed security controls are sufficient to mitigate the risk

d. an evaluation of whether the proposed security controls are implemented correctly

e. penetration testing

NOTE: Analysis complements testing – neither can prove security, but both increase confidence.

2.7.3
Where practicable, security analysis and testing should be integrated throughout the development lifecycle.

NOTE: This contrasts with relying on security analysis and testing only after completion of design and development. Continuous or iterative testing allows for potential faults and vulnerabilities to be identified much sooner.

2.7.4
The product or service should be subject to independent scrutiny to assess whether threats to its security pose unacceptable risks to safety.

NOTE: 'Independent' can refer to personnel inside the organisation, but not involved in product or service development, or to personnel from an external organisation.

2.7.5
The degree of security analysis and testing, and the level of independent scrutiny required should be commensurate with risk factors such as the following:

a. the safety criticality of the product or service

b. the level of threat to which the product or service is exposed

c. any known vulnerabilities in the product or service

d. the provenance of the product or service

NOTE: The requirements for independent assessment in safety standards (e.g., EN 50129 [3]) might need to be adjusted accordingly.

2.8 ASSURANCE

2.8.1
For safety-relevant products or services, an assurance case should be produced that justifies that the product or service is adequately safe, despite the presence of security threats.

NOTE: For complete systems, the assurance case will address the safety of the product or service, while for components, the assurance case will address their performance with respect to their specifications.

2.8.2
The assurance case should demonstrate that security threats that could affect safety have been adequately managed and show that the impact of security on safety has been considered throughout the entire lifecycle of the product or service, from initial conception through design, installation, operation and maintenance to decommissioning.

NOTE 1: Further guidance on assurance cases can be found in Appendix B and ISO/IEC 15026 2:2011 [35].

NOTE 2: EN 50129:2018 [3] requires the safety case to 'describe how IT-Security threats which have the potential to affect safety-related functions have been evaluated and how protection against them has been achieved'.

2.8.3
In cases where a safety-relevant product or service depends on products or services procured from third parties, assurance material should be obtained from the third party and integrated into the overall assurance case.

NOTE 1: It is preferable for the supplier of a component or subsystem to supply their own assurance case, but it is recognised that this might not always be possible for off-the-shelf products.

NOTE 2: Clause 8 of EN 50129:2018 defines the safety acceptance and approval process for safety-related systems, subsystems and equipment. Safety approvals that are granted by one safety authority can be accepted by another safety authority ('cross-acceptance'), but only generic products and generic applications can be approved in this way. Specific applications always require the full safety acceptance and approval process to be followed.

2.9 OPERATION, MAINTENANCE, AND DECOMMISSIONING

2.9.1
Railway operators and service providers that are responsible for systems and services that affect the safety of the overall railway system should ensure that those systems and services are operated, maintained, and decommissioned safely and securely.

2.9.2
If responsibility for operation, maintenance, transfer of ownership or decommissioning is delegated to an external organisation, the license or contract should require the external organisation to provide assurance of compliance with all safety and security requirements.

NOTE: The railway operator or service provider remains accountable for the safe operation of the railway.

2.9.3
The operational documentation for the product or service should include security requirements as well as safety requirements in order to ensure that the product or service can be operated safely and securely.

NOTE: This may include operating procedures, constraints on the operating environment, etc.

2.9.4
The maintenance documentation for the product or service should include security requirements as well as safety requirements in order to ensure that the security and safety of the product or service is not compromised during maintenance activities.

2.9.5
The decommissioning documentation for the product or service should include security requirements as well as safety requirements and ensure that any security-related material related to the product or service (e.g. cryptographic keys) is securely removed and destroyed during decommissioning, or whenever the system is repurposed or transferred to a new owner or operator.

03.
MAINTAINING EFFECTIVE DEFENCES

It is important to ensure that the safety and security of the system is maintained throughout its entire lifecycle, including operation, maintenance, transfer of ownership, and decommissioning.

In most safety-critical systems, defences do not need to be upgraded unless the assumptions made when the system was designed become invalid. In the rail sector, railway signalling systems have traditionally operated in a well-defined environment, with little to no communication with the outside world. Thus, the risks to rail transport safety were fairly static and well-known.

However, in the modern era of connected systems, defences are exposed to changing and evolving threats from the failure or compromise of systems and services. In the security arena, attackers are continually discovering new vulnerabilities or developing new techniques for defeating existing defences. Attack tools also have a tendency to become commoditised, or packaged for easier use. This means that attacks that might once have required a high degree of skill or knowledge can now be used by threat actors with lower capability. This section contains recommendations on how to maintain effective defences and respond to attacks, including upgrading systems to patch uncovered vulnerabilities and close down new avenues of attack.

Ideally, there should be a good level of independence between security protection and safety function, so that it is possible to update the security protection quickly to take into account a new threat, without updating the safety function of the system. The safety case for the product or service should explain how to update the security of the product or service without impacting safety.

3.1 LEGACY SYSTEMS

3.1.1
Protective measures should be put in place to reduce the risks posed by known vulnerabilities and weaknesses in legacy systems.

NOTE 1: It may not be feasible to fix a known vulnerability in a legacy system, so the presence of the vulnerability must be tolerated.

NOTE 2: The risk of exploiting a vulnerability is determined by its ease of exploitation and the impact of a successful attack.

3.2 PROTECT, DETECT, RESPOND

NOTE: The Common Safety Method for Monitoring [6] requires rail operators to monitor the effectiveness of their safety management system and risk control measures during operation and maintenance. Since security threats have an impact on safety risks, this includes monitoring the effectiveness of safety controls to protect against cyber attacks.

3.2.1
Railway operators and service providers should implement measures to protect their systems against cyber attack.

3.2.2
Railway operators and service providers should monitor their systems to detect potential cyber attacks; unusual behaviour that might indicate that the system has been compromised should be investigated (see 4.2).

3.2.3
Railway operators and service providers should respond to a confirmed cyber attack on their systems in a timely fashion and aim to minimise its impact (see 4.4).

NOTE 1: It is not sufficient to protect the system against cyber attacks. It is also important to be able to detect attacks that have penetrated the system's defences and respond in an appropriate manner.

NOTE 2: Timeliness can be judged in terms of exposure to risk. The urgency of response depends on threat intelligence, and the likelihood and consequence of the safety and security of the overall railway system being compromised if the cyber attack is not addressed.

3.3 SECURE MAINTENANCE AND DECOMMISSIONING

3.3.1
Railway operators and service providers that are responsible for systems and services that affect the safety of the overall railway system should ensure that those systems and services are maintained safely and securely, particularly if temporary special arrangements are put in place for maintenance.

NOTE: It is important to ensure that any special arrangements put in place while maintenance is carried out do not offer opportunities to attackers, even if they are temporary in nature.

3.3.2
Security requirements should be incorporated into maintenance contracts.

NOTE: Security requirements may include provision of a service-level agreement.

3.3.3
Maintenance contractors should only be granted access to the system for as long as is contractually necessary.

NOTE: Before and after maintenance, consider deleting or changing any authentication keys that are needed to access the system.

3.3.4
Any security-sensitive material contained in equipment that needs to be taken out of service for repair should be securely removed and destroyed before the equipment enters the repair cycle.

3.3.5
Any security-sensitive material contained in equipment that is sold, repurposed, or decommissioned should be securely removed and destroyed before the equipment is passed on.

3.4 BUSINESS CONTINUITY

3.4.1
Railway operators and service providers that are responsible for systems and services that affect the safety of the overall railway system should have arrangements in place to maintain essential functions during and after a cyber attack.

3.4.2
Such backup systems should ensure the safety and security of the overall railway system in any degraded mode of operation.

NOTE: EN ISO 22301 [36] and EN ISO 22313 [37] provide guidance on business continuity management systems.

3.5 IDENTITY AND ACCESS CONTROL

3.5.1
Railway operators and service providers should document and manage all access to systems and functions that support the safe operation of the railway.

NOTE 1: Access rights should be carefully controlled, especially rights that grant access to safety-critical operations. The rights granted to individuals should be periodically reviewed and removed when no longer required.

NOTE 2: Guidance on identity and access management is available from NCSC [38].

3.5.2
Organisations should verify the identity of potential employees and the authenticity of their identity documents as part of their recruitment process.

NOTE 1: It is important to verify a person's identity before granting them access to your systems. The degree of identity verification required depends on the level of access they will have.

NOTE 2: Guidance on pre-employment screening is available from CPNI [39].

3.5.3
Access to systems or data that are important for the safe operation of the railway should require an appropriate level of authorisation and authentication.

NOTE 1: It may be useful to distinguish between read and write access. For example, train movement data that has been published on a website is readable but not writable, and can therefore be made accessible to a broader set of users.

NOTE 2: In some situations, it may be necessary to allow immediate access to a system without authentication for safety reasons (for example, to invoke an emergency shutdown function without any delay). This is acceptable providing other controls are in place to limit access to the system (for example, physical access controls).

3.5.4
The strength of authentication required should be proportionate to the degree to which the systems or services support the safety or security of the ecosystem.

NOTE 1: Examples of stronger forms of authentication are two-factor and biometric authentication.

NOTE 2: Consider physical access controls as well as technical controls.

3.5.5
To ensure accountability, each user should have their own identity.

3.5.6
The number of users with privileged access to the system should be strictly limited and periodically reviewed – in particular, the need for privileged access should be reviewed whenever a user's role or responsibilities change.

NOTE: Ideally, there should be NO need for privileged access to the system, but it is recognised that this is not always practical.

3.5.7
Unauthorised individuals should be prevented from accessing data or services at all points within the system.

3.6 PRODUCT AND SERVICE UPDATES

3.6.1
Organisations that use products or services supplied by another organisation should make arrangements to receive updates from the supplier of the product or service that they depend on.

3.6.2
Organisations that supply products or services should take steps to inform users of their products or services about updates when they are made available, and should encourage their users to apply updates that improve the safety or security of the product or service.

NOTE: Consider allowing updates to be fetched from a centralised location and applied automatically ('unattended updates'), subject to appropriate risk control measures (for example, only security updates should be applied automatically, updates should be evaluated and tested before they are released for automatic installation).

3.6.3
Organisations should determine how quickly to distribute updates to their products and services by considering the severity of any safety or security issues addressed by the update.

3.6.4
Access to product and service updates should be restricted to users and authorised maintenance organisations.

NOTE: Potential attackers can reverse-engineer updates to discover vulnerabilities in the original system.

3.6.5
Updates that are accessed remotely should be downloaded from a trusted source via a secure communication channel.

3.6.6
Updates should only be applied if their authenticity and integrity can be verified.

NOTE: Techniques such as digital signatures can be used to verify the origin and integrity of an update.

3.6.7
An initial assessment of the impact of each update on the safety and security of the overall railway system should be performed in a timely fashion.

NOTE: Until the impact of an update on the safety or security of the overall system is understood, the system is exposed to an unknown risk.

3.6.8
An update should only be applied if its impact on the safety and security of the railway system has been assessed and accepted as tolerable or the risk of not applying the update is considered to be intolerable.

NOTE 1: A risk assessment can be used to look at the balance between the risk of modifying the system and the risk of leaving the system unchanged. Factors to consider include whether the update addresses a safety or security vulnerability, the degree of exposure to the threat, and the potential impact of an accident/attack.

NOTE 2: Consider including a Safety-Related Application Condition (SRAC) in the Application Safety Case that establishes the assumptions and conditions under which system updates should be applied so as to mitigate risks and allow continued safe operation of the system (see clause 5.3.13 of EN 50129:2018 [3]).

3.6.9
Updates that improve the safety and security of the overall railway system should be applied in a timely fashion.

NOTE 1: Timeliness can be judged in terms of exposure to risk. The urgency of applying the update depends on the likelihood and consequence of the safety and security of the overall railway system being compromised if the update is not applied.

NOTE 2: If maintenance is delegated or subcontracted to another organisation, the timely installation of updates can be arranged using contractual clauses.

3.6.10
If it is necessary to avoid or delay applying an update, the decision should be documented, justified and approved by a designated person in the organisation, and the risk incurred by the decision should be assessed and mitigated if needed.

NOTE 1: Some systems (particularly operational technology) may need to be taken offline in order to be updated and this may take time to organise. In other cases, the organisation may require time to assess, test and approve the update.

NOTE 2: IEC TR 62443-2-3:2015 [40] offers guidance on patching in the context of industrial automation and control systems.

3.6.11
Updates should be tested on a single system before they are rolled out more widely.

3.6.12
Unattended updates should only be applied when the system is in a 'safe' state and not currently operational (e.g. locomotives are stationary and have been taken out of service).

3.6.13
If an update is unsuccessful for some reason, the system should be restored to its original state and the risk of allowing the system to continue to operate without the update should be assessed and mitigated if necessary.

3.7 INNOVATION

NOTE: Innovation covers new, potentially disruptive, uses of technology that can affect the way products or services are used, and undermine the assumptions made during the initial risk assessment. This can open the system to new modes of attack, introduce new vulnerabilities, or change the impact of failure or compromise. An example of innovation in the rail context is the use of data analytics and cloud-based services to predict and avoid reactionary delay.

3.7.1
Organisations should monitor and assess the potential of new technology to reduce or increase security threats to safety-related risks.

NOTE 1: The adoption of new technologies or changes to the use of existing technologies in the rail ecosystem could have an impact on the security of the product or service.

NOTE 2: New technologies might also change the relevance of existing assets to safety and security. See clause 1.4.3.

3.7.2
Organisations should have a documented strategy for adapting their products and services so that they remain safe and secure in the face of changing technology and use.

3.8 DISCOVERY OF VULNERABILITIES

3.8.1
Organisations should have a programme in place for handling the discovery of vulnerabilities in their products or services.

3.8.2
The programme should include documented procedures for assessing the safety impact of any alleged or actual vulnerabilities or new attacks on products and services.

3.8.3
The programme should include a documented policy for handling communications from third parties reporting the discovery of vulnerabilities or new attacks on products and services.

3.8.4
The programme should encourage the ethical and/or responsible disclosure of vulnerabilities in products or services.

NOTE: EN ISO/IEC 29147 [41] gives guidelines for the disclosure of potential vulnerabilities in products and online services.

3.8.5
Reports of failures (e.g. from warranty returns/repairs) should be examined for indications of a deliberate or malicious causal factor.

3.8.6
Reports of anomalous system behaviour and security incidents should be analysed for indications of new vulnerabilities or attacks.

NOTE: Data used for anomaly detection might include data with privacy implications.

NOTE: See also Section 4 – Incident Management.

3.9 THREAT MONITORING

3.9.1
Organisations should take steps to monitor and understand the potential threats to their products, systems and services and maintain an up-to-date threat assessment.

3.9.2
Organisations should subscribe/participate in government-led or industry-adopted schemes for disseminating threat information.

NOTE: An example is the Cyber Security Information Sharing Partnership (CiSP) hosted by NCSC [42].

3.10 CONTINUING RISK MANAGEMENT

NOTE: The Common Safety Method for Monitoring [6] requires rail operators to monitor the effectiveness of their safety management system and risk control measures during operation and maintenance activities, and make any improvements that are necessary.

3.10.1
Organisations should continue to manage the impact of security threats on safety risks.

3.10.2
Assurance cases should be reviewed regularly to ensure that they remain valid.

NOTE: This is particularly relevant in the light of changing threats, knowledge about vulnerabilities, and the evolution of systems and their connectivity.

04.
INCIDENT MANAGEMENT

Organisations with responsibilities for safety in the rail sector are likely to already have a mature process in place to identify and mitigate safety issues related to the design, manufacture or operation of their products, services or systems. Such reporting regimes are common in many safety-critical industries (e.g. aviation, health). They will likely cover short-term events such as a random fault or a failure in manufacturing or design, as well as low-probability failures, which might be identified by longer-term statistical analysis. Organisations are also likely to have procedures for responding to and mitigating identified issues, such as informing customers and arranging for repair or recall.

Security issues that impact safety also need to be identified and analysed in order to determine an appropriate response. Security offers some unique challenges when compared to safety in this respect. Security incidents often occur with a higher tempo than purely safety accidents, and require a faster response to maintain safety. This mainly stems from the fact that vulnerabilities are often shared among systems of a common design, and therefore multiple systems can be accessed simultaneously by an attacker. In addition, a tactic sometimes employed by adversaries is to attack the system and the organisation's response capability in parallel, in order to hamper activities aimed at mitigating or containing the attack. Therefore, the security of the response arrangements themselves is a concern. Timely and rapid dissemination of information is also important in responding to a security incident, particularly if adversaries make use of misinformation tactics (e.g. to influence user behaviour to bring about hazardous situations).

DfT is the security regulator for the domestic railway network and the lead government department for incidents that have an impact on transport systems, including cyber incidents. Under the NIS Regulations 2018 [13], 'operators of essential services' have a duty to notify the competent authority about 'any incident which has a significant impact on the continuity of the essential service'. The DfT guidance on the implementation of the NIS regulations in the transport sector [43] sets out the requirements for incident notification and defines the reporting thresholds and the types of organisation that are in scope (for the rail sector, these include the operators of mainline rail and high-speed rail services).

4.1 PLANNING

4.1.1
The organisation should have a documented plan for managing security incidents that indicate a potential risk to the safety of their products and services.

4.1.2
The plan should aim to ensure the continuity of any services that are important to the safe operation of the railway.

4.1.3
The plan should include the handling of security issues as part of a coherent process.

4.1.4
The plan should include mitigation activities designed to contain or limit the impact of an attack or other security incident on the safety of the organisation's products or services and on the safe operation of the railway system as a whole.

