PAS 11281:2018

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

CPNI®
Centre for the Protection of National Infrastructure

bsi.

Publishing and copyright information

ISBN 978 0 539 02394 7

ICS 03.080.01, 03.220.20

Publication history

First published December 2018

Contents

Foreword

This PAS was sponsored by the Centre for the Protection of National Infrastructure (CPNI). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 31 December 2018.

Acknowledgement is given to the technical authors Robin Bloomfield, Eoin Butler, Peter Bishop and Robert Stroud of Adelard, and to the following organizations that were involved in the development of this PAS as members of the steering group:

- Adelard
- Atkins
- Automotive Electronic Systems Innovation Network (AESIN)
- BodVoc
- Centre for the Protection of National Infrastructure (CPNI)
- Defence Science and Technology Laboratory (Dstl)
- Department for Transport (DfT)
- Halfords Autocentres
- Highways England
- HORIBA MIRA
- McLaren Automotive Ltd
- Ricardo
- Stagecoach Group
- The National Cyber Security Centre (NCSC)
- Waverley House Consultancy Ltd

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

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a code of practice to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this document

As a code of practice, this PAS 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 PAS 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 PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Information about this document

The CAV principles given in this PAS are reproduced from the Department for Transport (DfT) Centre for Connected and Autonomous Vehicles (CCAV)'s "The key principles of cyber security for connected and automated vehicles" [1] and contain public sector information licensed under the Open Government Licence v.3.0.

Presentational conventions

The provisions of this PAS are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. "organization" rather than "organisation").

Contractual and legal considerations

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

Compliance with a PAS cannot confer immunity from legal obligations.

0 Introduction

0.1 The connected automotive ecosystem

The connected automotive ecosystem encompasses vehicles and all assets and activities that support the proper functioning of road transport and other off-road systems (such as farming and mining vehicles). This includes systems such as traffic monitoring and control systems, navigation, information and entertainment systems that enable efficient, economic and enjoyable journeys. Manufacturing, supply chain and maintenance activities, which provide the necessary support for the on-going functioning of the automotive ecosystem, are also part of the connected automotive system. The idea of the ecosystem also covers the concept of Cooperative-Intelligent Transport System (C-ITS), which is a type of ecosystem promoted by the European Commission in which users and managers share information and use it to coordinate their actions [2].

The technology supporting automotive transport has been rapidly evolving over the last few years. Connected vehicles and other systems are a reality, while increased automation is on the horizon. The term "connected and autonomous vehicles" (CAVs) is now widely used to refer to vehicles that include aspects of these new technologies.

CAV technology is seen as potentially enabling increased:

a) safety;
b) road capacity and reduced congestion; and
c) inclusion and accessibility for people unable to drive or access conventional modes of transport.

The UK Government has identified CAV technology as a priority area for research and development, and has announced investments in excess of £100 m in this area [3]. The UK Government's recent Industrial Strategy [4] singles out the automotive sector as one of the UK's particular strengths and recommends measures to support continued progress, particularly in research and development.

The UK's cyber security strategy [5] identified the growing Internet of Things, of which CAVs form a part, as a challenge to cyber security over the next few years. CAVs are an example of a class of cyber-physical systems, in which connected computer systems directly control the behaviour of a real-world system (this contrasts with cyber-only systems, e.g. banking systems, where compromise of the system does not cause direct physical harm). An example of a cyber-physical attack occurred in December 2015 in Ukraine: an energy provider was attacked, leading to a blackout for residents of the country. Many other similar attacks have been recorded. Thus, there is a direct link between cyber security and safety, as compromise of the cyber aspect of the system can manifest itself in the physical world. The technology and systems used in cyber-physical systems are often referred to as operational technology (OT), while cyber-only systems might be referred to as information technology (IT) respectively.

0.2 Security-informed safety

Security-informed safety is the consideration of the impact of security risks on safety. Traditionally, security and safety have been treated as separate disciplines, with their own regulations, standards, culture and engineering. Safety can be seen as protecting against harm due to unintentional actions, while security is often seen as preventing harm due to the intentional actions of malicious actors. However, there is a growing realization that security and safety are closely interconnected and interdependent: 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 the impact of security. This can be succinctly summarized as "if it's not secure, it's not safe".

While in many situations security and safety measures can comfortably be integrated together, there are other cases where there might be tension or conflict between safety and security needs. In some areas, such as frequency estimation, the techniques traditionally used in safety analysis might be inadequate, and require a qualitative approach, particularly if detailed threat information is not available. For example, 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. Finally, unlike security, where vulnerabilities are accepted or generally withheld until solutions are known, information on safety hazards is usually disseminated openly to enable providers to respond by taking action to ensure their products, systems or services are in a safe state, e.g. grounding of an aircraft.

0.3 The approach taken for this PAS

The initial development of this PAS was undertaken using a combination of "top-down" and "bottom-up" approaches.

The top-down approach started from an overall vision for the connected automotive ecosystem, a world where everyone has confidence in a safe and secure connected automotive ecosystem. From this, a top-level claim was derived, stating that there is justified confidence that security issues do not pose unacceptable risks to the safety and resilience of the connected automotive ecosystem. Then, using the claims-argument-evidence approach [6] to assurance, a network of linked sub-claims that are supported by a set of principles was developed. These principles were then used to derive the recommendations in this PAS.