NOTE: Further guidance on security incident management is available from NCSC [44], CREST [45], and ISO 27035 [11]. Organisations may wish to implement an incident detection system compliant with ISO 27035.

4.1.5
The plan should identify an organisational function or role (a 'point of contact') with responsibility for coordinating incident response activities.

4.1.6
The plan should identify specific individuals who are responsible for and adequately competent in assessing if an event has a safety dimension.

4.1.7
The plan should identify specific individuals with sufficient authority to authorise any actions needed to preserve the safety and security of the organisation's products or services.

4.1.8
The plan should define a clear policy for escalation in the event of a serious incident.

4.1.9
The plan should consider the possibility of a security incident so severe as to necessitate withdrawal or recall of the organisation's products or services.

04. INCIDENT MANAGEMENT

4.1.10
The plan should be exercised regularly.

NOTE: Some organisations may find it appropriate to perform exercises in conjunction with others.

4.1.11
The infrastructure used to prevent, detect, respond to, and manage incidents should be protected against attack.

NOTE: The incident management infrastructure may be targeted to hamper response efforts and therefore increase the impact of an attack.

4.1.12
All personnel should be made aware of the means for reporting a suspected safety or security-related incident.

4.2 DETECTION

4.2.1
Organisations responsible for delivering services that are important to the safe operation of the railway should monitor the security status of their networks and information systems for evidence of both known and previously unknown attacks.

NOTE: Attackers use a variety of techniques to avoid detection via standard security monitoring, so it is important to use proactive security event discovery to detect attacks that evade standard detection and prevention measures. Records of activity should be analysed to detect unusual patterns of activity that might indicate previously unknown attacks.

4.2.2
Organisations that depend on services provided by third parties should ensure that those services are monitored for security incidents, and that they are notified of any relevant incidents in a timely fashion, so that they can manage their risk.

NOTE: According to clause 4.8 of the DfT guidance on the implementation of the NIS regulations in the transport sector [43], the NIS requirements do not apply directly to the supply chains of operators of essential services. Instead, it is the operator's responsibility 'to put in place appropriate and proportionate measures, and ensure that their suppliers have in place appropriate measures, to manage risks of their services being disrupted via their supply chain'.

4.2.3
Organisations should subscribe to industry or government-led schemes that provide notifications of relevant security incidents.

4.3 ASSESSMENT

4.3.1
Organisations should adopt a scheme for classifying security incidents.

NOTE: An example of an incident categorisation system can be found in the NIST Computer Security Incident Handling Guide [46].

4.3.2
Organisations should assess the impact of security incidents on the safety of their products or services.

4.3.3
Detected events should be assessed as soon as possible, and within 24 hours, to determine if the event should be classified as a safety incident.

NOTE: The fact that a system is under attack might not be clear in the initial stages of the incident, and it might be necessary to reassess as more information becomes available.

4.4 RESPONSE

4.4.1
Organisations should prepare a set of pre-planned response scenarios that are graded depending on the impact of an incident.

NOTE 1: The response scenarios may be generic, and be tailored to the actual incident as part of the response.

NOTE 2: Pre-planned responses help to ensure an adequate speed of response to security incidents.

4.4.2
The response should include communicating with relevant entities, including:

a. government agencies;

b. suppliers;

c. customers;

d. other industry actors; and

e. end-users.

NOTE 1: Attacks may exploit vulnerabilities that are present in products or services provided by other organisations, and it is essential that such organisations are notified quickly to ensure that they can also respond as needed. It is also important to notify operators of services that may be affected by a degraded state of the organisation's systems.

NOTE 2: Communication with end-users is necessary to prevent misinformation causing changes in behaviour, which might lead to adverse effects on safety.

4.5 POST-EVENT

4.5.1
Evidence that may provide information about the sequence of events leading to the incident should be preserved and analysed.

NOTE 1: Evidence such as logs are frequently targeted by attackers to obscure the nature and origin of their attack. Measures to prevent the modification or deletion of log entries may need to be deployed to prevent this.

NOTE 2: EN ISO/IEC 27037 [47] contains guidance on the identification and capture of digital evidence, while EN ISO/IEC 27042 [48] contains guidance on its analysis.

4.5.2
When an incident occurs, steps should be taken to understand its root causes and ensure that appropriate remediating action is taken, including updating the risk assessment and any relevant risk management measures.

4.5.3
The performance of the incident management plan should be reviewed post-incident and the plan should be updated if necessary.

4.5.4
Incidents that potentially have a criminal nature should be reported to the appropriate law enforcement agencies.

4.5.5
Lessons learned from the review of the incident that might be of value to others in the rail sector should be shared via an appropriate mechanism (see clause 8.3 and 8.4).

05.
SECURE AND SAFE DESIGN

The design of safety systems is in part driven by the need to make the design as predictable as possible, and to include features that prevent, detect or mitigate faults. Some safety designs follow the philosophy that they ought to be as simple as possible, in order to reduce the number of potential faults introduced and aid in analysis.

In contrast, security concerns often require inclusion of additional functionality beyond that needed to ensure safety from non-security-related hazards. Such functionality might include features such as intrusion detection, cryptography, improved access control and authentication, increased logging, and methods for updating and patching the system against newly discovered vulnerabilities and attack vectors. As with safety, a defence-in-depth approach is advocated, in which security controls are layered so that failure of a single control will not lead directly to a hazardous situation (for example, authentication may be required for all messages sent over ostensibly closed networks). This section contains recommendations for security measures that can be added to a system to increase the resilience of a system to attack.

Further guidance on secure development and deployment [49] and secure design principles [50] is available from NCSC.

5.1 GENERAL

5.1.1

The measures described in this section should supplement, not replace, any measures that are specified in application-specific standards such as EN 50128 [51] and EN 50657 [52].

5.1.2

Measures whose application is judged to be inappropriate or disproportionate to the security benefit need not be applied, but the rationale for this judgement should be explicitly recorded.

NOTE 1: A balance has to be struck between cost, complexity and risk. Typically, organisations consider all risks to their business, including commercial, financial and reputational risks, as well as safety and security risks.

NOTE 2: A complex system might carry a higher risk of failure and might be harder to justify, which typically motivates making systems as simple as possible, while maintaining the required functionality, performance, reliability and security.

5.2 SECURE DESIGN PRINCIPLES

5.2.1

The design should be based on a recognised set of secure design principles.

NOTE: Examples of secure design principles can be found in the SAFECode 'Fundamental practices for secure software development' [53] and the OWASP 'Guide to building secure web applications and web services' [54], which both reference a set of secure design principles originally proposed by Saltzer and Schroeder [55]:

1. ***economy of mechanism**: keep the design as simple as possible*
2. ***fail-safe defaults**: base access decisions on permission rather than exclusion*
3. ***complete mediation**: every access to every object must be checked for authority*
4. ***open design**: the design should not be secret*
5. ***separation of privilege**: two keys are better than one*
6. ***least privilege**: every programme and every user of the system should operate using the least set of privileges necessary*
7. ***least common mechanism**: minimise the amount of mechanism common to more than one user and depended on by all*
8. ***psychological acceptability**: design for ease of use*

5.3 SECURE SYSTEM CONFIGURATION

5.3.1

The underlying hardware and software system platform should be locked down and configured with respect to a secure baseline.

5.3.2
In particular, the following measures should be applied:

a. Any unnecessary functionality or applications should be removed or disabled.

b. Any unnecessary network services should be removed or disabled.

c. Unnecessary peripheral devices and removable media should be removed or disabled.

d. Applications should be configured to run with least privilege.

e. Only authorised software should be allowed to run.

NOTE: Maintaining a list of authorised software ('whitelisting') is preferable to trying to identify all harmful software ('blacklisting') using anti-virus and malware detection technology.

5.3.3
It should not be possible to alter the system configuration or install or disable any software or services running on the system from a 'normal' user account.

5.3.4
Any changes that are made to the system configuration from a 'privileged' user account should be monitored and recorded.

5.3.5
Users should not be allowed to access the Internet or email unless such access is required to perform their role and the associated risk is managed.

NOTE: This is to protect against possible compromise via remotely delivered malware.

5.3.6
The impact of any deviations from the baseline system configuration on the overall safety and security of the system should be considered and documented as part of the risk assessment.

NOTE: Further guidance on secure configuration and recommended configurations for particular platforms is available from NCSC [56].

5.4 BEHAVIOUR ON FAILURE

5.4.1
The system should include mechanisms to detect component failures or unusual behaviour that might indicate that a component has been compromised as the result of a security failure.

5.4.2
The system should be designed to take a proportionate response to maintain safety if a component failure or suspected compromise is detected.

NOTE: Examples of responses may be an indication for maintenance, fall-back operation or transition to a minimal risk state. For some failures, the system might be able to continue to operate safely.

5.4.3
Consideration should be given to whether the system can continue to deliver a service safely in the event of a component failure.

NOTE: This might include the use of contingency mechanisms such as manual processes to ensure services can continue, providing this can be achieved without compromising safety.

5.4.4
Component failures or suspected compromises of components should be reported to the operator via an appropriate mechanism and recorded for subsequent analysis.

5.4.5
Components that store security-sensitive information in non-volatile memory should ensure that the information is protected against disclosure in the event of a failure.

5.5 DEFENCE-IN-DEPTH

NOTE: Further guidance on this topic can be found from ICS-CERT [57].

5.5.1
The design of the system should be such that safety does not rely on the correct operation of any single component or subsystem.

NOTE 1: For example, a measurement of train speed may be derived from diverse sources of information.

NOTE 2: For simple systems that are intended for integration into a larger system that contains measures to detect or mitigate failures, application of this clause might be disproportionate.

5.5.2
Computer networks should be appropriately segmented with access controls at the segment boundaries so that the spread of potential attacks is limited.

NOTE 1: The degree of segmentation will depend on the types of connectivity in the network. Segmenting simple networks might be infeasible or disproportionate (see 5.1.1).

NOTE 2: IEC 62443 [31] provides guidance on security zones and conduits for network segmentation.

5.5.3
The compromise of a single non-safety related component should not enable the compromise of a safety-related component.

NOTE: The compromise of a security system that is specifically protecting a safety system could potentially lead to a violation of this clause.

5.5.4
The design of the system should prevent a non-safety-related component inducing a safety-related component to take an unsafe action.

NOTE 1: Possible ways of achieving this are isolating safety-related components/systems from non-safety-related components/systems, or by treating non-safety-related components as untrustworthy and putting appropriate security barriers in place.

NOTE 2: Consider implementing safety-critical functionality on dedicated hardware that is not used for any non-safety function.

5.6 USE OF CRYPTOGRAPHY

NOTE: Cryptography has many applications in maintaining security, including preventing access to information/data (encryption), verifying data integrity, and authentication. More detailed guidance on cryptographic controls can be found in EN ISO/IEC 27002, Section 10 [28].

5.6.1
Only cryptographic algorithms that have been subject to analysis and approval by a competent independent expert group should be used.

5.6.2
Only cryptographic implementations that have been subject to analysis and approval by a competent independent expert group should be used.

NOTE: NCSC provides a list of certified cryptographic products [58].

5.6.3
There should be a secure mechanism for generating, distributing and installing cryptographic keys.

NOTE: EN 50159 [59] requires cryptographic keys to be used for safety-related communication over open networks to guard against masquerade attacks. This means that the safety of the system depends on the security of the cryptographic key.

5.6.4
Cryptographic keys stored by the system should be protected against unauthorised use, disclosure, modification or deletion.

NOTE 1: An attacker could attempt to gain access to the system by adding a false key or deny access to the system by deleting keys.

NOTE 2: Depending on the design of the system, an attacker might be able to make use of a key without needing to know the value of the key.

5.6.5
Cryptographic material stored in non-volatile storage should be protected against disclosure.

NOTE: This is particularly pertinent if the device fails and needs to be taken out of service for repairs. See also clause 3.3.5.

5.6.6
It should not be possible to use any key that might be obtained from a train or a system to access multiple trains or systems.

NOTE: This ensures that any key that might be extracted from a train or system cannot be used to compromise other trains or systems.

5.6.7
Keys with known values that are used for testing purposes should be deleted before the system is put into operation.

NOTE: Test suites used to ensure interoperability between systems may mandate the use of test keys with known values. This requirement prevents an attacker from using such test keys to attack an operational system.

5.7 PROTECTION OF SOFTWARE IMAGES

NOTE: The software image is the binary representation of the compiled source code for the system. The software image can also contain static configuration data that is expected to remain constant during run time. The software image must be loaded into memory before it can be executed. An attacker that is able to modify the software image either prior to execution or during execution would be able to override functional safety and make the system behave in arbitrary ways.

5.7.1
Software images should be protected against unauthorised modification.

NOTE: A simple checksum is not sufficient to guarantee the integrity of the software image because an attacker can modify the software and the checksum. The use of a cryptographic checksum or digital signature is recommended. Alternatively, the software image could be encrypted.

5.7.2
Software images should be protected from unauthorised analysis or reverse engineering.

NOTE: Reverse engineering and unauthorised analysis can be made more difficult using techniques such as encryption, obfuscation or stripping the symbol table from the software image. However, techniques that alter the structure of the executable code should be used with caution in safety systems.

5.7.3
The system should check the integrity and authenticity of all software images at load time.

5.7.4
The system should ensure the integrity of the software image in memory during run time.

NOTE: Depending on the system hardware, it may be possible to store the software image in read-only memory, which would prevent it from being modified at run time. Alternatively, the integrity of the image stored in memory could be checked periodically.

5.7.5
The system should include integrity checks on control flow to ensure that the software is not subverted at run time.

NOTE: Depending on the system hardware, it may be possible to store the software image in execute-only memory, which guards against some forms of buffer overflow attack [60] that attempt to overwrite memory with executable code, but not more sophisticated attacks such as Return Oriented Programming [61]. See [62] for more information on techniques to achieve data flow and control flow integrity.

5.8 DIAGNOSTICS AND MAINTENANCE

5.8.1
The system should provide a secure interface for diagnosing faults.

NOTE: If the design makes provision for secure fault diagnosis, the motivation for bypassing security controls to diagnose faults is reduced. However, it is permissible for the manufacturer to restrict access to more powerful diagnostic functions, such as the ability to change parameters that could compromise the safety of the system.

5.8.2
Interfaces that are intended for diagnostic purposes should be protected against misuse.

NOTE: Physically hiding access ports is not considered adequate protection. An example of adequate protection might be requiring authentication before allowing access through the interface.

5.8.3
Diagnostic or debugging actions that interact with safety-relevant systems should be restricted in scope so as not to allow them to be abused to create a hazardous situation.

NOTE: For example, the diagnostic action may be restricted to only act when the train is moving at low speed.

5.8.4
Diagnostic equipment should be stored in a physically secure location.

5.8.5
Diagnostic equipment should require authentication before use.

NOTE: To ensure accountability, it might be necessary to require that each user of the equipment has a personal set of authentication credentials that are not shared between users.

5.8.6
All diagnostic and corrective actions performed during maintenance should be recorded in a secure fashion in a log.

5.8.7
The log should include details of the action performed, the time at which it was performed, and the identity of the user who performed the action.

5.8.8
Commands that affect the system's state or configuration, or cause an action, should be managed using secure protocols, including authentication.

5.9 PATCHING AND UPDATES

5.9.1
The mechanism for applying patches and updates should be safe and secure.

NOTE: For example, it should only be possible to update the system when it is in a safe state, and the update should be checked for authenticity before it is applied.

5.9.2
The design should facilitate the system being updated without compromising its overall safety and security.

NOTE: For example, the system could be designed in a modular fashion with an architecture that enforced strong separation between components such as a separation kernel [63].

5.9.3
It should be possible to revert an update or restore the system to a known good state if the update process fails or needs to be reversed for any reason.

NOTE: For example, an update might be installed successfully and then discovered to have an adverse effect on safety or performance. See also clause 3.5.

5.9.4
It should be possible for users to identify the revision of software installed on a system or device and determine whether updates are available, without the need for access to restricted information or specialised equipment.

NOTE: Equipment such as cables or interfacing software supplied with a product or device is not considered to be specialised equipment.

5.10 PROTECTION OF COMMUNICATIONS

NOTE: Appendix E provides further guidance on network security.

5.10.1
Networks used by passengers (e.g. passenger wi-fi) should be isolated from networks used for train control and railway signalling.

NOTE: The network architecture should prevent direct passenger access to a train's control and command systems. If physical network isolation is considered to be too difficult or expensive to implement, logical network isolation should be implemented using firewalls and routers.

5.10.2
Safety-critical data should only be transmitted over a secure channel to ensure that non-safety-related components cannot interfere with the data.

NOTE: Ideally, safety-critical data should be transmitted over a dedicated link, but if this is not possible, it is acceptable to use virtual channels to separate traffic over a shared link, providing that traffic isolation and adequate bandwidth/quality of service can be guaranteed for the secure channel.

5.10.3
All data received by the system should be checked for integrity and validity.

*NOTE: **Integrity** means that the data has not been corrupted. **Validity** means that the content of the data satisfies application-specific constraints. Data that passes an **integrity** check is not necessarily **valid**. It is also important to check that the data is meaningful and consistent, for example, to check that the values of data fields are within range and are internally consistent.*

5.10.4
All data received from an external source should be checked for authenticity.

NOTE: Authenticity means that the origin of the data can be confirmed with some degree of certainty and the data is known not to be a forgery. A simple integrity check is not enough because an attacker with knowledge of the algorithm could forge the data and the integrity check. To ensure authenticity, the use of cryptographic techniques is recommended – further guidance can be found in Appendix E and EN 50159.

5.10.5
Data received from an internal source should also be checked for authenticity unless it can be shown that the internal data link cannot be accessed by an external source or an untrusted internal source.

NOTE: Timing constraints and bandwidth limitations may mean that it is not technically feasible to check the authenticity of data sent over a real-time bus, but this is only acceptable if it can be shown that the internal network cannot be accessed by an attacker.

5.10.6
Data that reveals sensitive information about the system that might facilitate an attack should be encrypted to ensure confidentiality.

5.10.7
Secure communication protocols should be designed to enforce a minimum level of security.

NOTE 1: The strength of a security protocol depends on factors such as key length and choice of cryptographic primitive (encryption algorithm, hash function, etc.). The protocol implementation version may also be significant if certain implementations are known to contain vulnerabilities.

A minimum level of security can be enforced by updating the software at both ends of the communication in lockstep or by using protocol negotiation to agree on these parameters whenever a new communication session is established.

NOTE 2: If the protocol does not enforce a minimum level of security, an attacker could force the protocol to operate with a reduced level of security that was susceptible to attack.

5.10.8
The design and implementation of secure communication protocols should be periodically reviewed and updated if necessary to ensure that the protocol remains secure.

NOTE 1: Flaws in the design or implementation of a protocol can make the protocol insecure and potentially unsafe to use.

NOTE 2: Advice and guidelines on the use of cryptography are available from organisations such as NIST [64] and equivalent national and international organisations.

5.11 PROTECTION OF CONFIGURATION DATA

5.11.1
Configuration data that affects the safe operation of the system should be protected against unauthorised modifications.

NOTE: This includes data used to configure the interlocking or signalling system, for example, data about maximum safe speeds and track geometry.

5.11.2
There should be a mechanism for resetting the system to its default factory state and deleting any security-sensitive information that is required for its operation (e.g., cryptographic keys).

NOTE: This mechanism is intended to be used before transfer of ownership or decommissioning to prevent the inadvertent disclosure of security-sensitive information.

5.12 EXTERNAL SERVICES AND DEVICES

5.12.1
The system should be designed to interact safely and securely with external services and devices.

NOTE: 'External devices' are devices that are not permanently integrated with the system.

5.12.2
The integrity, validity, and authenticity of data received from external services and devices should be verified.

5.12.3
The degree to which external data is trusted should depend on the safety-impact of the data and the trustworthiness of the source.

NOTE: For example, data without any impact on safety might be accepted from a potentially untrustworthy source, data with moderate safety relevance might require a trusted source, while safety-critical data might only be accepted from two independent sources.

5.12.4
The system should not make safety-related decisions on the basis of information received from an external source, unless the source is known to be trustworthy, the information can be verified, or the risk from ignoring the information is unacceptable.

NOTE: An example of verification would be corroboration by an independent source.

5.12.5
The system should not rely on the availability of external services to operate safely.

NOTE: For example, even highly-reliable services such as GNSS can be jammed by attackers.

5.12.6
The system should be able to withstand receiving corrupt, invalid or malicious communications on external interfaces, while maintaining safe operation.

NOTE: This includes flooding, denial of service and jamming.

5.13 PHYSICAL SECURITY

5.13.1
Cables into buildings and cabinets containing systems that are important for safe railway operations should be protected against physical attacks that might facilitate cyber attacks.

NOTE: Guidance on perimeter security is available from CPNI [65].

5.13.2
Appropriate protective security measures should be incorporated into the design of new stations and redevelopments of existing stations.

NOTE: DfT (in conjunction with CPNI and the British Transport Police) published guidance on security in the design of stations (SIDOS) [66].

5.13.3
The vulnerability of CCTV, emergency alarm, and building management systems to cyber attack should be considered.

5.14 FORENSIC RECORDING

5.14.1
The system should include mechanisms to record system activities securely to enable forensic examination and aid identification of the cause of a cyber security incident.

NOTE 1: Safety systems often include an event data recorder or 'black box' device that can be used to investigate the cause of a safety incident and this device can also be used to investigate the cause of security incidents.

NOTE 2: EN ISO/IEC 27037 [47] contains guidance on the identification and capture of digital evidence.

5.14.2
All records of system activity should be preserved for a sufficient time period to allow for the detection and investigation of security incidents.

NOTE 1: The appropriate time period will be determined by factors such as the criticality and sensitivity of the data, and the amount of time that might be required for the incident to be detected and an investigation instigated. Sophisticated attacks such as advanced persistent threats can take place over a period of 6-12 months, so records should potentially be retained for at least a year.

NOTE 2: Attention is drawn to the possibility that such records might contain personally identifiable data, in which case data protection legislation would be applicable and might impose requirements for how the data is stored and protected.

5.14.3
Where practicable, a component or subsystem that is to be integrated into a larger system should be capable of outputting messages to an external logging device as well as any internal recording facility.

NOTE: This might not be practicable for some low-level components.

5.14.4
The forensic recording facility should be designed so that it is not possible for an attacker to conceal their actions by suppressing logging messages or modifying or deleting logging records.

5.14.5
The forensic recording facility should be designed so that actions are logged as they are performed, or immediately thereafter.

NOTE: If logging is designated as low-priority, there is a risk that some actions may not be logged in time to ensure their preservation, e.g. if power is lost to the unit.

5.14.6
All significant actions and events should be recorded, particularly actions and events that have an impact on the safety or security of the system.

5.14.7
To ensure traceability and guard against component or subsystem failures, the inputs, actions, and outputs of each component or subsystem should be logged independently.

NOTE: If a component or subsystem is responsible for logging its own inputs, actions, and outputs, in the event of a failure or compromise of the component, the log messages are no longer reliable or trustworthy.

5.14.8
Changes made to safety-relevant and security-relevant parameters should be recorded together with the time and the origin of the change.

5.14.9
It should be possible to reconstruct the sequence of events or actions from the forensic record of log messages.

NOTE: For example, all logging messages could be timestamped using a global clock or shared time reference.

5.14.10
It should be possible to reconstruct the sequence of events or actions from the forensic record of log messages.

5.15 SECURE USER INTERFACES

5.15.1
The possibility for compromised components or systems to affect user behaviour in an unsafe way should be mitigated by the design of the user interface.

NOTE: Examples of ways in which user behaviour can be changed include distraction, presentation of misleading information, or incentives to change or disable safety or security functionality.

5.15.2
The system should be designed so as to permit and promote secure user behaviour.

NOTE: For example, the system might promote the use of strong authentication methods such as two-factor authentication and discourage the use of shared passwords to ensure accountability.

5.15.3
Diagnostics and error messages should not include information that might help a potential attacker.

NOTE: For example, the error message for a failed login attempt should not tell the user whether the username or password were correct. Similarly, diagnostic messages displayed to the user should not include internal details about the software such as file names.

5.16 DEVELOPMENT ENVIRONMENT

5.16.1
All software should be developed in accordance with secure coding practices.

NOTE: Examples of guidance on secure coding practices are MISRA-C [67], SEI CERT C Coding Standard [68] and SAFECode [53]. Further guidance on safe and secure coding practices can be found in Appendix F.

5.16.2
Each tool used in the development and assurance process should be assessed for its role in mitigating security-related safety risks and its potential role as an attack vector.

NOTE: Tools include specialised tools for development and verification (compilers, debuggers, static analysers, formal verification tools, testing tools), general purpose development tools (build tools, configuration management tools, issue tracking and code review tools), general purpose applications (email, web browser, office applications, document tracking systems), and operating systems (client and server).

5.16.3
The design and development environment and infrastructure should be secured against threats that might manipulate the design and development process or compromise the integrity of the product or service.

NOTE: This includes physical, personnel and information security.

5.17 SOFTWARE DISTRIBUTION

5.17.1
Software images should not be publicly available.

NOTE: Publishing the software image on a web server whose name is not advertised does not provide sufficient protection. There have been instances of security researchers using Google to locate software images on public web servers, downloading the software, and analysing it for security flaws [69].

5.17.2
Software images should only be accessible to authorised users.

NOTE: For example, customers should be required to log on to a secure web site in order to download a copy of the software.

5.17.3
All access to software images should be logged.

5.17.4
Software images should only be generated by authorised staff.

NOTE 1: This is to prevent developers from generating 'unofficial' versions of the software image.

NOTE 2: This does not prevent developers from generating test versions of the software image during development, but the system should distinguish between test versions and official versions.

5.17.5
Software images should only be published by authorised staff.

NOTE: This is to prevent unauthorised publication of software images and can be achieved using procedural controls. Consider using 'separation of duty' to separate the privileges required to generate and publish an authentic software image.

06.
CONTRIBUTING TO A SAFE AND SECURE WORLD

In safety industries, lessons learned are typically shared to push best practice forward. The safety of systems is often communicated to end users and society at large via compliance with regulations, certification to standards, or specific testing schemes. Accident and near-miss investigations provide a formalised route for learning from experience, especially in the regulated high-hazard industries.

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

It is worth noting that an organisation's assets could be used to compromise the assets of another, and the resilience of the railway system 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 organisation 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, and the protocols for reporting and escalating externally. This is particularly relevant in the context of systemic failure, where hazardous situations can be caused in a class of systems due to a shared common vulnerability.

6.1 MANAGING RISKS

6.1.1
The organisation should assess and manage risks to:

a. the wider rail system

b. society more generally

These risks might be derived from failure or compromise of its products or services.

NOTE 1: The approach will depend on the 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 organisation's products and services, leading to a reduction in rail transport capacity with a consequential impact on many other activities.

6.2 COMPATIBILITY AND INTEROPERABILITY

6.2.1
The organisation's products 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.

6.3 INFORMATION SHARING

6.3.1
Organisations should enable customers to assess the security of their products and services by making sufficient design and assurance information available.

NOTE: To protect intellectual property, confidential information such as detailed design documentation can be made available under an NDA.

6.3.2
The organisation should be able to provide third parties with assurance or certification that the organisation's processes relevant to the production of a safe product or service are secure.

6.3.3
The organisation should collaborate with relevant organisations to obtain knowledge and understanding of current and relevant threats.

6.3.4
If the organisation becomes aware of vulnerabilities that affect or might affect the products or services of another organisation, they should responsibly disclose such vulnerabilities to those organisations.

NOTE: Vulnerabilities might be identified through post-incident analysis (see Section 4.5), or reported by third parties.

6.3.5
The organisation should support other organisations in the ecosystem to understand and manage security risks arising from the use or abuse of its services or products.

NOTE: Relevant organisations might include governmental organisations (including security agencies), industry umbrella groups and other industry actors.

06.
CONTRIBUTING TO A SAFE AND SECURE WORLD

6.4 COLLABORATION

6.4.1
The organisation should collaborate with relevant organisations to share, develop and foster the adoption of good engineering practices to mitigate current and relevant threats.

NOTE: Relevant organisations might include governmental organisations (including security and law enforcement agencies), industry umbrella groups and other industry actors.

6.4.2
The organisation should define an approach for adopting open design practices and deciding when and how to share designs and source code.

6.5 INTERNATIONAL ISSUES

6.5.1
Organisations should consider the implications of working with organisations from other countries throughout their supply chain. Some countries may harbour malicious intent towards the UK.

NOTE: Further guidance on supply chain risk is available from CPNI [34] and NCSC [26].

GLOSSARY

BS	British Standard
CAE	Claims Argument Evidence
CAF	Cyber Assessment Framework
CCAV	Centre for Connected and Autonomous Vehicles
CERT	Computer Emergency Response Team
CiSP	Cyber Security Information Sharing Partnership
CoP	Code of Practice
CPNI	Centre for Protection of National Infrastructure
CSAP	(Rail) Cyber Security Assurance Principle
EN	European Norm
ENISA	European Union Agency for Network and Information Security
DfT	Department for Transport
FTA	Fault Tree Analysis
GB	Great Britain
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GSN	Goal Structured Notation

GLOSSARY

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IET	Institute of Engineering and Technology
ISO	International Organisation for Standardization
HAZOP	Hazard and Operability
HS2	High Speed 2
LAN	Local Area Network
MISRA	Motor Industry Software Reliability Association
NCSC	National Cyber Security Centre
NDA	Non-Disclosure Agreement
NHTSA	(US) National Highway Traffic Safety Administration
NIST	(US) National Institute of Standards and Technology
NIS	Network and Information Security
ONR	Office for Nuclear Regulation
ORR	Office of Rail and Road
PAS	Publicly Available Specification
RAM	Reliability, Availability, Maintainability

GLOSSARY

RAMS	Reliability, Availability, Maintainability, Safety
RSSB	Rail Safety and Standards Board
SAFECode	Software Assurance Forum for Excellence in Code
SAF	(Network Rail) Security Assurance Framework
SEI	Software Engineering Institute
SFAIRP	So far as is reasonably practicable
SIL	Safety Integrity Level
SRAC	Safety-Related Application Condition
WAN	Wide Area Network

BIBLIOGRAPHY

[1] HM Government, The Railways and Other Guided Transport Systems (Safety) Regulations 2006 http://www.legislation.gov.uk/uksi/2006/599/

[2] DfT, Rail Cyber Security, Guidance to industry, February 2016 https://www.gov.uk/government/publications/rail-cyber-security-reducing-the-risk-of-cyber-attack

[3] EN 50129:2018 – Railway Applications – Communication, signalling and processing systems – Safety related electronic systems for signalling, November 2018

[4] PD CLC/TS 50701:2021, Railway applications – Cybersecurity, July 2021

[5] Commission Implementing Regulation (EU) 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment, as amended by the Rail Safety (Amendment etc.) (EU Exit) Regulations 2019 https://www.legislation.gov.uk/eur/2013/402/

[6] Commission Implementing Regulation (EU) 1078/2012 of 16 November 2012 on the common safety method for monitoring, as amended by the Rail Safety (Amendment etc.) (EU Exit) Regulations 2019 https://www.legislation.gov.uk/eur/2012/1078/

[7] IET, Code of Practice, Cyber Security and Safety, 2020 https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/

[8] EN 61508-1:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements, June 2010

[9] PD ISO/IEC TR 19791:2010, Information technology – Security techniques – Security assessment of operational systems

[10] IEC 62443, Security for industrial automation and control system

[11] ISO/IEC 27035-1:2016, Information Technology – Security Techniques – Part 1: Principles of Incident Management

[12] RSSB, Taking safe decisions, August 2019 revision https://www.rssb.co.uk/Standards-and-Safety/Improving-Safety-Health--Wellbeing/Applying-Guidance-and-Good-Practice/Taking-Safe-Decisions

[13] HM Government, The Network and Information System Regulations, 2018 https://www.legislation.gov.uk/uksi/2018/506

[14] HM Government, Data Protection Act, 2018 https://www.legislation.gov.uk/ukpga/2018/12

[15] PAS 555:2013, Cyber security risk – Governance and management – Specification

[16] BS 10754-1:2018, Information Technology – Systems Trustworthiness – Part 1: Governance and management specification

[17] NCSC, CAF guidance, version 3.1, April 2022 https://www.ncsc.gov.uk/collection/caf

[18] HM Government, Health and Safety at Work etc. Act, 1974 https://www.legislation.gov.uk/ukpga/1974/37

[19] CPNI, Physical Security https://www.cpni.gov.uk/physical-security

[20] CPNI, Personnel and People Security https://www.cpni.gov.uk/personnel-and-people-security

[21] NCSC, Advice and Guidance https://www.ncsc.gov.uk/section/advice-guidance/all-topics

[22] Cyber Essentials https://www.ncsc.gov.uk/cyberessentials/overview

[23] EN ISO/IEC 27001:2017, Information technology — Security techniques — Information security management systems – Requirements

[24] IEC 62443-2-4:2019, Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers

[25] CPNI, Supply chain guidance https://www.cpni.gov.uk/protected-procurement

BIBLIOGRAPHY

[26] NCSC, Supply chain security guidance, version 1.0, November 2018 https://www.ncsc.gov.uk/collection/supply-chain-security

[27] NCSC Certified Training https://www.ncsc.gov.uk/information/certified-training

[28] EN ISO/IEC 27002:2017, Information technology — Security techniques — Code of practice for information security controls

[29] Cabinet Office, Government Security Classifications, v1.1, May 2018 https://www.gov.uk/government/publications/government-security-classifications

[30] EN 50126-1:2017, Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS process

[31] IEC TS 62443-1-1:2009, Industrial communication networks — Network and system security — Part 1 1: Terminology, concepts and models

[32] ISO/IEC/IEEE 15288:2015, Systems and software engineering – System lifecycle processes

[33] NCSC, Risk management guidance, version 1.0, November 2018 https://www.ncsc.gov.uk/collection/risk-management-collection

[34] PAS 1085:2018, Manufacturing – Establishing and implementing a security-minded approach – Specification, May 2018

[35] ISO/IEC 15026-2:2011, Systems and software engineering — Systems and software assurance, Part 2: Assurance case, 2011

[36] ISO 22301:2019, Security and resilience – Business continuity management systems – Requirements

[37] ISO 22313:2020, Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301

[38] NCSC, Introduction to identity and access management, version 1.0, January 2018 https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management

[39] CPNI, Employment screening – Good practice guide, Edition 7, August 2021 https://www.cpni.gov.uk/resources/pre-employment-screening-good-practice-guide-edition-7

[40] PD IEC/TR 62443-2-3:2015, Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment

[41] EN ISO/IEC 29147:2020, Information Technology – Security Techniques – Vulnerability Disclosure

[42] NCSC, Cyber Security Information Sharing Partnership (CiSP) https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

[43] DfT, Implementation of the NIS Directive: DfT Guidance, Version 1.1, December 2018 https://www.gov.uk/government/publications/implementing-the-network-and-information-systems-directive-in-the-transport-sector