The bottom-up approach started from existing sets of security and safety focused principles and guidance that have been produced for the automotive sector as well as other safety-related sectors. These include:

a) Department for Transport (DfT) Centre for Connected and Autonomous Vehicles (CCAV): The key principles of cyber security for connected and automated vehicles [1];
b) European Union Agency Network and Information Security (ENISA): Cyber security and resilience of smart cars – good practices and recommendations [7];
c) National Highway Traffic Safety Administration (NHTSA): Cybersecurity for Modern Vehicles [8];
d) National Cybersecurity Centre (NCSC): Network and Information Security (NIS) Directive guidance [9];
e) Rail Industry Cyber Security Assurance Group: Cyber Security Assurance Principles [10]; and
f) Office for Nuclear Regulation (ONR): Security Assessment Principles for the Civil Nuclear Industry [11].

Various sets of principles were examined to see where they overlapped and common themes extracted that were relevant for connected vehicles. These were compared with the initial set of recommendations derived from the "top down" approach given above to ensure that there was adequate coverage of the important points.

This PAS has been developed in order to ensure that the recommendations are aligned with on-going work in the sector.

0.4 How this PAS helps

This PAS aims to help organizations in the connected automotive ecosystem to ensure that security-related risks in their products, services or activities do not pose unacceptable risks to safety. In line with modern regulatory approaches, the recommendations are framed as outcome-based measures, while also suggesting some specific features that adequate security arrangements would be expected to have. While such features can aid with some other non-safety-related security concerns (e.g. privacy and theft), such concerns are not covered in this PAS.

The outcome-based approach has the added benefit of enabling compatibility with other standards and guidance in the area. Some example scenarios are given below:

- Sector- or topic-specific standards can be used to guide detailed implementation of the recommendations contained within this PAS. For example, BS ISO/IEC 27035 can be used to implement a security incident management system.
- All or part of the PAS can be used as means of providing assurance that requirements stemming from more general standards or regulations have been satisfied. For example, IEC 61511 Part 1 **8.2.4** and **11.2.12**, which address the security of a safety system.
- Compliance with the PAS might also be used as a means of demonstrating due diligence for commercial arrangements, or as evidence in an assurance case.
- Organizations can make use of the PAS as a benchmark against which to measure their security arrangements, and identify shortcomings or areas for improvement.

It is expected that different readers of this PAS use it in different ways, mostly by paying more attention to clauses that are of special interest to them. This depends on the role of the individual reader within their organization. Some examples of scenarios are shown in Table 1:

Table 1 – Individual roles

Role	Clauses of special interest
Director of security/safety	Clause **3** Security policy, organization and culture Clause **4** Security-aware development process Clause **8** Contributing to a safe and secure world
Technical architect	Clause **7** Secure and safe design
Programme manager	Clause **4** Security-aware development process
Procurement manager	Clause **3** Security policy, organization and culture Clause **4** Security-aware development process
Security manager	Clause **3** Security policy, organization and culture Clause **5** Maintaining effective defences Clause **6** Incident management

The Annexes provide informative guidance on specific topics that might aid organizations to implement the recommendations:

a) risk assessment (Annex A);
b) assurance and safety cases (Annex B);
c) secure versus safe coding practices (Annex C);
d) approaching safety and security integration (Annex D);
e) automotive networks (Annex E);
f) security and safety of a composite system (Annex F); and
g) UK Government CAV principles (Annex G).

1 Scope

This PAS gives recommendations for managing security risks that might lead to a compromise of safety in a connected automotive ecosystem.

The PAS covers both the entire connected automotive ecosystem and its constituent systems throughout their lifetimes (including manufacturing, supply chain and maintenance activities). The ecosystem includes vehicles (both those used on public roads, such as cars, and those used for off-road activities such as farming and mining), as well as road-side and other static infrastructure, communication channels between vehicles and infrastructure, servicing and repair facilities, digital services, data and information and other services that support the proper operation of road transport. All levels of vehicle automation and autonomy are in scope.

The PAS applies to risks that can affect a single system, a few systems, or are on a small scale. It also gives recommendations for managing systemic risks – wider risks which might appear small, but which become more significant when interdependencies are considered and where the vulnerability of a single or a few entities poses more widespread risk.

The PAS is intended to be used by manufacturers, operators and maintainers of products, systems and services used in a connected automotive ecosystem. This includes manufacturers of vehicle subsystems, vehicle manufacturers, maintenance organizations, infrastructure operators, owners of large vehicle fleets, and digital service providers.

This PAS might be of interest to regulators and other stakeholders in the connected automotive ecosystem and to users/operators of vehicles.

2 Terms, definitions and abbreviations

For the purpose of this PAS, the following terms and definitions apply.

2.1 Terms and definitions

2.1.1 accident

any unplanned event that resulted in injury or ill-health of people, or damage or loss to property, plant, materials or the environment or a loss of business opportunity

[SOURCE Health and Safety Executive [12]]

2.1.2 asset

anything that has value to an individual, organization or government

[SOURCE BS ISO/IEC 27032:2012, **4.6**]

NOTE 1 *An asset can be fixed, mobile or movable. It can be an individual item of equipment or plant, a system of connected equipment, an entire piece of infrastructure, or a portfolio of assets.*

NOTE 2 *An asset might also comprise information or intellectual property (e.g. software) in digital or in printed form, as well as an organization's internal processes.*

NOTE 3 *Digital information can be localized (i.e. based on a single data source), or distributed (i.e. derived from multiple data sources and/or locations).*

NOTE 4 *The value of an asset might vary throughout its life and an asset might still have value at the end of its life. Value can be tangible, intangible, financial or non-financial.*

2.1.3 assurance case

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

[SOURCE Bishop, et al., The future of goal-based assurance cases [13]]

2.1.4 attack

successful or unsuccessful attempt(s) to circumvent a security measure

[Adapted from BS EN ISO 22300]

2.1.5 competence

ability to apply knowledge and skills to achieve intended results

2.1.6 component

entity or system that forms a part of a larger system

2.1.7 connected system

system that makes use of one or more communication technologies to communicate with other systems

2.1.8 development process

set of steps performed to turn concepts and ideas into a finished product

2.1.9 disclosure

action of making sensitive, classified or closed data and/or information known

[SOURCE PAS 1885:2018, **3.10**]

2.1.10 hazard

source of potential harm

2.1.11 impact

evaluated consequence of a particular outcome

2.1.12 organization

person or group of people that has its own function with responsibilities, authorities and relationships to achieve its objectives

[SOURCE BS ISO 55000:2014]

2.1.13 personnel

individuals employed by an organization, including contractors or temporary staff used to fulfil roles that are undertaken by that organization

[SOURCE PAS 1192-5:2015]

2.1.14 product

article that is manufactured for sale

NOTE *Product includes both physical goods and intangible goods, such as software.*

2.1.15 resilience

ability to absorb and adapt in a changing environment

[SOURCE BS EN ISO 22300:2018]

2.1.16 risk

combination of the probability of occurrence of harm and the severity of that harm

[SOURCE ISO/IEC Guide 51:1999, **3.2**]

2.1.17 risk appetite

amount or type of risk that an organization is willing to pursue or retain

[SOURCE BS EN ISO 22300:2018]

2.1.18 risk assessment

overall process of risk identification, risk analysis and risk evaluation

NOTE *Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the likelihood and impact of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.*

[SOURCE BS EN ISO 22300:2018]

2.1.19 risk management

co-ordinated activities to direct and control an organization with regard to risk

NOTE *Risk management generally includes risk assessment, risk treatment, risk acceptance, and risk communication.*

[SOURCE BS ISO 22300:2018]

2.1.20 safety

state of being protected from or unlikely to cause danger, risk, or injury

[SOURCE Oxford English Dictionary]

2.1.21 safety case

assurance case that makes claims with regard to safety

2.1.22 security

state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts

[SOURCE Engineering Council, 2016 [14]]

NOTE *When considering the harm that could be caused by exploitation of a security vulnerability the aim should be to reduce the risk of:*

a) physical injury to people, whether in/on the vehicle or outside it; and

b) damage to assets and the environment.

2.1.23 security incident

event or events during which the security of an asset, organization or person is, or might be, compromised, either accidentally or deliberately

NOTE *Security incidents can take a number of forms including:*

a) unauthorized harmful modification to, damage to or destruction of a physical asset;

b) supply of counterfeit raw materials, ingredients, physical and/or digital components, assemblies or sub-systems;

c) loss or theft of documents, storage media, IT equipment, attractive or valuable items;

d) loss, theft or unauthorized access to information or data;

e) loss, compromise, unauthorized manipulation or change of project or asset information;

f) unauthorized access to the built asset, or a restricted access area within the built asset;

g) loss of keys, access control tokens, passes, etc.;

h) planting of bugs or other surveillance devices; and

i) unauthorized access to, misuse of, or fraudulent use of ICT equipment or systems.

[SOURCE PAS 1885:2018]

2.1.24 security-informed safety

inclusion of security considerations when managing safety risks

2.1.25 service

work done to meet some administrative, general or public need

NOTE *In an automotive context, a system supplying a vehicle user or public need includes navigation, road charging, communications and information.*

[SOURCE: PAS 1885:2018, **3.37**]

2.1.26 supply chain

network of organizations, directly or indirectly interlinked and interdependent, resources, activities and technology involved in the creation and sale of products and/or systems, and any related services, from the delivery of source material(s) from the supplier(s) to the manufacturing organization, through to eventual delivery to the end user

2.1.27 system

interacting or interdependent set of things working together and forming an integrated whole

NOTE *Systems can be made up of smaller systems, or subsystems.*

2.1.28 threat

potential cause of an incident which might result in harm to an asset(s), individual(s), and/or organization(s)

[SOURCE adapted from PAS 1885:2018]

2.1.29 threat agent

person or organization that can pose threats

2.1.30 vulnerability

weakness that can be exploited by one or more threats

[SOURCE: PAS 1885:2018, **3.49**]

2.2 Abbreviations

For the purpose of this PAS, the following abbreviations apply.