[44] NCSC, 10 Steps to Cyber Security: Incident Management, Version 1.0, May 2021 https://www.ncsc.gov.uk/collection/10-steps/incident-management

[45] CREST, Cyber Security Incident Response Guide https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

[46] NIST, Computer Security Incident Handling Guide, Special Publication 800-61, Rev. 2, 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[47] EN ISO/IEC 27037:2016, Information Technology – Security Techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence

[48] EN ISO/IEC 27042:2016, Information Technology – Security Techniques – Guidelines for the analysis and interpretation of digital evidence

BIBLIOGRAPHY

[49] NCSC, Secure development and deployment guidance
https://www.ncsc.gov.uk/collection/developers-collection

[50] NCSC, Secure design principles
https://www.ncsc.gov.uk/collection/cyber-security-design-principles

[51] EN 50128:2011+A2:2020, Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems

[52] EN 50657:2017, Railway applications — Rolling stock applications — Software on board rolling stock

[53] SAFECode, Fundamental practices for secure software development, Third edition, March 2018
https://safecode.org/uncategorized/fundamental-practices-secure-software-development/

[54] OWASP, A guide to building secure web applications and web services, Version 2.0.1, June 2014
https://github.com/OWASP/DevGuide/wiki

[55] Jerome H. Saltzer and Michael D. Schroeder, The protection of information in computer systems, Fourth ACM Symposium on Operating Systems Principles (October 1973), Revised version in Communications of the ACM 17,7 (July 1974)
http://web.mit.edu/Saltzer/www/publications/protection/

[56] NCSC, Device security guidance
https://www.ncsc.gov.uk/collection/device-security-guidance

[57] ICS-CERT, Recommended practice – Improving Industrial Control System Security with Defence-in-depth strategies, September 2016
https://www.cisa.gov/uscert/ics/Abstract-Defense-Depth-RP

[58] NCSC, Products & services
https://www.ncsc.gov.uk/section/products-services/introduction

[59] EN 50159:2010+A1:2020, Railway applications — Communication, signalling and processing systems — Safety-related communication in transmission systems

[60] Aleph One, Smashing the stack for fun and profit, Phrack 49, 1998
http://phrack.org/issues/49/14.html#article

[61] Hovav Shacham, Erik Buchanan, Ryan Roemer, Stefan Savage, Return-oriented programming: exploits without code injection, Black Hat USA, August 2008
https://hovav.net/ucsd/talks/blackhat08.html

[62] Peter Stavroulakis, Mark Stamp (Editors). Handbook of Information and Communication Security, Springer-Verlag Berlin Heidelberg, 2010
https://www.springer.com/gp/book/9783642041167

[63] John Rushby, The Design and Verification of Secure Systems, Eighth ACM Symposium on Operating System Principles, pp. 12-21, December 1981. (ACM Operating Systems Review, Vol. 15, No. 5)
http://www.csl.sri.com/users/rushby/abstracts/sosp81

[64] NIST, Cryptographic standards and guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

[65] CPNI, Building & Infrastructure
https://www.cpni.gov.uk/building-infrastructure

[66] DfT, Security in the design of stations (SIDOS), October 2018
https://www.gov.uk/government/collections/land-transport-security

[67] MISRA. MISRA-C:2012 — Guidelines for the use of the C language in critical systems. MIRA Limited, Nuneaton, Warwickshire, UK, March 2013

[68] Software Engineering Institute, Carnegie Mellon University. SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems (2016 edition)
https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards

[69] Ruben Santamarta, In flight hacking system, IOActive, Dec 2016
https://ioactive.com/in-flight-hacking-system

APPENDIX A
RISK ASSESSMENT

GENERAL

There is a wide range of generic and industry-specific standards and guidance for separately addressing safety and security risks. While these approaches are relatively mature, challenges arise when applying them together in a security-informed safety context. This appendix discusses some of these challenges.

IMPACT ON THE PROJECT LIFECYCLE

This CoP considers the impact of security on safety for overall governance and for individual phases of the project lifecycle. However, it is important to recognise that safety and security currently follow their own lifecycles and have differing scopes (e.g. security seeks to protect assets that might not be relevant to safety). An integrated approach requires there to be one or more points of interaction in the safety and security lifecycles, where security specialists and safety engineers can exchange safety and security concerns and agree on appropriate controls.

IMPACT ON HAZARD IDENTIFICATION

Security concerns could have an impact on:

- the system boundaries
- the systems that could potentially affect safety
- the stakeholders involved, and
- the validity of design safety assumptions

A conventional safety analysis uses a fairly well-defined system boundary, and the analysis identifies causal factors (typically random or accidental events) that could result in a hazard. This is shown graphically in Figure 1. The hazard occurs on the boundary of the system being analysed. Barriers (shown in red) are mitigations or countermeasures within the system that aim to reduce the likelihood of a hazard developing from its identified causes. Further barriers can be used outside the system boundary to reduce the likelihood that the hazard will lead to an accident. These barriers are shown in Figure 1 with red vertical lines. The terms ‘countermeasure’, ‘barrier’ and ‘control’ are often used interchangeably, although ‘control’ is perhaps more generic and applies better to security situations.

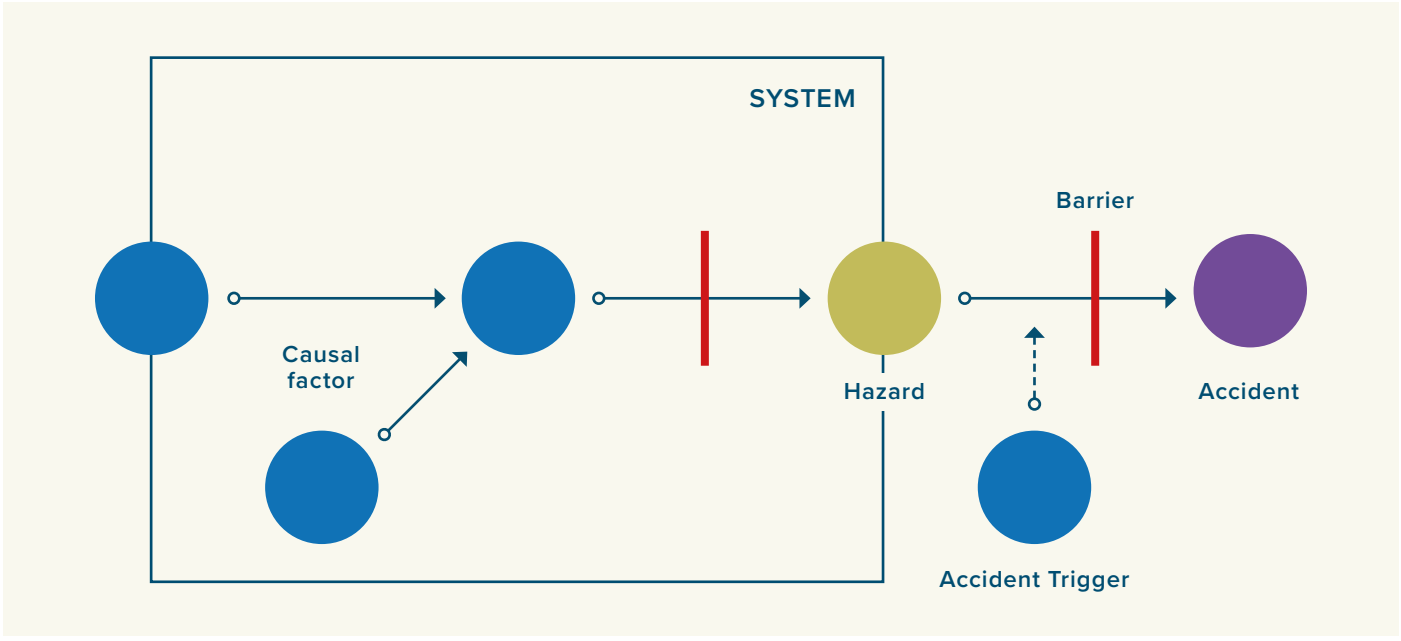


Figure 1: Schematic showing the relationship between causal factors, hazards and accidents

APPENDIX A
RISK ASSESSMENT

If security concerns are included in the safety analysis, we need to consider external threats that can exploit vulnerabilities within the system and compromise the system's functionality, leading to an unsafe system state. This is shown in Figure 2, where security controls are shown with a red vertical line.

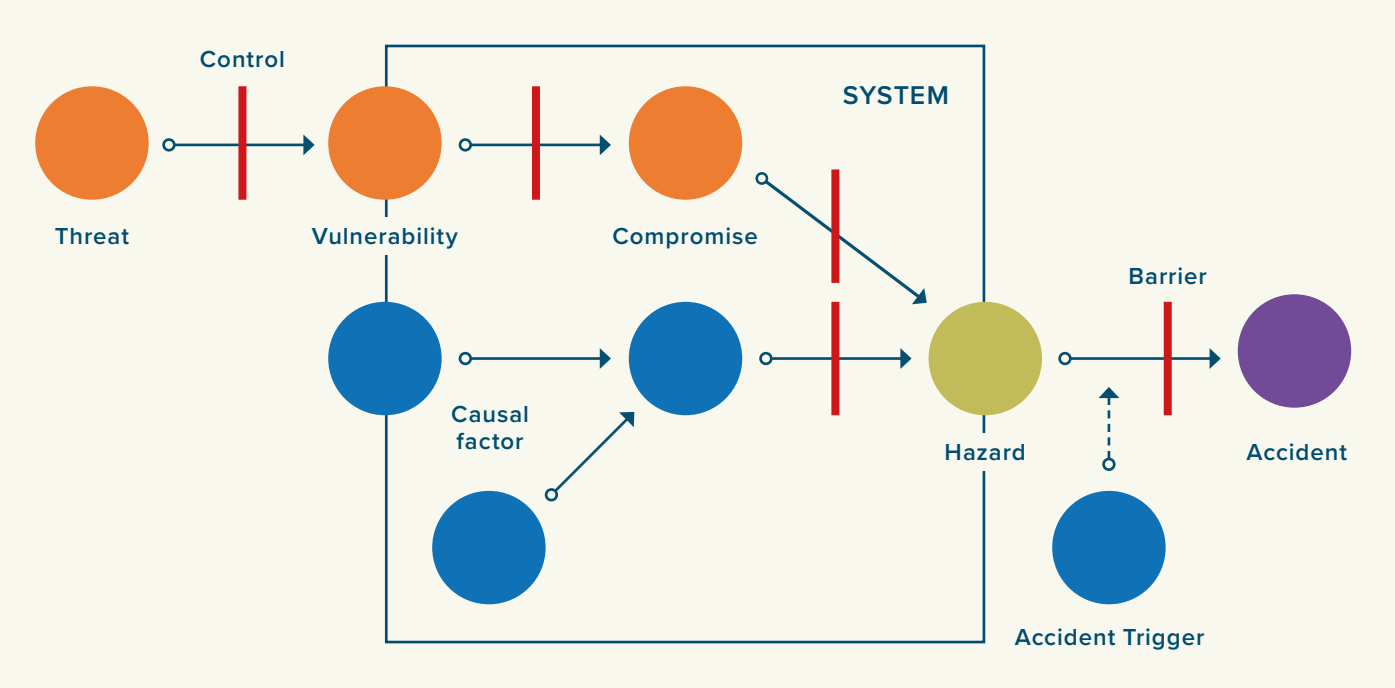


Figure 2: Extension of Figure 1 to include security

In addition, the analysis might take account of security controls outside the system boundary that limit the risk of attack, and additional controls might need to be implemented within the system. Typically, security threats do not create new hazards (i.e. new unsafe states) but do alter the likelihoods of the existing hazards, and can make hazards that were previously deemed incredible, plausible. Enhanced hazard identification techniques are being developed to take these issues into account (e.g. [1][2]).

IMPACT ON RISK ESTIMATION

Conventional safety analysis presumes a relatively stable environment, where the initiating events are well-understood and remain relatively unchanged over time.

Therefore, in principle, it is possible to perform a quantified risk assessment for a system with a high degree of confidence in its accuracy. Risk estimation in a safety context is based on factors such as:

- the frequency of the initiating event
- the impact of the event
- controls and mitigations for the event

However, in a security context, the types of attack are not necessarily known in advance and the likelihood and frequency of attack varies over time depending on the nature and number of attackers, discovery of vulnerabilities, and advances in attack technology.

APPENDIX A
RISK ASSESSMENT

Furthermore, some of the assumptions that safety engineers might make (for example, about the failure independence of redundant components or diverse 'defence-in-depth' barriers) are no longer guaranteed if these elements are all vulnerable to attack. Addressing these uncertainties requires a balance of qualitative and quantitative approaches. For example, a system might be designed to withstand attacks up to some qualitative capability level.

Meaningful discussions about the capabilities of attackers and the risk of an attack succeeding require a common vocabulary [3]. STIX (Structure Threat Information eXpression) is a language developed for cyber threat intelligence sharing that is emerging as a de facto standard. The STIX vocabulary for Threat Actor Sophistication [4] defines 7 levels of sophistication ranging from **None**, through **Minimal**, **Intermediate**, **Advanced**, **Expert**, and **Innovator**, to **Strategic**, as shown in the table below.

Level of sophistication	Description
None	Can carry out random acts of disruption or destruction by running tools they do not understand. Actors in this category have average computer skills. Example roles: Average User These actors: • cannot launch targeted attacks
Minimal	Can minimally use existing and frequently well-known and easy-to-find techniques and programs or scripts to search for and exploit weaknesses in other computers. Commonly referred to as a script-kiddie. These actors rely on others to develop the malicious tools, delivery mechanisms, and execution strategy and often do not fully understand the tools they are using or how they work. They also lack the ability to conduct their own reconnaissance and targeting research. Example roles: Script-Kiddie These actors: • attack known weaknesses; • use well-known scripts and tools; and • have minimal knowledge of the tools.

APPENDIX A
RISK ASSESSMENT

Level of sophistication	Description
Intermediate	Can proficiently use existing attack frameworks and toolkits to search for and exploit vulnerabilities in computers or systems. Actors in this category have computer skills equivalent to an IT professional and typically have a working knowledge of networks, operating systems, and possibly even defensive techniques and will typically exhibit some operational security. These actors rely on others to develop the malicious tools and delivery mechanisms, but are able to plan their own execution strategy. They are proficient in the tools they are using and how they work and can even make minimal modifications as needed. Example roles: Toolkit User These actors: • attack known vulnerabilities; • use attack frameworks and toolkits; and • have proficient knowledge of the tools.
Advanced	Can develop their own tools or scripts from publicly known vulnerabilities to target systems and users. Actors in this category are very adept at IT systems and have a background in software development along with a solid understanding of defensive techniques and operational security. These actors rely on others to find and identify weaknesses and vulnerabilities in systems, but are able to create their own tools, delivery mechanisms, and execution strategies. Example roles: Toolkit Developer These actors: • attack known vulnerabilities; • can create their own tools; and • have proficient knowledge of the tools.

APPENDIX A
RISK ASSESSMENT

Level of sophistication	Description
Expert	Can focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode rootkits, frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data. Actors in this category are very adept at IT systems and software development and are experts with security systems, defensive techniques, attack methods, and operational security. Example roles: Vulnerability Researcher, Reverse Engineer, Threat Researcher, Malware Creator. These actors: • attack unknown and known vulnerabilities; • can create their own tools from scratch; and • have proficient knowledge of the tools.
Innovator	Typically criminal or state actors who are organised, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits. Demonstrates sophisticated capability. An innovator has the ability to create and script unique programs and codes targeting virtually any form of technology. At this level, this actor has a deep knowledge of networks, operating systems, programming languages, firmware, and infrastructure topologies and will demonstrate operational security when conducting his activities. Innovators are largely responsible for the discovery of 0-day vulnerabilities and the development of new attack techniques. Example roles: Toolkit Innovator, 0-Day Exploit Author. These actors: • attack unknown and known vulnerabilities; • create attacks against 0-Day exploits from scratch; and • create new and innovative attacks and toolkits.
Strategic	State actors who create vulnerabilities through an active program to 'influence' commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest. These actors: • can create or use entire supply chains to launch an attack; • can create and design attacks for any systems, software package, or device; and • are responsible for APT-level attacks.

APPENDIX A
RISK ASSESSMENT

The sophistication of the attack, along with other factors such as motivation, might be taken into account to produce an overall estimate of the risk. A quantitative risk might be estimated for attacks up to a given level of sophistication. Attacks beyond that level (e.g. nation state attacks) might be presumed to be infeasible to prevent, and separate measures, such as resilience and incident management, might be needed to maintain safety in such circumstances.

Safety risk estimates that include security threats might also need to be more frequently updated than risk estimates for purely safety risks. The update could be prompted by developments such as the release of a tool enabling lower-capability agents to carry out attacks previously only within the reach of higher-capability agents.

IMPACT ON RISK TREATMENT

Even though there are inherent uncertainties associated with malicious attacks, the risks posed by such attacks still need to be tolerable. The identification of control measures needs to take account of a number of factors including:

- the level of uncertainty (which might be expressed qualitatively)
- what is proportionate (given the societal impact if the attack succeeds)
- the side effects of additional controls and complexity
- what recovery measures are needed (recognising that these could also be attacked)
- the impact of security considerations on the effectiveness of risk reduction measures

More generally, there is a need to take a more dynamic view of risk that ensures that new forms of attack can be recognised and responded to over the system lifetime.