CAV	connected and autonomous vehicles
GDPR	EU General Data Protection Regulation [15]
NCSC	National Cybersecurity Centre
NDA	non-disclosure agreement
NIS	network and information security

3 Security policy, organization and culture

*COMMENTARY ON CLAUSE **3***

Organizations have legal responsibilities to manage safety risks associated with their products, systems and services. Organizations responsible for safety-related products, systems and services would be expected to have a safety policy that describes the organization's approach to the safety of their products, systems, services or activities. A safety policy typically provides a statement of general policy on health and safety, the quality and safety of its products, systems and services, and also sets out commitments to managing safety effectively.

"Security-informed safety" is the term used to describe the inclusion of security considerations when managing safety risks. The organization also needs to have an approach of how to consider security. A possible approach for the automotive sector can be found in PAS 1885. Consideration of security issues, whether in their own right or integrated with a safety policy, necessitates significant departures from existing approaches. For example, the impact of threat agents on safety risks needs to be considered throughout the lifecycle of products, systems and services. In addition, security considerations lead to a need for a greater degree of confidentiality than is customary in safety, as information about systems might enable attacks. This is particularly applicable to information on the organization's picture of the threats and the countermeasures it has taken, which might enable an attacker to identify exploitable vulnerabilities. Personnel with responsibility for overseeing safety activities might not be competent in the security area. Therefore, additional responsible roles might need to be defined.

Security concerns that are not directly safety-related, such as confidentiality and privacy requirements arising from the EU General Data Protection Regulation (GDPR) [15], falls outside the scope of this PAS, although they could indirectly lead to safety issues (for example, theft of design documentation might enable an attack, or information on the movement of traffic might identify a high value target). Such concerns are dealt with in PAS 1885.

3.1 Policies and processes

3.1.1 The organization should formulate a policy that sets out its overall stance and aims with respect to the security-informed safety of its products, systems and services.

3.1.2 The organization should define and implement processes to support this policy and to ensure that security-informed safety is addressed throughout the organization, its partners and suppliers, and in all phases of the lifecycle of its products, systems and services.

3.1.3 The processes should consider personnel, physical, technical, procedural and managerial protection measures.

***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.*

3.1.4 The organization should take steps to ensure that these policies and processes are described, communicated and implemented effectively.

***NOTE** Guidance on developing policies and processes can be found in the NCSC guidance [9] on the NIS Directive [16], specifically, Objective B1: Service protection policies and processes.*

3.1.5 The organization should produce and retain sufficient documentary evidence regarding its policies and processes and its decisions relating to security and safety to enable them to be reviewed and justified in the future.

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

3.1.6 The organization should define for how long its documentary evidence is retained.

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

3.2 Responsibility and accountability

3.2.1 Accountability for security-informed safety issues should be clearly defined, and traceable to the board level.

NOTE *The organization's board need to be aware of the organization's overall approach to security.*

3.2.2 A member of the organization's board or equivalent senior responsible person should be responsible for defining the organization's security-informed safety policies, processes and work.

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

3.2.4 If responsibility for implementing aspects of the security-informed safety programme is delegated to members of the organization, the identity, roles and responsibilities of such individuals should be clearly recorded.

NOTE *Individuals can be identified by role or by name.*

3.3 Risk management

NOTE *There are a large number of risk management approaches that might be suitable for adoption (with or without tailoring) by the organization. Examples can be found in the NCSC Risk Management collection [17], and detailed processes developed with the automotive and manufacturing sectors in mind are described in PAS 1885 and PAS 1085.*

3.3.1 The organization's approach to security should recognize that the organization has a responsibility to ensure that security does not pose unacceptable risks to safety.

3.3.2 The organization should articulate and document its risk appetite with regard to safety and security risks so that decision makers at all levels of the organization can make informed decisions.

3.3.3 The organization should document in its safety policy its overall approach to how the impact of security considerations on safety risks is addressed, setting out its commitment to managing such issues effectively and defining responsibilities accordingly.

3.3.4 The organization should adopt a formal, holistic, approach to identifying, assessing and understanding security-informed safety risks to its products, services and activities throughout the whole lifecycle.

3.3.5 The organization should document in its safety policy how it determines the tolerability of risks.

NOTE 1 *An example of a tolerability policy might be to reduce the risk to a level that is as low as reasonable practicable (ALARP). However, interactions and trade-offs between different risks often make the task more complicated than this.*

NOTE 2 *The tolerability of risks derived from an activity often depends on the relative benefit derived from the activity, who reaps the benefit, and who bears the risks.*

3.3.6 The organization should adopt an approach to resolving any conflicts between safety and security that might occur at any stage of the service/product lifecycle.

NOTE *Further guidance on this topic can be found in Annex D.*

3.3.7 The organization should identify, assess and understand the impact of assumptions it might have made regarding the prevalence, capabilities and motivations of threat agents on its demonstration that risks are tolerable.

3.3.8 The organization should manage risks to the safety and security of its products, services and activities arising from physical threats.

NOTE *Guidance on physical security is available from CPNI [18].*

3.3.9 The organization should manage risks to the safety and security of its products, services and activities arising from threats from among the organization's personnel.

NOTE *Guidance on personnel security is available from CPNI [19].*

3.3.10 The organization should manage risks to the safety and security of its products, services and activities arising from cyber threats.

NOTE *Guidance on cyber security is available from NCSC [20].*

3.3.11 The organization should include evidence that security risks have been adequately managed in any safety cases it produces for its products, services and activities.

3.4 Asset management

3.4.1 All assets (systems and services) that are required to deliver, maintain or support the security and safety of the organization's products, systems and services should be identified and recorded, along with the importance of their role in maintaining safety and security.

NOTE 1 *Assets include data, people and systems as well as any supporting infrastructure. Assets can be both tangible and intangible (see **2.2**).*

NOTE 2 *Detailed guidance on implementing an asset-based risk register can be found in PAS 1885 2018, **5.6** and **6.2**.*

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

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

3.4.3 Existing or legacy assets, developed in the past and which might not have been designed with security in mind, should be subject to a risk assessment to identify, and where needed, mitigate security-related risks associated with them.

3.5 Supply chain and other external dependencies

3.5.1 The organization should assess and manage security risks specific to, and/or encompassing, supply chains, sub-contractors and service providers.

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

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

NOTE 3 *More detailed guidance on managing the security of supply chains is provided in Clauses **5** and **8** of PAS 1885 2018 for the automotive sector, which is a possible means of complying with this clause. Similar guidance is provided in PAS 1085 for the manufacturing sector.*

3.5.2 The management of supply chain-related risks should be integrated into design, specification and procurement processes.

3.5.3 The organization should assess, and periodically re-assess, the security of its suppliers. The frequency of re-assessment should be determined by the organization's safety policy (see **3.1**) and risk management (see **3.3**).

3.5.4 The organization should ensure that suppliers have an appropriate security and safety policy and programme in place.

NOTE *Possible means of ensuring this include audits and external accreditation.*

3.5.5 For designed or engineered products, systems or services, security requirements and requirements for good security engineering practices should be included in procurement contracts.

3.5.6 The organization should include security requirements in procurement contracts with suppliers, and ensure that such requirements are cascaded along the supply chain as necessary.

NOTE *A potential way of complying with this clause is to require the supplier to comply with all or part of this PAS.*

3.5.7 The organization should have a process for managing information that is provided to the supply chain and has potential security implications so that the risk of misuse of such information is mitigated.

NOTE *Further information on the protection of data and/or information is provided in **3.8**.*

3.5.8 The organization should take all reasonable steps to ensure that all components received from suppliers are authentic and of trusted origin.

NOTE *Guidance on assuring the integrity of the supply chain can be found from NCSC [21], CPNI [22] and PAS 1885, **8.3** and for manufacturers in PAS 1085, Clause **8**.*

3.6 Security awareness and competency

3.6.1 All personnel should be trained, knowledgeable, aware of and competent in safety and security issues relevant to their roles.

NOTE *The level of training needed varies depending on the role, but it is likely that all personnel need at least a basic level of security training.*

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

3.6.3 The organization should assess the need for specialist security expertise, and develop or obtain such expertise as needed.

3.7 Culture and communication

3.7.1 The organization should promote a healthy security culture among those responsible for the safety of its products, systems and services.

3.7.2 Communication channels for security matters relating to the organization should be established and integrated with those for safety.

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

NOTE *An example of a measure to promote cooperation and collaboration would be a joint review of a product, system or service for security-related safety issues at an appropriate point in the design and development process.*

3.8 Protection of information

3.8.1 The organization should ensure that the security of information, documentation and data, compromise of which could affect the safety of its systems, is maintained.

NOTE 1 *Unauthorized access to, disclosure, modification or destruction of such information can significantly increase safety and security risks, as it can assist threat agents to identify vulnerabilities.*

NOTE 2 *This includes information in both electronic and physical form (e.g. USB sticks, paper copies, cloud storage).*

NOTE 3 *This includes information on design that would aid an attacker to successfully compromise a system.*

3.8.2 The organization 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 BS EN ISO/IEC 27002,* ***8.2****.*

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

NOTE 1 *Examples of requirements could be the length of retention, the process to be followed for release and the measures to be taken to protect the information.*

NOTE 2 *Using a formal data and information sharing agreement (DISA) is a possible approach. Further details on DISAs can be found in PAS 1085 and PAS 1885.*

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

4 Security-aware development process

COMMENTARY ON CLAUSE 4

Safety-focussed development approaches aim to reduce the number and impact of faults and vulnerabilities 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 risk. In addition, requirements for safe operation, maintenance and decommissioning are documented.

A security-aware approach mirrors a safety approach, but aims to reduce the number and impact of vulnerabilities in the product or service. Many steps of the process are very similar at a high level. However, is important to note that it might be necessary to follow a security-aware development process to products, systems or services that do not have a direct safety impact. This is because systems that do not have direct safety relevance (e.g. infotainment or monitoring systems) might be used by threat agents as an initial means of compromise to gain a foothold in the system before going on to attack further parts of the system.