ADDRESSING UNCERTAINTY

As noted by NCSC in its risk management guidance [5] [6], risk assessment has limitations. In particular, most methods fail to recognise the level of uncertainty inherent in the judgements made in the assessment, for example, regarding the completeness of the set of attacks or the effectiveness of countermeasures. It is therefore important to allow for these uncertainties, for example, by monitoring the performance of countermeasures and adapting to changes in the threat picture. It is also important to have a system architecture that is capable of being updated when new security problems are identified.

BIBLIOGRAPHY

[1] Fovino, I.N., Masera, M., De Cian, A., Integrating Cyber Attacks within Fault Trees. Reliability Engineering and System Safety. vol. 94, no. 9, pp. 1394–1402, 2009

[2] Steiner, M., Liggesmeyer, P., Combination of Safety and Security Analysis – Finding Security Problems that Threaten the Safety of a System. In: Workshop on Dependable Embedded and Cyber-physical Systems (DECS), pp. 1–8, 2013

[3] NCSC, Rating hackers, rating defences, blog post, September 2018 https://www.ncsc.gov.uk/blog-post/rating-hackers-rating-defences

[4] Oasis Open, STIX Version 2.1, Threat Actor Sophistication Vocabulary https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html

[5] NCSC, Risk management guidance, The fundamentals of risk, Version 1.0, September 2016 https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/fundamentals

[6] NCSC, Risk management guidance, Security governance, enabling sensible risk management decisions & communication, Version 1.0, September 2016 https://www.ncsc.gov.uk/collection/risk-management-collection/governance-cyber-risk/security-governance-enabling-sensible-risk-management-decisions-communication

APPENDIX B
ASSURANCE AND SAFETY CASES

INTRODUCTION

Systems can have a variety of safety roles: they can directly provide some form of protection, initiating a safety function (such as a braking system), they can indirectly support safety by providing an operator with information to make a safe decision, or they can provide a service that has to be delivered within a particular functional and performance envelope for the system to be safe. In all these situations, the system, service, component or operator needs to have sufficient and well-placed confidence that they will get the service required: the systems they depend on have to be both trusted and trustworthy.

In the safety area, safety cases are a well-known approach for describing whether a system is safe, how it might be hazardous and why that judgement can be trusted. Safety cases are the appropriate approach for dealing with systems whose failure can lead to danger. For subsystems and other services that have an indirect impact on safety, or for components of a safety-relevant system, there only needs to be confidence that the subsystem or service will meet its explicit or implicit requirements and will not have a negative effect on the safety of the overall system.

Assurance cases are a general approach to addressing the need for confidence in engineering decisions. An assurance case can be defined as

> *'a documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment' [1]*

In practice, assurance cases can be very complex and can include thousands of pages of documentation, diagrams, analyses, and tests. Therefore, summary reports (e.g. a safety case report) are provided that pull together the reasoning and the evidence.

STRUCTURING ASSURANCE CASES

An assurance case often starts from a top-level claim. The top-level claim states the overall intention for the assurance case. If the assurance case is developed to demonstrate some aspect of regulatory compliance, the top-level claim is often derived from the regulation the assurance case is trying to meet. For example, the top-level claim might be

> *"System X is safe"*

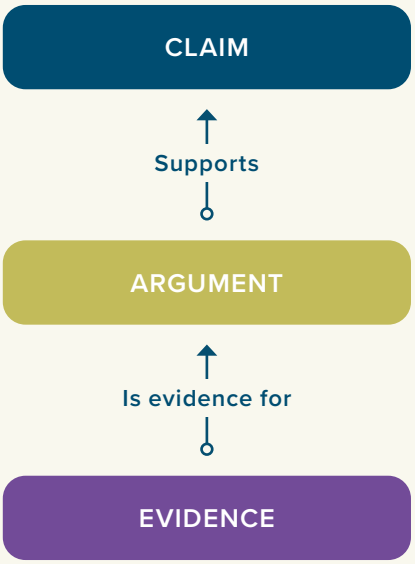
This claim needs to be fleshed out in the remainder of the case by providing the precise meaning of "safe" and details of the system context and environment.

Over the past decade, there has been a move to develop an explicit claim or goal-based approach to engineering justification, and considerable work has been done on the structuring of engineering arguments (e.g. [2][3][4]) and supporting standards (e.g. [5][6]). Current assurance case practice makes use of a basic approach that can be related to ideas originally developed by Toulmin [7] – claims are supported by evidence and an argument ('warrant') that links the evidence to the claim. There are variants of this basic approach that present the claim structure graphically such as Goal Structuring Notation (GSN) [2] or Claims, Arguments and Evidence (CAE) [3] (see Figure 3). These notations can be supported by tools [8][9] that can help to create and modify the claim structure and also assist in the tracking of evidence status, propagation of changes through the case, and handling of automatic links to other requirements and management tools. A rigorous analysis of assurance cases is provided in [10].

APPENDIX B
ASSURANCE AND SAFETY CASES

The key elements of the Claims, Argument, Evidence (CAE) approach are:

- Claims, which are assertions put forward for general acceptance. They are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called sub-claims.
- Arguments, which link the evidence to the claim. They are 'statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established' [7], together with the validation for the scientific and engineering laws used. In an engineering context, arguments should be explicit.
- Evidence, which is used as the basis for justifying the claim. Possible sources of evidence include the design, the development process, prior field experience, testing (including statistical testing), source code analysis or formal analysis.



In order to support the use of CAE, a graphical notation is used to describe the interrelationship of the claims, arguments and evidence.

Top-level claims such as "the system is adequately secure" are too vague or are not directly supported or refuted by evidence. It is therefore necessary to break claims down into sub-claims recursively until the sub-claims can be directly supported (or refuted) with evidence. The basic concepts of CAE are supported by an international standard [5] and industry guidance [3].

An empirical analysis of actual safety cases identified a number of basic building blocks (CAE blocks) that can be used to construct a well-structured safety justification [11]. These blocks are:

- **concretion blocks** – used where a claim needs further clarification, for example, because it is too vague or general.
- **substitution blocks** – used to substitute a claim about a property of a system with another claim that is easier to justify. For example, making a simpler conservative claim, or making a claim about a test system rather than the real system.
- **decomposition blocks** – very commonly used in a divide and conquer approach, where a claim about a system is decomposed into claims about constituent subsystems, or where a property is divided into sub-properties (e.g. security into confidentiality, availability and integrity, or hazards into different classes of hazards).
- **calculation blocks** – used to calculate a value associated with a claim from sub-claims.
- **evidence incorporation block** – used to make the link between a claim and its supporting evidence.

The resulting CAE argument structure outlines the argument that justifies the top-level claim, but needs to be supported by narrative and analyses that explain the arguments and sub-claims that justify the top-level claim. Narrative is an essential part of an assurance case.

Figure 3: The CAE framework

APPENDIX B
ASSURANCE AND SAFETY CASES

SAFETY CASES IN THE RAIL CONTEXT

EN 50129:2018 [12] defines the conditions that need to be satisfied in order for a safety-related electronic railway system/sub-system/equipment to be accepted as adequately safe for its intended application.

Three kinds of evidence are required:

- evidence of quality management
- evidence of safety management
- evidence of functional and technical safety

Evidence that these conditions have been satisfied is included in a structured safety justification document, known as the Safety Case. The Safety Case forms part of the overall documentary evidence that has to be submitted to the relevant safety authority in order to obtain safety approval for a generic product, a class of application or a specific application.

ADDRESSING SECURITY ISSUES

Although the GSN and CAE notations are very general-purpose and provide a framework for security assurance, there are two types of change that security issues bring to the fore. The first is the need to introduce more rigour into the reasoning of the cases to manage the wider scope of the claim. The development of CAE blocks addresses this to some extent [11], as do longer-term visions of automated reasoning support [9]. Increased rigour also brings with it the need for better approaches to structuring the detailed case – for example, the notion of a layered assurance approach that structures cases as a series of 'layers' covering requirements and policy, architecture, and implementation [13][14].

The provisions of this CoP provide a clear indication of the scope of the security content that is required in general. The CAE framework can be used to analyse the impact of security on existing safety assessments or safety cases and thus identify the significant changes needed to address security explicitly [14][15]. Incorporating security into the safety assessment impacts the design and implementation process as well as the approach to verification and validation.

In particular, the following issues need to be considered from a security perspective:

- Integration and interaction of requirements, e.g. of safety, with security and resilience supported by security-informed hazard analysis techniques.
- Supply-chain integrity, e.g. mitigating the risks of devices being supplied compromised or having egregious vulnerabilities.
- Post-deployment malicious events that will change in nature and scope as the threat environment changes and a corresponding need to consider prevention (e.g. implementing a risk-based patching policy) but also recovery and resilience.
- Reduced lifetime of installed equipment as there is a weakening of security controls as attackers' capabilities and technologies change.
- Threats to the effectiveness and independence of safety barriers and defence in depth.
- Design changes to address user interactions, training, configuration, and software vulnerabilities and patching. These might lead to additional functional requirements for security controls.
- Possible exploitation of the device/service to attack itself or other systems and the need for confidentiality of design and deployment information.
- The trustworthiness and provenance of the evidence offered.

BIBLIOGRAPHY

[1] P G Bishop, R E Bloomfield, S Guerra, The future of goal-based assurance cases. In Proceedings of Workshop on Assurance Cases. Supplemental Volume of the 2004 International Conference on Dependable Systems and Networks, pp. 390-395, Florence, Italy, June 2004 https://www.adelard.com/assets/files/docs/dsn2004v10.pdf

[2] T P Kelly, R A Weaver, The Goal Structuring Notation — A Safety Argument Notation, Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, July 2004 https://www-users.cs.york.ac.uk/~tpk/dsn2004.pdf

APPENDIX B
ASSURANCE AND SAFETY CASES

[3] [3] R E Bloomfield, P G Bishop, C C M Jones, P K D Froome, ASCAD—Adelard Safety Case Development Manual, 1998
https://www.adelard.com/resources/ascad.html

[4] [4] P G Bishop, R E Bloomfield, A Methodology for Safety Case Development. In: F Redmill, T Anderson, (eds.) Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-Critical Systems Symposium, Birmingham 1998, pp. 194–203. Springer, London, 1998
https://www.adelard.com/assets/files/docs/sss98web.pdf

[5] [5] ISO/IEC 15026-2:2011, Systems and software engineering — Systems and software assurance, Part 2: Assurance case, 2011

[6] [6] Safety Critical Systems Club, Assurance Case Working Group, SCSC-141C, Goal Structuring Notation Community Standard, Version 3, May 2021
https://scsc.uk/r141C:1

[7] [7] S E Toulmin, The Uses of Argument, Cambridge University Press, 1958

[8] [8] L Emmet, G Cleland, Graphical Notations, Narratives and Persuasion: A Pliant Systems Approach to Hypertext Tool Design, in Proceedings of ACM Hypertext 2002 (HT'02), College Park, Maryland, USA, June 11-15, 2002
https://www.adelard.com/assets/files/docs/ht2002_emmet_cleland_asce_paper.pdf

[9] [9] J Rushby, Mechanized support for assurance case argumentation, in Proc. 1st International Workshop on Argument for Agreement and Assurance (AAA 2013), Springer LNCS, 2013
http://www.csl.sri.com/users/rushby/papers/aaa13.pdf

[10] R Bloomfield and J Rushby, Assessing Confidence with Assurance 2.0, CSL Technical Report SRI-CSL-2022-02, June 2022
http://www.csl.sri.com/users/rushby/papers/confidence22.pdf

[11] R Bloomfield and J Rushby, Assessing Confidence with Assurance 2.0, CSL Technical Report SRI-CSL-2022-02, June 2022
http://www.csl.sri.com/users/rushby/papers/confidence22.pdf

[12] EN 50129:2018, Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling

[13] Delong, Compositional Certification, Lecture Notes. Real-Time Embedded Systems Forum, The Open Group (TOG) conference, Toronto, Canada (2009) and the Layered Assurance Workshop (LAW)

[14] K Netkachova, K Müller, M Paulitsch, R E Bloomfield, Investigation into a Layered Approach to Architecting Security-Informed Safety Cases, IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), Sept 2015, Prague, Czech Republic, DOI: 10.1109/DASC.2015.7311447
https://openaccess.city.ac.uk/id/eprint/12967/1/267netka_final.pdf

[15] R E Bloomfield, K Netkachova, R Stroud, Security-Informed Safety: If it's not secure, it's not safe. Paper presented at the 5th International Workshop on Software Engineering for Resilient Systems (SERENE 2013), 3rd - 4th October 2013, Kiev, Ukraine
https://www.adelard.com/assets/files/docs/Bloomfield_serene_2013.pdf

APPENDIX C
SYSTEM COMPOSITION

SECURITY AND SAFETY OF A COMPOSITE SYSTEM

Systems are nearly always developed by integrating components and subsystems purchased from a supply chain to form a new system. The term used to describe this is 'composition'. The challenge is to assure the safety and security of the overall system. It is not sufficient to assume that assurance of the component parts is enough to assure the safety and security of the overall system – a justification for the overall system is needed.

Sometimes the development of composite systems follows a formalised path, as described in EN 50129:2018 [1], which deals with the composition of equipment and subsystems to form a railway signalling system, but in other parts of the railway ecosystem, the development may be less formalised, for example, the integration of information and communication systems to provide a new service). Composition involving intangible assets such as information and data is also important, particularly when security issues such as confidentiality are considered. Although strict confidentiality concerns are outside the scope of the CoP, it should be borne in mind that threat agents can make use of information to identify vulnerabilities or otherwise aid attacks.

The structure of a composite system is defined by its architecture or design, which describes how the components are brought together to form the overall system. EN 50129 distinguishes between systems, sub-systems, and equipment:

- **system** – a set of sub-systems which interact according to a design
- **sub-system** – a portion of a system which fulfils a specialised function
- **equipment** – a functional physical item

The conditions for safety acceptance must be satisfied at each of these levels before a safety-related system can be accepted as adequately safe.

In particular, each safety case is only valid within a specified range of external influences (typically environmental conditions) that are defined by the systems requirements specification.

In addition, the safety case can specify a set of rules, conditions and constraints that must be observed in the application of the system/sub-system/equipment.

Composition of safety cases is allowed, providing it can be shown that the environmental conditions and any safety-related application conditions for the relevant system/sub-system/equipment are satisfied. If necessary, safety-related application conditions can be inherited by the parent safety case – for example, the safety-related application conditions for a system might include the safety-related application conditions for each of its sub-systems.

EN 50129 makes a distinction between a generic product and a configuration of that product for a particular application:

- **product** – a collection of elements, interconnected to form a system/sub-system/equipment, in a manner which meets the specified requirements
- **configuration** – the structuring and interconnection of the hardware and software of a system for its intended application

The standard distinguishes between three kinds of safety case:

- **generic product safety case** (independent of application) – a generic product can be re-used for different independent applications
- **generic application safety case** (for a class of application) – a generic application can be re-used for a class/type of application with common functions
- **specific application safety case** (for a specific application) – a specific application is used for only one particular installation

Each specific application of a generic safety case must show that the environmental conditions and context of use are compatible with the generic application conditions.

APPENDIX C
SYSTEM COMPOSITION

In addition, for specific applications of generic products, safety approval is needed for both the application design of the system and its physical implementation (including manufacture, installation and test, and facilities for operation and maintenance). For this reason, the safety case for specific applications is divided into two portions: the application design safety case, and the physical implementation safety case.

In the context of security-informed safety cases, it is worth noting that the security context is considered to be an external influence on a safety case. In particular, clause B.4.6 of EN 50129 discusses protection against unauthorised access. Similarly, safety-related application conditions cover topics such as configuration, operation and maintenance, and monitoring and decommissioning, all of which have security implications as well as safety implications.

THE BEHAVIOUR OF A COMPOSITE SYSTEM

The attributes of a composite system are related to the attributes of its component systems, but the relationship is not necessarily straightforward.

For example, the composite system might:

- share some of the attributes of its component systems
- have additional attributes due to emergent behaviour
- mitigate unwanted behaviour caused by vulnerabilities in its component systems

In order to assess whether the composite system has the desired properties in a security context, it is necessary to consider:

- initiating events (or attacks)
- vulnerabilities
- potential faults and error conditions
- hazards
- failures or consequences
- controls, mitigations or barriers

The impact of each of these considerations on the security of the combined system is elaborated in Table 3.

Composition question	Security-related example
What is the impact of composition on the frequency and nature of attacks?	• Does an increase in the attack surface or the aggregation of assets, including intangible assets such as information, lead to the system being easier to attack and a more attractive target?
What are the combined vulnerabilities of the systems?	• Does a vulnerability that might be benign in one component allow the exploitation of another component? • Does the combined system include mechanisms to limit the impact of vulnerabilities in individual components?
What is the impact of composition on faults of the overall system?	• Would the reliability of the system be impacted adversely by the unreliability of a security control?

APPENDIX C
SYSTEM COMPOSITION

Composition question	Security-related example
What is the impact of composition on the nature and consequences of the hazards?	• Would a security attack or compromise make some hazards more credible or increase the consequences of an accident?
What is the impact of composition on controls, barriers and mitigations?	• Are the controls in the different components compatible or do they interact in an unfortunate way? • Does security make any independence or common mode failure assumptions invalid? • Are there covert channels between the components? • Are there common vulnerabilities across the components that increase the chance of a common mode failure?
What is the impact on recovery?	• How would an attack on the recovery mechanisms and communication mechanisms impact recovery and resilience? • Are the mechanisms compatible?

Table 3: Composition questions

A rigorous approach to assuring a composite system would need to address each of these questions.