This Clause includes a minimal set of measures to be incorporated into the product/service development process. The measures are not to be regarded as complete, and do not exclude the incorporation of any other measures indicated by standards or risk assessment.

A detailed security-aware development process can be found in PAS 1885.

4.1 General

4.1.1 All development activities should be documented and records retained.

4.1.2 The development of all products, systems and services should follow a formal, structured process.

4.1.3 The development of all safety-relevant services or products should follow a safety process as specified in an accepted safety standard appropriate for the system.

NOTE *Examples of relevant safety standards include ISO 26262 Road vehicles – Functional Safety, and IEC 61508:2010, Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related Systems. Such standards define a safety lifecycle process and techniques and measures for reducing the safety risk.*

4.1.4 For all products, systems and services, each phase of the development 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 *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 SAE J3061 [23], IEC/ISA 62443 and BS 10754.*

4.1.5 The development 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 is implemented to ensure that a safe and secure product or service is produced.

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

a) aligning security and safety activities with project management gateways;

b) including iterative security assurance activities; and

c) aligning safety and security approval and sign-off activities.

NOTE 2 *The production of a complicated system such as an automobile involves a number of interlocking and integrated lifecycle processes. BS/ISO/IEC/IEEE 15288 identifies 30 system lifecycle processes, which are divided into four groups:*

a) agreement processes;

b) organizational project-enabling processes;

c) technical management processes; and

d) technical processes.

4.1.6 No measure should be applied if its application is judged to be disproportionate to the security or safety benefit, but the rationale for this judgement should be explicitly recorded.

NOTE *A balance has to be struck between cost and risk. Typically organizations need to consider all risks to their business, which includes commercial and financial risks as well as safety and security.*

4.2 Risk assessment and requirements definition

NOTE *Further guidance on risk assessment is given in Annex A.*

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

NOTE 1 *The safety of a service (or a product/system used to provide a service) includes affecting the safety of products, systems and other services that interact with that service.*

NOTE 2 *Established techniques for performing risk assessments can be found in NCSC's Risk Management Collection [17]. Detailed approaches for the automotive and manufacturing sectors are described in PAS 1885 and PAS 1085 respectively.*

4.2.2 The risk assessment should, at a minimum, consider the risks posed by the following classes of attacks:

a) technical (e.g. hacking);

b) sociotechnical (e.g. social engineering);

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

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

4.2.3 The risk assessment should consider the interactions or conflicts between safety and security.

NOTE *Further guidance on this topic can be found in Annex D.*

4.2.4 The risk assessment should take into account interdependencies in products, systems and services and the potential interaction of simultaneous failures and their consequences.

NOTE *This includes the possibility of cascade failures.*

4.2.5 The risk assessment should allow for the possibility that increased or unknown 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 network is physically isolated from other networks, and can be bypassed if connectivity is added.*

4.2.6 The risk assessment should consider the potential effect of evolving threats and exploitable vulnerabilities on the safety of the product, system or service over its lifetime.

4.2.7 The risk assessment should include security risks posed by threat agents who aim to cause physical harm as well as threat agents who might accidentally cause harm incidental to other activities.

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

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

4.2.9 The requirements derived from the risk assessment should include security requirements to mitigate the safety risks posed by threat agents to a tolerable level.

NOTE 3.3.5 *recommends the organization define what is tolerable.*

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

NOTE *Guidance on safe and secure composite systems can be found in Annex F.*

4.3 Design considerations

4.3.1 The product, system or service should be designed to be fail-safe and secure by design.

4.3.2 The design should address security and safety throughout the lifecycle of the product, system or service.

NOTE *Further guidance on secure design principles can be found in Clause **7**.*

4.4 Demonstration of security

4.4.1 There should be a documented plan for demonstrating that the safety and security of the product, system or service meets its safety and security requirements.

4.4.2 The product, system 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; and

c) penetration testing.

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

NOTE *This contrasts with relying on 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.*

4.4.4 The product, system 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 organization, but not involved in product or service development, or to personnel from an external organization.*

4.4.5 The level of independent scrutiny required should be commensurate with the vulnerability of the system, the threat environment and the safety-criticality.

NOTE *The requirements for independent assessment in safety standards (e.g. ISO 26262) might need to be increased accordingly.*

4.5 Assurance

4.5.1 For safety-relevant products, systems, services or activities, an assurance case that justifies that the product, system or service is adequately safe, taking into account security threats, should be produced.

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

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

NOTE *Guidance on assurance cases can be found in BS ISO/IEC 15026-2 and Annex B.*

4.5.3 Where a safety-relevant product, system, service or activity depends on products, systems, services procured from third parties, assurance material should be obtained from the third party and integrated into the overall assurance case.

NOTE *It is preferred that the supplier of a component or subsystem supply their own assurance case, but it is recognized that this might not always be possible for, e.g. off-the-shelf products.*

4.6 Manufacturing

4.6.1 The product or system 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 IEC/ISA 62443 and PAS 1085.*

4.7 Third-party components

NOTE 4.7 *provides recommendations for when part of a product, system or service is procured from a third party. Recommendations for supply chain considerations relevant to the entire organization are also in* ***3.5****.*

4.7.1 When part of the product, system or service is procured from a third party, the risk assessment should consider the potential impact on the safety and security that might be caused due to contamination, faults or vulnerabilities in the procured part.

NOTE *For cyber-physical products and systems, contamination can take the form of malicious code or unauthorized modification to data and/or information, for example changes to configuration and reference data. In both cases the outcome may be that the product or system could operate in an unsafe manner."*

4.7.2 The organization should take all reasonable steps to ascertain if procured equipment or software contains functionality that could compromise the safety or security of the systems, and if so, take this into account in the risk assessment.

NOTE 1 *It is common for products to include manufacturer-only functionality used for servicing, debugging or testing, which might not be intended for use by the customer, and not be documented publicly.*

NOTE 2 *Steps might include contractual requirements on the supplier to disclose the presence of such functionality, or by auditing the supplier.*

4.7.3 The organization should make arrangements to be informed of any safety or security issues relevant to a procured product, system or service that are discovered after delivery.

4.7.4 The organization should take steps to ensure that, if any third-party products, systems or services are discontinued or cease to be maintained, the resultant risk is managed.

NOTE 1 *Possible steps include requiring advance notice of discontinuation or ensuring a diverse source or substitute for the product, system or service is available.*

NOTE 2 *This means that if supply or maintenance of a product or service ceases, the organization might need to either stop using the product or service or mitigate the resulting risk to its own products, system and services.*

4.8 Deployment

4.8.1 A documented approach for deploying a product, system or service in the field in a safe and secure way should be developed during the design and development process.

4.8.2 Deployment of a product, system or service in the field should be carried out so that safety and security of the connected automotive ecosystem is maintained.

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

4.9 Operation, maintenance and decommissioning

4.9.1 Before release for sale or operation, a product or service should have a documented approach for how it can be operated safely and securely.

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

4.9.2 Before release for sale or operation, a product, system or service should have a documented approach for how security and safety is maintained throughout maintenance activities, particularly if temporary special arrangements are put in place for maintenance.

4.9.3 Before release for sale or operation, a product, system or service should have a documented approach for how it can be decommissioned, repurposed, or be transferred to a new owner or operator while maintaining safety and security.

5 Maintaining effective defences

*COMMENTARY ON CLAUSE **5***

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 automotive sector, systems (including vehicles and infrastructure) have traditionally operated in a well-defined environment, with little to no communication between systems. Thus, the risks to road transport safety were fairly static and well-known.

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 commoditized, 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 agents with lower capability. This Clause contains recommendations on how to maintain effective defences, including upgrading systems to close avenues of attack or to patch uncovered vulnerabilities and close down new avenues of attack.

5.1 Protect, detect, respond

5.1.1 The organization should implement measures to protect the assets, systems and services that are under its control and that affect the safety of the connected automotive ecosystem against attack.

5.1.2 The organization should implement measures to detect attacks against the assets, systems and services that are under its control and that affect the safety of the connected automotive ecosystem (see **6.2**).

5.1.3 The organization should be capable of responding to confirmed attacks on the products, assets, systems and services that affect the safety of the connected automotive ecosystem (see **6.4**).

5.2 Secure operation, maintenance and decommissioning

5.2.1 The organization should ensure that all systems and services under their control are operated in a safe and secure way, and follow the documented approach developed in **4.8.1**.

5.2.2 The organization should ensure that all systems and services under their control are maintained in a safe and secure way, and follow the documented approach developed in **4.8.2**.

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

5.2.3 For licensed or sub-contracted service/maintenance organizations, security requirements should be incorporated in their license/contract.

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

5.2.4 The organization should ensure that any security-related material contained in their assets (e.g. keys, design information) is securely removed or destroyed when the asset is sold, repurposed, or disposed.

***NOTE** Where this is delegated to a third-party or contractor, **5.2.4** can be complied with by including requirements in the contract.*

5.3 Access control

5.3.1 The organization should document and manage all access rights to its systems and assets. The rights granted to individuals should be periodically reviewed and removed when no longer required.

NOTE 1 *Access rights need to be carefully controlled, especially rights that grant access to safety-critical operations.*

NOTE 2 *Controlling access needs to be balanced with the need for availability of information needed for end-users to operate and maintain their products. For example, access to a user's manual would not typically be restricted.*

5.3.2 Except for publicly available information systems/ services, access to a product, system or service should be protected by authentication.

NOTE 1 *Designers are encouraged to consider alternative means of authentication to passwords. Several sources of guidance on authentication methods exist, e.g. NIST, Digital Identity Guidelines [24].*

NOTE 2 *For a single vehicle, access might be by a physical key, which counts as a form authentication.*

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

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

5.3.4 Physical access to systems or assets that deliver or support safety or security-relevant products, systems or services should be controlled and monitored.

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

5.4 Product, system and service updates

5.4.1 The organization should take steps to inform an end-user of its products, systems or services about updates when they are made available and encourage them to apply them.