SUMMARY

Security adds complexity to the challenge of assuring a composite system. While many aspects are similar to the safety perspective, a potentially significant difference is that knowledge that a system could be used as a component in a composite system might change the threat profile for that component. Additionally, the techniques needed to address vulnerabilities and their interactions in a composite system might be different to the techniques needed to address safety hazards. The derivation of integrity levels might also be significantly impacted by security issues.

BIBLIOGRAPHY

[1] EN 50129:2018, Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling

APPENDIX D
INTERACTIONS BETWEEN SAFETY AND SECURITY

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
- overlapping functionality
- the use of shared resources or platforms
- information flow
- misuse or abuse

In general, these safety and security interactions might present the opportunity to make decisions that could result in trade-offs between safety and security. In some cases, they could result in direct conflicts between safety and security that cannot easily be resolved. For example, consider an access system that remains in a locked state if it fails. Such a system is fail-secure, in that an attacker cannot gain access, but is not fail-safe, in that personnel cannot escape in the event of a fire. The interactions between a security policy and the safety requirements need to be assessed and any trade-offs identified. In some circumstances, increased security might reduce safety, so it is essential to consider the trade-offs holistically.

For safety, the most important considerations are ensuring that systems provide the required functionality with a given level of reliability, integrity and availability. When the security perspective is included, confidentiality also becomes a concern. In this CoP we have recommended measures to protect the confidentiality of information that could be used by a threat agent to identify vulnerabilities and facilitate an attack. The privacy of individuals is outside the scope of the CoP, but there might be situations in which personal data could be used to inform an attack, or where the disclosure of sensitive data leads to non-physical harm.

Figure 4, which is taken and generalised 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 show that these constraints are acceptably safe even if they do cause higher workload or operational complexities.
- **top left corner** – this is a contrasting area in which safety issues dominate and the security policy is the same or weakened. In this case, the security analysis must show that the identified security threats are satisfactorily mitigated by other means.
- **top right corner** – this is a very uncertain area where some special capabilities might be needed, for example, a manual override of security policy.

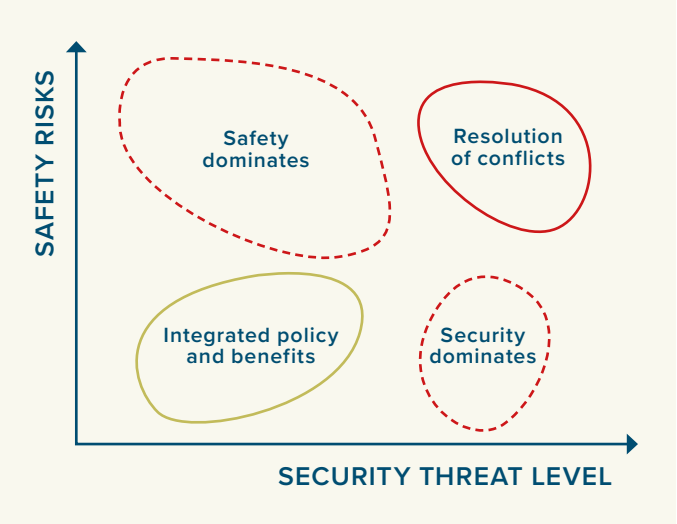


Figure 4: A schematic showing how security and safety interact in different scenarios

APPENDIX D
INTERACTIONS BETWEEN SAFETY AND SECURITY

An organisation has a clear legal and ethical responsibility to deliver a safe product or service. This CoP also articulates a responsibility to enable safe behaviour in others and to promote the safety and security of the ecosystem as a whole.

Therefore, despite the complexities that consideration of security brings, safety responsibilities and requirements are not to be diluted.

Instead, the organisational, technical and resourcing advantages that security brings should be recognised and encouraged.

EXAMPLES OF SPECIFIC ACTIONS

Table 4 highlights some specific areas where actions can be taken to minimise the need to trade-off safety and security.

Topic	Actions
Security policy, organisation and culture	• Address confidentiality conflicts, so that safety is not compromised by the withholding of relevant information on security grounds ('need to know') and put in place appropriate information-sharing. • Make suitably competent and experienced security people available for integrated hazard analysis, taking into account competing resource needs.
Security-aware lifecycle	• Analyse requirements early on for policy interactions between safety and security. • Explicitly address uncertainties in the likelihood of attacks in risk assessments. • Recognise and encourage the safety benefit from building in security (e.g. greater use of static analysis, high integrity coding practices).
Maintaining effective defences	• Balance the relative risks and benefits of timely intervention with respect to patching and system modification. • Ensure sufficient resources are available to review and where necessary update safety assurance cases, particularly so that security patches or updates are not unduly delayed.
Incident management	• Ensure that the primary aim of incident management is to maintain safety, while also ensuring that other aims, such as cost and availability are also adequately considered. • Identify requirements to support incident management at the design stage. This will enable the system to deliver the safety benefit with a high level of security. For example, consider using an integrated forensics capability to capture both security- and safety-related events.

APPENDIX D
INTERACTIONS BETWEEN SAFETY AND SECURITY

Topic	Actions
Secure and safe design	• Take into account the increased attack surface when calculating the net safety gain from redundant systems. Once security is taken into account, the safety gain might be reduced or minimal. • Define information flow policies to enable maximum use of information when the system is under stress. • Ensure that security measures (such as forensic recording) that might impose an additional burden on the system's resources do not increase the risk of unsafe failure.
Contributing to a safe and secure world	• Ensure that securing a product does not lead to safety issues for others in the ecosystem, e.g. by restricting recovery, information flows.

Table 4: Examples of specific actions

In expressing the need to prioritise safety, we have conveniently ignored the question of scope: safe for whom? An action to increase the safety of one system might pose or increase a (safety) hazard or a (security) threat to another. For example, consider a system in a train that automatically calls the emergency services if a crash is detected. Making the thresholds and barriers to activating such a system as low as possible provides the greatest assurance that help will be called in the event of a train crash, but might also enable flooding or denial-of-service attacks on the emergency system, which would be detrimental to the safety of the ecosystem as a whole. Conversely, increasing security controls by, for example, blacklisting unknown sources of calls, could increase the chance that a valid call is rejected.

Such a situation requires resilience to be considered. Resilience is a property that describes the ability to change and adapt, and applies both to individual products, systems and services as well as to the ecosystem as a whole. Examples of resilience include the preparation of fall-back modes of operation or a plan to adapt to and recover from, unforeseen circumstances.

BIBLIOGRAPHY

[1] K Netkachova, K Müller, M Paulitsch, R E Bloomfield, Investigation into a Layered Approach to Architecting Security-Informed Safety Cases, IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), Sept 2015, Prague, Czech Republic, DOI: 10.1109/DASC.2015.7311447 https://openaccess.city.ac.uk/id/eprint/12967/

APPENDIX E
NETWORK SECURITY

INTRODUCTION

This appendix reviews the railway signalling requirements for safe communication over a network from a security perspective, and considers what additional issues would need to be covered by a security analysis. We start by summarising the basic requirements for safe communication in EN 50159 [1], which are expressed in terms of potential threats to messages sent over the network and possible defences against those threats. The standard distinguishes between different categories of network, which pose different threats to safe communication and therefore require different defences. We examine the issue of network categorisation from a security perspective and discuss how it might be challenged, thereby identifying additional claims, arguments and evidence that would need to form part of a security-informed safety case.

REQUIREMENTS FOR SAFE COMMUNICATION

EN 50159 defines the requirements for safe communication between safety-related systems over a network. The network is not required to have any safety properties, so it is necessary to show that end-to-end communication is safe, despite various threats to messages sent over the network.

The standard identifies the following basic message errors as potential threats:

- repeated message
- inserted message
- deleted message
- re-sequenced message
- corrupted message
- delayed message
- masqueraded message

Each of these threats could be caused by one or more hazardous events, including random and systematic hardware and software failures, as well as deliberate attacks.

In order to reduce the risks posed by these threats, the standard requires the following safety services to be considered:

- message authenticity
- message integrity
- message timeliness
- message sequence

The standard identifies a number of standard defences against the message threats that can be used to provide these services and specifies the requirements for each defence:

- sequence number
- time stamp
- timeout
- source and destination identifiers
- feed-back message
- identification procedure
- safety code
- cryptographic techniques

The defences that are required depend on the characteristics of the network and the likelihood of the various threats. The standard identifies three kinds of network, which are distinguished according to whether the network is open or closed, and whether the risk of unauthorised access is considered to be negligible or not. A closed network is defined as a network that is completely under the control of the designer with a fixed or maximum number of participants and known properties, whereas an open network has unknown characteristics and is potentially shared with other users. Open networks are susceptible to unauthorised access, but depending on the characteristics of the particular network, it may be possible to consider the risk of unauthorised access to be negligible. Thus, the three categories of network are:

- **Category 1** – closed network
- **Category 2** – open network, negligible risk of unauthorised access
- **Category 3** – open network, significant opportunity for unauthorised access

APPENDIX E
NETWORK SECURITY

Safe communication over Category 3 networks requires the use of cryptographic techniques to guard against the possibility of malicious attacks, in particular, masqueraded messages.

SECURITY CONSIDERATIONS

The threats to safe communication depend on the nature of the network used to transmit messages. If an argument can be made that the risk of unauthorised access to the network is negligible, then the standard allows masquerade errors to be ignored, which means that there is no need to use cryptographic techniques to protect messages in transmission. Thus, it is important to challenge the assumptions that underpin such an argument from a security perspective to ensure that they are justified.

OPEN OR CLOSED NETWORK?

The distinction between an open and closed network is very significant. A closed network has a fixed number of participants and known properties. This means that the only way to compromise the network is to compromise one of its end points. Otherwise, it is not possible to gain access to the network and send false messages that appear to come from a genuine end point. In other words, a closed network is not susceptible to masquerade attacks.

Very few kinds of network are truly closed in this sense. Table B.1 in Annex B of EN 50159 suggests three examples of a closed network:

1. Close ‘air gap’ transmission (e.g. between track balise and train antenna)
2. Proprietary serial bus internal to the safety-related equipment
3. Industry-standard LAN connecting different equipment (safety-related and non-safety-related) within a single system, subject to fulfilment and maintenance of the preconditions

The air gap between the track and the train can reasonably be treated as a closed network providing the train antenna is focused on the track and shielded against signals from elsewhere[1]. However, if it is possible for the train antenna to pick up balise transmissions from sources other than the track, for example, a false balise onboard the train, the network would extend beyond the air gap and could no longer be considered to be closed.

A proprietary serial bus that is internal to the safety-related equipment is also a reasonable example of a closed network. For example, a dedicated internal bus might be used in a SIL 4 system to allow processors to vote on the outcome of each operation. An attacker would not be able to gain access to this bus without dismantling the equipment and any attempt to tamper with the bus is likely to be detected by error-checking mechanisms built into the SIL 4 system.

In contrast, the use of an industry-standard LAN to connect different equipment (safety-related and non-safety-related) within a single system is more problematic for two reasons: firstly, non-safety-related equipment could potentially be compromised and used as a platform for attacking safety-related equipment, and secondly, in order for the closed network assumption to remain valid, the LAN must remain isolated throughout the lifetime of the system.

The first issue can be avoided by not allowing non-safety-related equipment to connect to a LAN that is used to support safe communication between safety-related equipment. Otherwise, non-safety-related equipment should be regarded as untrustworthy and the safety case should demonstrate that the safety of the system cannot be affected by the misbehaviour of the non-safety-related equipment, including the possibility of the non-safety-related equipment sending forged safety-related messages over the network (i.e. masquerade attacks).

The second issue requires the safety case to impose conditions on the operation, maintenance and upgrade of the system to ensure that the LAN remains isolated, and is never connected to other systems or networks. Any change to the network architecture or network configuration could potentially invalidate this assumption. Thus, access ports on switches and routers need to be locked down and ideally, some form of network access control should be used to only allow connections from authenticated devices. This could be problematic from a maintenance perspective.

[1] Note that although the air gap can be classified as a closed network, the network could still be compromised if an endpoint was not trustworthy, for example, if a false balise was placed on the track.

APPENDIX E
NETWORK SECURITY

Otherwise, without strong guarantees about the validity of the closed network assumption, it would be more appropriate to consider a LAN to be an open network from a security perspective.

RISK OF UNAUTHORISED ACCESS

Open networks do not necessarily allow unauthorised access. EN 50159 makes a distinction between Category 2 networks, which are open but have a negligible risk of an unauthorised access, and Category 3 networks, which are open and have a significant risk of an unauthorised access. Again, any claims that a network is Category 2 rather than Category 3 need to be challenged from a security perspective to ensure that the claim is valid.

EN 50159 provides several examples of Category 2 networks, including:

1. Industry-standard LAN connecting several different systems within a controlled and limited area
2. WAN belonging to the railway, connecting different systems at various locations
3. Leased point-to-point circuit in public telecoms network

In each case, it is possible to limit the possibility of unauthorised access using appropriate controls, but these controls would need to be considered as part of a security-informed safety case. For example, a LAN in a data centre would be protected by physical and personnel controls – physical controls would prevent unauthorised access to the data centre, and personnel controls would ensure that those who had access to the data centre were trustworthy.

A claim that the risk of unauthorised access to a WAN was negligible would require more justification. The claim would depend on details of how the network was managed, how it was accessed, and what access it allowed to other networks. It is likely that access to a railway WAN would be offered as a managed service with various quality-of-service guarantees, which would need to be supported by a separate assurance case. A particular concern might be about personnel security – unlike a LAN in a data centre, a WAN belonging to the railway is potentially accessible to anyone working in the railway industry.

Again, without strong guarantees about controls preventing unauthorised access, it might be more appropriate to consider a WAN to be a Category 3 network.

ABUSE OF TRUST

The various defences suggested in EN 50159 are intended to protect safety-related messages from the various threats posed by an untrusted network that provides little or no safety guarantees. In particular, the standard is intended to guarantee the authenticity and integrity of messages. However, it is important to realise that these guarantees are only provided with respect to threats posed by the network – in particular, the standard does not provide any protection against intentional or unintentional misuse from authorised sources. In other words, the standard does not deal with 'abuse of trust' – false messages generated by an authorised and therefore trusted source that has either been compromised or is untrustworthy.

This caveat is stated explicitly in the second paragraph of clause 5:

> *'[...] meeting the requirements of this standard does not give protection against intentional or unintentional misuse coming from authorised sources. It is necessary for the safety case to address these aspects'.*

One consequence of this is that it is important to ensure that trusted components are trustworthy and cannot be compromised. This is particularly important for components that are connected to multiple networks – it is important to ensure that the component is robust against attacks via the more open network to prevent the attack from spreading into the more closed network.

ADDITIONAL DEFENCES

A system that is designed under a closed network assumption will only remain safe as long as that assumption is valid. If an attacker is able to gain access to the network, the network is no longer safe. Hence, it would be desirable from both a safety and a security perspective to include some additional defences so that the system is more resilient to attack.

For example, network monitoring can be used to detect the presence of unauthorised activity on a network and raise an alert. This provides some insurance against the risk that a closed network assumption turns out to be invalid.

APPENDIX E
NETWORK SECURITY

Similarly, the use of authentication and encryption protocols for safety-related messages would ensure that an intruder who gained access to the network would not be able to compromise the safety of the system without compromising the additional security protocols.

It is important to ensure that any additional security mechanisms do not interfere with the safe operation of the system. This poses an interesting dilemma – does the security mechanism form part of the safety system? In principle, the presence of the security mechanism should have no impact on the safety system, but if the purpose of the security mechanism is to guarantee certain properties that the safety system depends on, then it is arguably part of the safety system.

DISCUSSION

In order to design a safe communication system, it is necessary to consider the possible threats to safe communication. The possibility of an attacker gaining unauthorised access to the network is a significant threat that requires significant countermeasures based on cryptographic techniques, but if it can be shown that this risk is negligible, there is no need for such countermeasures, which can impose a significant overhead.

A security-informed safety case will need to examine the justification for categorising the network in detail. What security controls are used to protect the network from unauthorised access? What happens if an attacker gains access to the network? Are there any security controls to detect unauthorised access? Does the system continue to operate safely even though the network has been compromised?

An additional consideration is that all the devices attached to a trusted network are effectively trusted and must therefore be trustworthy. In particular, a compromised device would be authorised to send safety-related messages over the network, and additional controls would be needed at the application level to detect malicious or false messages, which would not be prevented by controls at the network level.

There is a number of other security issues that need to be considered as part of the design of safe communication protocols, such as key management, confidentiality and availability, but for the purposes of this appendix, we have focused on the issue of how a network is categorised by EN 50159, and whether this categorisation is justified.

BIBLIOGRAPHY

[1] EN 50159:2010+A1:2020, Railway applications — Communication, signalling and processing systems — Safety-related communication in transmission systems

APPENDIX F
SECURE CODING STANDARDS

INTRODUCTION

Software safety standards such as EN 61508-3 [1] and EN 50128 [2] require all safety-related software to be developed in accordance with a suitable coding standard. One of the reasons for using a coding standard is to avoid the use of unsafe programming language features. According to PD ISO/IEC TR 24772-1:2019 [3] which provides guidance on avoiding vulnerabilities in programming languages:

> *'All programming languages contain constructs that are incompletely specified, exhibit undefined behaviour, are implementation-dependent, or are difficult to use correctly. The use of those constructs may therefore give rise to vulnerabilities, as a result of which, software programs can execute differently than intended by the writer. In some cases, these vulnerabilities can compromise the safety of a system or be exploited by attackers to compromise the security or privacy of a system'.*

Many security vulnerabilities are the result of software defects. This has resulted in the emergence of secure software development as a discipline. The aim is to develop software that is free from security defects, and a broad consensus has developed around a set of common principles and practices that span the entire software engineering lifecycle.

Coding is only one part of the lifecycle, but empirical evidence suggests that approximately 50% of software defects are caused by coding bugs that can be eliminated by the use of secure coding practices [4]. The remaining defects are caused by architectural or design flaws that are more difficult to fix.

Coding bugs are a particular problem in 'unsafe' programming languages such as C and C++ that do not protect against simple kinds of attack such as 'buffer overflow'. Programs written using languages such as Java or Ada are less likely to contain coding bugs but are still susceptible to security defects caused by design flaws.

A number of standards and guidelines for secure coding in C and C++ have been developed, three of which are described in this appendix.

PD ISO/IEC TS 17961

PD ISO/IEC TS 17961 [1] proposes a set of secure coding rules for C. The rules are designed to provide a check against a set of programming flaws that are known from practical experience to have led to vulnerabilities. All of the rules are designed to be enforceable by static analysis. The current edition of the standard (as of publication) contains 46 secure coding rules that cover a broad range of topics, including pointers, arrays, integer arithmetic, dynamic memory allocation, signal handling, error codes, and input/output. However, unlike other standards, no attempt is made to organise these rules into categories that relate to particular classes of vulnerability.

An unusual but important aspect of the standard is that it deals with a concept called 'taint analysis'. The idea is that input data should be considered 'tainted' until it has been 'sanitised', and this leads to a series of rules that are designed to limit the spread of tainted data throughout the program. Such rules effectively impose constraints on data flow within the program.

SAFECODE

The Software Assurance Forum for Excellence in Code (SAFECode) has published a guide to fundamental secure software development practices that have been shown to be effective in practice [1]. These cover design, coding and testing – in particular, eight secure coding practices are identified:

- minimise use of unsafe string and buffer functions
- validate input and output to mitigate common vulnerabilities
- use robust integer operations for dynamic memory allocations and array offsets
- use anti-cross site scripting (XSS) libraries
- use canonical data formats
- avoid string concatenation for dynamic SQL statements
- eliminate weak cryptography
- use logging and tracing

APPENDIX F
SECURE CODING STANDARDS

MISRA C

The Motor Industry Software Reliability Association (MISRA) publishes a set of guidelines for the use of the C language in critical systems, popularly known as MISRA C. The most recent edition of these guidelines was published in February 2019 [7].

The publication of PD ISO/IEC TS 17961 led to a discussion within the MISRA C community about the extent to which MISRA C could be used as both a safe coding standard and a secure coding standard [8]. A detailed comparison of the two standards resulted in the publication of a security amendment for MISRA C [9], but demonstrated that the existing MISRA standard already provided good coverage of most of the secure coding rules in PD ISO/IEC TS 17961 (see [10]). The security amendment was subsequently incorporated into the February 2019 update to the MISRA C guidelines.

DISCUSSION

There is considerable overlap between safe coding standards such as MISRA C and secure coding standards such as PD ISO/IEC TS 17961. Both are concerned with preventing common mistakes that could result in runtime errors or undefined behaviour. However, the focus of safety standards and security standards is slightly different. Safe coding standards are concerned with producing high quality code whereas secure coding standards are concerned with producing code that is free from particular coding bugs. Both aim to reduce the likelihood of coding errors that could result in unsafe/insecure code, but neither guarantees functional correctness.

In principle, software designed to meet safety requirements should validate all inputs and therefore not be vulnerable to attack, but this depends on the extent to which the safety requirements anticipate the possibility of deliberately malicious inputs that are designed to exploit weaknesses in the input validation. For this reason, it is perhaps significant that the security amendment to MISRA C includes an explicit directive that requires external inputs to be checked for validity:

> ***Directive 4.14*** *– The validity of values received from external sources shall be checked.*

This implies that the requirements of MISRA C are not adequately secure without this addition.

The introduction to PD ISO/IEC TS 17961 contains some interesting observations about secure programming guidelines and security-critical systems:

> *'The largest underserved market in security is ordinary, non-security-critical code. The security-critical nature of code depends on its purpose rather than its environment. [...] There are already standards that address safety-critical code and therefore security-critical code. The problem is that because they must focus on preventing they are required to be so strict that most people outside the safety-critical community do not want to use them. This leaves ordinary code [...] unprotected'.*

It is clear from the more general secure coding guidelines published by SAFECode that several classes of security vulnerability are application-specific and therefore fall outside the scope of general-purpose guidelines for safe/secure coding like MISRA C and PD ISO/IEC TS 17961. Although security vulnerabilities in web applications might appear to have little relevance to safety-critical software, this depends on the nature of the interface between the safety system and external systems, so it is important for the designers of safety critical systems to be aware of these kinds of vulnerability.

One of the requirements of EN 61508-3 [1] is to ensure that there is an adequate separation between safety-related code and non-safety-related code on the same system. In order to demonstrate non-interference between software elements on the same computer, it is necessary to consider the possibility of a security vulnerability in a non-safety function being used to compromise the platform and hence its safety-critical functions.

Finally, although safe communication protocols over open networks require the use of cryptographic protocols to ensure the authenticity of messages, safe coding standards provide little or no guidance on the choice of cryptographic algorithms and technologies. This is a specialised area that requires expert knowledge and the use of proprietary algorithms and implementations is actively discouraged. Instead, best practice is to build safety-critical systems using standard protocols and technologies that are known to be secure, ideally using approved cryptographic hardware and software.

APPENDIX F
SECURE CODING STANDARDS

BIBLIOGRAPHY

[1] EN 61508-3:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements, May 2010

[2] EN 50128:2011+A2:2020, Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems

[3] PD ISO/IEC TR 24772-1:2019, Information Technology — Programming Languages — Guidance to avoiding vulnerabilities in programming languages – Part 1: Language-independent guidance

[4] Gary McGraw, Software Security – Building Security In, Addison-Wesley, 2006

[5] PD ISO/IEC TS 17961:2013, Information technology — Programming languages, their environments & system software interfaces — C Secure Coding Rules. ISO/IEC, Geneva, Switzerland, November 2013

[6] SAFECode, Fundamental practices for secure software development, Third edition, March 2018 https://safecode.org/uncategorized/fundamental-practices-secure-software-development/

[7] MISRA C:2012, Guidelines for the use of the C language in critical systems, Third edition, first revision, February 2019

[8] Roberto Bagnara, MISRA C, For Security's Sake! 14th workshop on automotive software and systems, Milan, November 2016 https://arxiv.org/abs/1705.03517

[9] MISRA C:2012 Amendment 1, Additional security guidelines for MISRA C:2012, April 2016

[10] MISRA C:2012 Addendum 2, Coverage of MISRA C:2012 against ISO/IEC TS 17961:2013 "C Secure", April 2016

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

IET – CODE OF PRACTICE ON CYBER SECURITY AND SAFETY

The IET Code of Practice on Cyber Security and Safety is written for safety and cyber security professionals and their managers. It argues that safety and cyber security are mostly complementary risk-based approaches and sets out some shared principles, and recommended practices, based on a systems engineering approach.

The shared principles are divided into management principles and technical principles, and the recommended practices are comparable to Section 1 and Section 2 of the Rail Code of Practice, which cover Security Policy, Organisation, and Culture, and Lifecycle Considerations respectively.

The correspondence between the IET Code of Practice and the Rail Code of Practice is shown in Table 5.

IET Code of Practice		Rail Code of Practice
MANAGEMENT PRINCIPLES	**1. Accountability for safety and security of an organisation's operations is held at board level**	1.2 Responsibility and accountability
	2. The organisation's governance of safety, security and their interaction is defined	1.1 Policies and processes
	3. Demonstrably effective management systems are in place	1.1 Policies and processes
	4. The level of independence in assurance is proportionate to the potential harm	1.3 Risk management
	5. The organisation promotes an open/ learning culture while maintaining appropriate confidentiality	1.8 Culture and communication 1.9 Protection of information
	6. Organisations are demonstrably competent to undertake activities that are critical to achieving safety and security objectives	1.7 Security awareness and competency
	7. The organisation manages its supply chain to support the assurance of safety and security in accordance with its overarching safety/security strategy	1.6 Supply chain and other external dependencies 2.5 Supply chain

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

IET Code of Practice		Rail Code of Practice
TECHNICAL PRINCIPLES	**8. The scope of the system-of-interest, including its boundaries and interfaces is defined**	2.2 Risk assessment and requirements definition
	9. Safety and security are addressed as coordinated views of the integrated systems engineering process	2.1 General requirements
	10. The resources expended in safety and security risk management, and the required integrity and resilience characteristics, are proportionate to the potential harm	2.7 Demonstration of security
	11. Safety and security assessments are used to inform each other and provide a coherent solution	2.2 Risk assessment and requirements definition
	12. The risks associated with the system-of-interest are identified by considerations including safety and security	2.2 Risk assessment and requirements definition
	13. System architectures are resilient to faults and attacks	2.3 Design 5. Secure and safe design
	14. The risk justification demonstrates that the safety and security risks have been reduced to an acceptable level	2.8 Assurance
	15. The safety and security considerations are applied and maintained throughout the life of the system	2.9 Operation, maintenance and decommissioning 3. Maintaining effective defences 4. Incident response

Table 5: Comparison between IET Code of Practice and Rail Code of Practice

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

The IET Code of Practice provides general guidance on the interaction between cyber security and functional safety. Unlike the Rail Code of Practice, it is not specific to any particular industry sector, but considers safety-related operational technology in general. The principles and recommended practices are presented at a high level, and the IET Code of Practice does not have the depth of the Rail Code of Practice, which includes detailed chapters on secure and safe design, maintaining effective defences, and incident response. However, it includes some useful background material, including an introduction to safety, security and systems engineering, and a discussion of challenges at the intersection of safety and security.

DFT – RAIL CYBER SECURITY GUIDANCE

The DfT Rail Cyber Security Guidance is organised as three main chapters, which are summarised in Table 6.

Chapter	Topics covered
1. Overview	Role of government Using the guidance The threats Resilience
2. Protecting infrastructure and rolling-stock systems	Risk assessment and management Principles for effective cyber security Concepts for effective cyber security Designing in security Protecting against attacks on new and current systems
3. Handling incidents and threats	Overview A rise in threat level or unexpected attack Contingency in the event of a cyber attack Clear up and recovery

Table 6: Contents of DfT rail cyber security guidance

The DfT guidance document is designed to be high-level. It sets out the principles and general approach to cyber security as good practice, but does not provide detailed instruction and is not intended to be used as a code of practice.

The first chapter of the DfT guidance contains a general discussion of why cyber attack poses a threat to the rail network and how government can support industry, including an explanation of how the guidance is intended to be used. The second chapter outlines a general approach to cyber security as good practice and the third chapter discusses the National Cyber Security Incident Management Policy (NCSIMP) and the Cyber Incident Coordination Plan (CICP).

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

For the purposes of comparison, the second chapter of the DfT guidance is most relevant. Table 7 illustrates the relationship between the general approach to cyber security outlined in the DfT guidance, and the detailed recommendations in the code of practice.

DfT guidance		Rail Code of Practice	
Section	**Topic**	**Section**	**Topic**
RISK ASSESSMENT AND MANAGEMENT	**Governance**	**1. Security policy, organisation and culture**	1.2 Responsibility and accountability
	Cyber security in rail systems	**2. Lifecycle considerations**	2.1 General requirements
	Legacy/current and whole life-cycle systems	**2. Lifecycle considerations**	2.2 Risk assessment and requirements definition
		3. Maintaining effective defences	3.1 Legacy systems 3.3 Secure operation, maintenance, and decommissioning
	Third-party systems	**1. Security policy, organisation and culture**	1.5 Supply chain and other external dependencies
	Review and future-proofing	**3. Maintaining effective defences**	3.10 Continuing risk management
	Communication and co-operation	**6. Contributing to a safe and secure world**	6.4 Collaboration
	Interfaces	**5. Secure and safe design**	5.10 Protection of communications 5.12 External services and devices

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

DfT guidance		Rail Code of Practice	
Section	**Topic**	**Section**	**Topic**
PRINCIPLES FOR EFFECTIVE CYBER SECURITY	**'If it's not secure, it is unlikely to be safe'**	**1. Security policy, organisation and culture**	1.3 Risk management
	Proportionate response	**2. Lifecycle considerations**	2.1 General requirements
	Goal-based security	**1. Security policy, organisation and culture**	1.1 Policies and processes
	Designed-in security	**2. Lifecycle considerations**	2.2 Risk assessment and requirements definition 2.3 Design
	Saltzer & Schroeder's principles	**5. Secure and safe design**	5.2 Secure design principles
CONCEPTS FOR EFFECTIVE CYBER SECURITY	**Holistic security**	**1. Security policy, organisation and culture**	1.3 Risk management
	Defence in depth	**5. Secure and safe design**	5.5 Defence in depth
	Protect, detect, respond	**3. Maintaining effective defences**	3.2 Protect, detect, respond
		4. Incident management	4.2 Detection of security issues 4.4 Response
	Technical, procedural and managerial protection measures	**1. Security policy, organisation and culture**	1.1 Policies and processes 1.2 Responsibility and accountability 1.6 Security awareness and competency 1.7 Culture and communication

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

DfT guidance		Rail Code of Practice	
Section	**Topic**	**Section**	**Topic**
CONCEPTS FOR EFFECTIVE CYBER SECURITY	**Regulatory issues**	**1. Security policy, organisation and culture**	1.3 Risk management
	Industry training	**1. Security policy, organisation and culture**	1.6 Security awareness and competency
	Design	**2. Lifecycle considerations**	2.3 Design
		5. Secure and safe design	5.4 Behaviour on failure 5.5 Defence in depth 5.10 Protection of communications
DESIGNING IN SECURITY	**Development**	**5. Secure and safe design**	5.16 Development environment
	Installation	**2. Lifecycle considerations**	2.6 Installation
	Maintenance	**2. Lifecycle considerations**	2.9 Operation, maintenance, and decommissioning
		3. Maintaining effective defences	3.3 Secure operation, maintenance, and decommissioning
	Decommissioning and disposal	**2. Security-aware lifecycle**	2.9 Operation, maintenance, and decommissioning
		3. Maintaining effective defences	3.3 Secure operation, maintenance, and decommissioning
	Patching and updates	**3. Maintaining effective defences**	3.6 Product and service updates

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

DfT guidance		Rail Code of Practice	
Section	**Topic**	**Section**	**Topic**
PROTECTING AGAINST ATTACKS ON NEW AND CURRENT SYSTEMS	**Train control and signalling interface**	**5. Secure and safe design**	5.10 Protection of communications
	Physical and cyber attacks	**1. Security policy, organisation and culture**	1.3 Risk management
	Cabling	**5. Secure and safe design**	5.13 Physical security
	Capability and competence	**1. Security policy, organisation and culture**	1.6 Security awareness and competency
	International issues	**6. Contributing to a safe and secure world**	2.5 Supply chain 6.5 International issues

Table 7: Detailed comparison between DfT guidance and CoP

NCSC – CAF COLLECTION

To support the introduction of the NIS regulations, NCSC developed a Cyber Assessment Framework (CAF) to provide guidance for organisations responsible for vitally important services and activities. This set of guidance is known as the CAF collection and includes a set of cyber security and resilience principles for securing essential services, which is organised as four objectives and 14 principles.

Table 8 provides a detailed comparison between the CAF Principles and the Rail CoP.

CAF Principles		Rail Code of Practice	
Objective	**Principle**	**Section**	**Topic**
OBJECTIVE A: MANAGING SECURITY RISK	**A.1 Governance**	**1. Security policy, organisation and culture**	1.1 Policies and processes 1.2 Responsibility and accountability 1.3 Risk management

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

CAF Principles		Rail Code of Practice	
Objective	**Principle**	**Section**	**Topic**
OBJECTIVE A: MANAGING SECURITY RISK	**A.2 Risk management**	**1. Security policy, organisation and culture**	1.3 Risk management
	A.3 Asset management	**1. Security policy, organisation and culture**	1.4 Asset management
	A.4 Supply chain	**1. Security policy, organisation and culture**	1.5 Supply chain and other external dependencies
OBJECTIVE B: PROTECTING AGAINST CYBER ATTACK	**B.1 Service protection policies and processes**	**1. Security policy, organisation and culture**	1.1 Policies and processes
	B.2 Identity and access control	**3. Maintaining effective defences**	3.5 Identity and access control
	B.3 Data security	**1. Security policy, organisation and culture**	1.8 Protection of information
	B.4 System security	**5. Secure and safe design**	5.3 Secure system configuration 5.5 Defence in depth 5.12 Protection of communications
	B.5 Resilient networks and systems	**5. Secure and safe design**	5.4 Behaviour on failure
	B.6 Staff awareness and training	**1. Security policy, organisation and culture**	1.6 Security awareness and competency 1.7 Culture and communication

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

CAF Principles		Rail Code of Practice	
Objective	**Principle**	**Section**	**Topic**
OBJECTIVE C: DETECTING CYBER SECURITY EVENTS	**C.1 Security monitoring**	**3. Maintaining effective defences**	3.2 Protect, detect, respond 3.9 Threat monitoring
	C.2 Proactive security event discovery	**3. Maintaining effective defences**	3.2 Protect, detect, respond 3.9 Threat monitoring
OBJECTIVE D: MINIMISING THE IMPACT OF CYBER SECURITY INCIDENTS	**D.1 Response and recovery planning**	**4. Incident management**	4.1 Planning
	D.2 Lessons learned	**4. Incident management**	4.5 Post-event

Table 8: Detailed comparison between NCSC CAF objectives & principles and CoP

On the basis of this comparison, the most relevant sections of the CoP for the NCSC guidance appear to be:

1. Security policy, organisation and culture

3. Maintaining effective defences

4. Incident management

5. Secure and safe design

Conversely, the NCSC guidance does not appear to cover:

2. Lifecycle considerations

6. Contributing to a safe and secure world

The apparent lack of coverage for 'Contributing to a safe and secure world' is surprising, given that the main motivation for the NIS regulations is to improve the safety and security of essential services.

EN 50126

In this section, we consider the relationship between the security-informed lifecycle described in the CoP and the generic RAMS process for railway applications described in EN 50126-1:2017.

The CoP is outcome-focused and does not prescribe any particular lifecycle or safety process. Instead, it provides both high-level and detailed guidance about security-informed safety considerations at different stages of a generic safety lifecycle.

In particular, Section 2 of the CoP provides a high-level overview of security-informed safety considerations at various stages in a safety lifecycle while Sections 3, 4 and 5 of the CoP provide detailed guidance about specific aspects of the lifecycle (operation and maintenance, incident response, and design and implementation).

In contrast, EN 50126-1:2017 specifies a detailed lifecycle with 12 phases grouped into three major blocks, namely risk assessment, implementation, and operation.

Table 9 shows a mapping between the generic RAMS process defined in EN 50126-1:2017 and the various stages of the lifecycle considered in Section 2 of the CoP. The mapping demonstrates that the lifecycle considered in Section 2 of the CoP is broadly comparable with the EN 50126 RAMS process.

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

Major block	Rail Code of Practice	Rail CoP
Risk assessment (on the basis of the system definition), including the specification of RAMS requirements	**Phase 1 – Concept** **Phase 2 – System definition and operational context** **Phase 3 – Risk analysis and evaluation** **Phase 4 – Specification of system requirements** **Phase 5 – Architecture and apportionment of system requirements**	Clause 2.2 – Risk assessment and requirements definition
Implementation and demonstration that the system fulfils the specified RAMS requirements	**Phase 6 – Design and implementation** **Phase 7 – Manufacture** **Phase 8 – Integration** **Phase 9 – System validation** **Phase 10 – System acceptance**	Clause 2.3 – Design Clause 2.4 – Manufacturing Clause 2.5 – Supply chain Clause 2.6 – Installation Clause 2.7 – Demonstration of security Clause 2.8 – Assurance
Operation, maintenance and decommissioning	**Phase 11 – Operation, maintenance and performance monitoring** **Phase 12 – Decommissioning**	Clause 2.9 – Operation, maintenance and decommissioning

Table 9: Mapping between Section 2 of the CoP and EN 50126

PD CLC/TS 50701

In 2021, CENELEC published PD CLC/TS 50701, a new cybersecurity standard for railway applications. The standard provides railway operators, system integrators and product suppliers with guidance on how to manage cybersecurity in the context of the EN 50126-1 RAMS lifecycle process and

> *'ensure that the residual risk from security threats is identified, supervised and managed to an acceptable level by the railway system duty holder'.*

Hence, the focus is on

> *'additional requirements arising from threats and related security vulnerabilities and for which specific measures and activities need to be taken and managed throughout the lifecycle. The aim [...] is to ensure that the RAMS characteristics of railway systems / subsystems / equipment cannot be reduced, lost or compromised in the case of intentional attacks'.*

In particular, clause 5 discusses cybersecurity within a railway lifecycle, and identifies some specific security activities, synchronisation points to ensure coordination with other system engineering activities, and deliverables to be exchanged.

APPENDIX G
RELATIONSHIP TO OTHER INDUSTRY GUIDANCE

Clauses 6, 7 8 cover system definition, initial risk assessment, detailed risk assessment, resulting in a set of cybersecurity requirements that are allocated to subsystems and components.

Clause 9 discusses cybersecurity assurance and system acceptance for operation, and clause 10 covers operational, maintenance, and disposal requirements.

There is also a number of informative annexes, including a discussion of the relationship between security and safety, which argues that safety functions can only fulfil their intended use in an appropriate security environment that protects against adverse external influences.

The security models, concepts and risk assessment methods described in PD CLC/TS 50701 are based on or derived from the IEC 62443 series of standards, which makes the standard very prescriptive, particularly with respect to risk assessment and security architecture (zones and conduits). In particular, the security requirements are derived from the system security requirements from IEC 62443-3-3, with additional guidance on railway applications.

In contrast, the Rail CoP does not advocate any particular approach to risk assessment and is outcome-focused rather than prescriptive, focusing on principles rather than detailed guidance.

In this sense, the two documents are complementary. Section 2 of the Rail CoP discusses principles and recommended practices for a security-informed lifecycle, while PD CLC/TS 50701 provides detailed guidance on cybersecurity risk management within the context of the EN 50126 lifecycle. More broadly, the Rail CoP also covers security policy, organisation and culture, secure and safe design, maintaining effective defences, incident management, and contributing to a safe and secure world. These broader topics are not addressed directly by PD CLC/TS 50701, except to the extent that they are realised by the detailed system security requirements obtained from IEC 62443-3-3.

APPENDIX H
GUIDANCE FOR READERS

ASSUMED BACKGROUND AND PRE-REQUISITES

The code of practice is primarily aimed at people with a safety background who need to know how security issues impact on their existing safety practice, but it might also be read by people with a security background who need to know something about how the rail industry manages safety.

Readers who are not familiar with how the rail industry manages safety may find it helpful to read 'Taking Safe Decisions' [12], an RSSB guidance document that explains how Britain's railways take decisions that affect safety. Readers with a railway background who are not familiar with cyber security may find the DfT guidance on Rail Cyber Security [2] helpful as a starting point.

The CoP builds on both of these documents by suggesting a set of principles and specific actions for security-informed safety that conform to best practice and address the requirements of the DfT guidance on Rail Cyber Security, while complying with the RSSB guidance on 'Taking Safe Decisions'.

INDICATIVE ROLES

The CoP is intended to cover the entire rail ecosystem, which is very broad. Each railway stakeholder will have their own perspective on the CoP and will find some sections more relevant than others. In order to provide some guidance for the intended readership, we have identified a broad set of individual and organisational roles that are representative of various stakeholders in the railway industry.

Table 10 identifies some individual roles that might be accountable or responsible for different aspects of safety or security within a railway organisation.

Role	Responsibility
Director of safety	Accountable for the safety of all rail equipment and systems within an organisation
Director of Information Technology	Accountable for the security of all information systems within an organisation
Duty holder	Accountable for the safety of a particular system
Project manager	Responsible for managing a project to deliver a change to the overall railway
Technical architect	Responsible for designing a technical solution that meets a set of safety and security requirements

Table 10: Individual roles within the railway industry

APPENDIX H
GUIDANCE FOR READERS

Similarly, Table 11 identifies a broad set of organisational roles within the rail industry.

Organisation	Responsibility
Infrastructure manager	Manages the trackside infrastructure, including signalling and traffic management
Telecoms provider	Manages all railway communications over both fixed and wireless networks
Train operator (TOC)	Operates one or more train services
Rolling stock owner (ROSCO)	Owns the rolling stock, which is leased to one or more train operators
Maintenance organisation	Maintains and services the rolling stock or track infrastructure
Equipment manufacturer	Supplies trackside or onboard equipment
Service provider	Provides a service such as passenger wi-fi
Component manufacturer	Supplies components to be used in railway equipment
Independent safety assessor	Provides an independent assessment of whether the necessary safety processes and risk assessments have been adequately performed
Safety authority	Safety regulator with statutory powers

Table 11: Organisational roles within the railway industry

In general, we distinguish between rail operators and rail suppliers. Rail operators are responsible for delivering a safe railway service using equipment and services provided by rail suppliers.

Rail suppliers need to provide rail operators with assurance that the equipment and services they supply are safe and secure by design. Independent safety assessors provide an independent level of assurance.

Rail operators are responsible for ensuring the safety of the overall railway system, which requires them to manage the safety and security of all equipment and services from deployment through operation to decommissioning. Railway operators are licensed to operate by the safety regulator, who requires evidence that all safety risks have been adequately controlled.

APPENDIX H
GUIDANCE FOR READERS

Rail suppliers are responsible for informing rail operators about any vulnerabilities that are discovered during the lifetime of their equipment and services and providing advice on risk mitigation. In return, rail operators have a responsibility to inform rail suppliers of any issues encountered during operation, so that the underlying cause can be investigated and the safety and security of the equipment or service can be improved as necessary.

In practice, the rail supply chain is more complex than this. Rail systems and services are constructed and delivered using equipment and components from multiple organisations, so information about potential security and safety vulnerabilities needs to flow up and down the supply chain in order to ensure the safety and security of the overall railway, which remains the responsibility of rail operators. This means that railway suppliers in the middle of the supply chain have a dual role, reporting vulnerabilities to the users of their equipment and reporting potential issues to their suppliers.

SUGGESTED TOPICS FOR EACH ROLE

In this section, we use the roles identified in the previous section to provide guidance on the sections of the CoP that might be most relevant to particular individuals and organisations. The roles are intended to be illustrative and the guidance is indicative rather than definitive. In practice, individuals and organisations are expected to take what they need from the CoP and adapt it to their circumstances.

INDIVIDUAL ROLES

Table 12 suggests some topics that might be of interest to particular roles. In general, we distinguish between managerial roles and technical roles. Managerial roles will typically be most interested in sections of the CoP that are concerned with setting policies and procedures for managing risk, whereas technical roles will be more concerned with the detail of how risk is managed.

Role	Particular sections of interest	Relevant appendices	Rationale
Director of Safety	**1. Security policy, organisation and culture** **2. Lifecycle considerations** **6. Contributing to a safe and secure world**	**A. Risk assessment** **B. Assurance and safety cases** **D. Interactions between safety and security**	Accountable at Board level for ensuring the safety of all rail equipment and systems within an organisation. Primarily concerned with setting policies and procedures for managing safety risk within the organisation. Will want to ensure that security risks to safety are properly managed and that appropriate assurance is provided to or obtained from related organisations (e.g. customers and the supply chain). Will also wish to enhance organisational reputation and minimise risk of reputational damage by collaborating with other organisations to ensure a safe and secure railway ecosystem.

APPENDIX H
GUIDANCE FOR READERS

Role	Particular sections of interest	Relevant appendices	Rationale
Director of Information Technology	**1. Security policy, organisation and culture** **3. Maintaining effective defences** **4. Incident management**	**A. Risk assessment** **B. Assurance and safety cases** **E. Network security**	Accountable at Board level for ensuring the security of all information systems within an organisation. Will work closely with the Director of Safety to ensure that information systems do not pose a threat to operational systems.
Safety manager	**2. Lifecycle considerations** **3. Maintaining effective defences**	**A. Risk assessment** **B. Assurance and safety cases** **D. Interactions between safety and security**	Responsible for the safe operation of a particular railway system. Will want to have assurance that security risks have been considered during the development of the system and that security will be managed during the operation of the system.
Project manager	**1. Security policy, organisation and culture** **2. Lifecycle considerations** **5. Secure and safe design**	**A. Risk assessment** **D. Interactions between safety and security**	Responsible for managing a project to deliver a safe change to the railway. Will want to ensure that best practice is being followed.
Technical architect	**5. Secure and safe design**	**E. Network security** **F. Secure coding standards**	Responsible for the design and implementation of a railway system. Will need to know how to design a system that is both safe and secure.

Table 12: Topics by role

ORGANISATIONAL ROLES

Table 13 suggests some topics that might be of interest to particular organisations. Rail operators will tend to be more interested in the operational aspects of the CoP, whereas rail suppliers are more interested in the design aspects of the CoP. But both parties will have an interest in risk management in general and the importance of managing risks during the development process. Independent safety assessors and the safety authority will have a particular interest in security risk assessment and assurance cases.

APPENDIX H
GUIDANCE FOR READERS

Role	Relevant sections of code of practice	Relevant appendices	Rationale
Infrastructure manager	**1. Security policy, organisation and culture** **2. Lifecycle considerations** **3. Maintaining effective defences** **4. Incident management** **6. Contributing to a safe and secure world**	**A. Risk assessment** **B. Assurance and safety cases** **C. System composition** **D. Interactions between safety and security** **E. Network security**	Required by ROGS to establish a safety management system and ensure that railway operations are safe and secure. Needs to maintain effective defences, respond to security incidents, and collaborate with other railway operators. Manages the safety and security of a complex system of systems, connected together using a variety of networks.
Telecoms provider	**3. Maintaining effective defences** **4. Incident management** **5. Secure and safe design** **6. Contributing to a safe and secure world**	**A. Risk assessment** **B. Assurance and safety cases** **C. System composition** **D. Interactions between safety and security** **E. Network security**	Responsible for railway communications – needs to protect the communication network against attack and ensure that it cannot be used to compromise the safety of railway operations.
Train operator	**1. Security policy, organisation and culture** **2. Lifecycle considerations** **3. Maintaining effective defences** **4. Incident management** **6. Contributing to a safe and secure world**	**A. Risk assessment** **B. Assurance and safety cases** **D. Interactions between safety and security**	Required by ROGS to establish a safety management system and ensure that railway operations are safe and secure. Needs to maintain effective defences, respond to security incidents, and collaborate with other railway operators.

APPENDIX H
GUIDANCE FOR READERS

Role	Relevant sections of code of practice	Relevant appendices	Rationale
Rolling stock owner	**2. Lifecycle considerations** **3. Maintaining effective defences** **5. Secure and safe design**	**A. Risk assessment** **B. Assurance and safety cases** **C. System composition** **D. Interactions between safety and security** **E. Network security** **F. Secure coding standards**	Leases rolling stock to train operators – purchases equipment for installation in train from railway suppliers. In order to protect investment, needs to be an intelligent customer with knowledge of best practice for secure and safe design.
Maintenance organisation	**1. Security policy, organisation and culture** **2. Lifecycle considerations** **3. Maintaining effective defences**	**A. Risk assessment** **B Assurance and safety cases** **D. Interactions between safety and security**	Required by ROGS to establish a safety management system and ensure that railway operations are safe and secure. Will need to ensure that all maintenance changes are applied safely and securely.
Equipment manufacturer	**2. Lifecycle considerations** **3. Maintaining effective defences** **5. Secure and safe design** **6. Contributing to a safe and secure world**	**A. Risk assessment** **B. Assurance and safety cases** **C. System composition** **D. Interactions between safety and security** **E. Network security** **F. Secure coding standards**	Designs and implements equipment for railway operators that needs to be safe and secure by design. Will need to provide assurance in the form of a security-informed safety case. Must ensure that components from third-party suppliers do not compromise the security of the design. Will be required to notify railway operators if a vulnerability is discovered.

APPENDIX H
GUIDANCE FOR READERS

Role	Relevant sections of code of practice	Relevant appendices	Rationale
Service provider	**3. Maintaining effective defences** **4. Incident management** **6. Contributing to a safe and secure world**	**A. Risk assessment** **B. Assurance and safety cases** **C. System composition** **D. Interactions between safety and security** **E. Network security**	Provides a service to railway operators – needs to ensure that the service remains secure and cannot be used to compromise the safety of the railway system. Will need to respond appropriately to any security incidents and advise customers on safety implications.
Component manufacturer	**3. Maintaining effective defences** **5. Secure and safe design** **6. Contributing to a safe and secure world**	**B. Assurance and safety cases** **E. Network security** **F. Secure coding standards**	Supplies components to railway equipment manufacturers. Needs to follow best practice for secure and safe design to prevent components from creating security vulnerability. Will be required to notify equipment manufacturers if a vulnerability is discovered and advise on safety implications.
Independent safety assessor	**1. Security policy, organisation and culture** **2. Lifecycle considerations** **3. Maintaining effective defences** **5. Secure and safe design**	**A. Risk assessment** **B. Assurance and safety cases** **C. System composition** **D. Interactions between safety and security** **E. Network security** **F. Secure coding standards**	Provides independent assurance that railway systems and services can be operated safely. Needs to be familiar with best practice for building in security and to have confidence that safety and security will be managed throughout the lifecycle.

APPENDIX H
GUIDANCE FOR READERS

Role	Relevant sections of code of practice	Relevant appendices	Rationale
Safety authority	**1. Security policy, organisation and culture** **2. Lifecycle considerations** **3. Maintaining effective defences** **6. Contributing to a safe and secure world.**	**A. Risk assessment** **B. Assurance and safety cases** **D. Interactions between safety and security**	Regulatory authority responsible for issuing safety certificates to railway operators – will require organisations to demonstrate that they have an appropriate safety management system in place and will co-operate with other organisations to ensure the safety and security of railway operations.

Table 13: Topics by organisation

Disclaimer

This guide has been prepared by CPNI and is intended to support the implementation of security-informed safety in the rail sector and provides guidance on security issues for railway safety engineers and managers. This document is provided on an information basis only, and whilst CPNI has used all reasonable care in producing it, CPNI provides no warranty as to its accuracy or completeness.

It is important to emphasise that no security measures are proof against all threats. You remain entirely responsible for the security of your own sites and/or business and compliance with any applicable law and regulations and must use your own judgement as to whether and how to implement our recommendations.

To the fullest extent permitted by law, CPNI accepts no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using the [report]. This exclusion applies to all losses and damages whether arising in contract, tort, by statute or otherwise including where it is a result of negligence. CPNI separately and expressly exclude any liability for any special, indirect and/or consequential losses, including any loss of or damage to business, market share; reputation, profits or goodwill and/or costs of dealing with regulators and fines from regulators.

No Endorsement

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 favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

CPNI
Centre for the Protection of National Infrastructure