NOTE 1 *The end-user can be encouraged by, for example, emphasizing the security and/or safety impact of the update.*

NOTE 2 *It is preferred if software updates can be applied with as little effort as practicable. It might be possible to apply software updates to products or systems wirelessly ("over the air") or enable end-users, such as domestic vehicle owners, to update their systems without the need for specialist equipment.*

5.4.2 The organization should consider the severity of any security or safety issue addressed by the update to determine how quickly it should be distributed.

5.4.3 Organizations supplying products, systems or services should take steps to ensure that the ability of customers and users (or their subcontracted maintenance providers) to acquire and apply updates is not unduly restricted.

NOTE *It is important to bear in mind that it is common for attackers to reverse-engineer updates to discover any vulnerabilities it mitigates and there might be a rationale for the organization to require a license or other arrangement for access to updates.*

5.4.4 The organization should make arrangements to receive updates from the manufacturers or suppliers of products, systems, or services that it supplies, redistributes or depends on.

5.4.5 The organization should make arrangements to ensure that updates to its assets are applied in a timely way, particularly if they have a security impact.

NOTE 1 *Attention is drawn to the Automated and Electric Vehicles Act 2018 [25]. Section 4 of that Act allows an insurance policy for an automated vehicle to limit or exclude the insurer's liability for damage occurring as a direct result of failure to install safety-critical updates.*

NOTE 2 *If maintenance is delegated or subcontracted to another organization, this can be arranged using contractual clauses.*

5.4.6 A safety or security-relevant system or service (e.g. infrastructure) should not be updated unless the impact of the update on the safety and security of the system or service and the wider ecosystem has been assessed and accepted to be tolerable.

5.4.7 An update should not be applied to a product, system or service unless its authenticity and integrity can be verified.

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

5.4.8 Where it is necessary to not apply or delay applying an update, the decision should be documented, justified and approved by a designated person in the organization, and the risk the decision incurs should be assessed and mitigated if needed.

NOTE 1 *Some systems (particularly operational technology (OT)) might need to be taken offline to update, and this might take time to organize. In other cases, the organization might require time to analyse the impact of the update.*

NOTE 2 *EC/ISA 62443 offers guidance on patching in the context of industrial automation and control systems.*

5.5 Innovation

NOTE *Innovation covers new, potentially disruptive, uses of technology that can affect the way products, systems or services are used and undermine the assumptions made during the initial risk assessment. (An example of innovation is the use of cameras and image analysis to recognize road signs intended for use by drivers.) Innovation has the potential to expose the system to new modes of attack, introduce new vulnerabilities, or change the impact of failure or compromise.*

5.5.1 The organization should monitor the adoption of new technology amongst customers and end-users of its products, systems or services, and amongst other actors in the ecosystem to assess their potential to reduce or increase safety related risks.

NOTE *Innovation might also change the relevance of assets to safety and security. See also* ***3.4.3****.*

5.5.2 The organization should have a documented strategy to adapt its products, systems and services so that they remain safe and secure in the face of changing technology and use.

5.6 Discovery of vulnerabilities

5.6.1 The organization should have a documented process for handling communications from third parties reporting the discovery of vulnerabilities or new attacks that affect its products, systems and services.

NOTE *The flow of information on vulnerabilities needs to be bidirectional. Informing third-parties when the organization discovers vulnerabilities in their products is covered in* ***8.3.4****.*

5.6.2 The organization should have a published policy for how it interacts with security researchers outside the industry. The policy should, at a minimum, enable ethical and/or responsible disclosure of vulnerabilities.

NOTE *BS ISO/IEC 29147 gives guidelines for the disclosure of potential vulnerabilities in products, systems and services.*

5.6.3 The organization should have documented processes to assess the safety impact of any alleged or actual vulnerabilities or new attacks.

NOTE *See also Clause* ***6****.*

5.7 Threat monitoring

5.7.1 The organization should take steps to monitor and understand the threats posed to its products, systems or services.

5.7.2 Where available, the organization should subscribe/participate in government-led or industry-adopted schemes for disseminating threat information.

NOTE *An example is the Automotive Information Sharing and Analysis Centre (Auto ISAC), https://www.automotiveisac.com.*

5.7.3 Reports of security incidents and anomalous system behaviour should be analysed for indications of new threats and the impact they might have on safety risk and design assumptions.

NOTE 1 *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 threats that evade standard detection and prevention measures. Activity can be analysed to detect unusual patterns of activity that might indicate previously unknown threats.*

NOTE 2 *Data used for anomaly detection might include data with privacy implications.*

5.8 Continuing risk management

5.8.1 The organization should have a standard process for continuing to manage security-related safety risks.

5.8.2 Assurance cases should be reviewed yearly and in rapidly changing threat environments more frequently, 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.*

6 Incident management

*COMMENTARY ON CLAUSE **6***

Organizations with responsibilities for safety in the automotive 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 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. Organizations are also likely to have procedures for responding to and mitigating identified issues, such as informing users and 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 more rapid response to ensure safety is maintained. This mainly stems from the fact that vulnerabilities are often shared amongst systems of a common design, and therefore multiple systems can be accessed simultaneously by an attacker. In addition, a tactic sometimes employed by threat agents is to attack the system and the organization'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 threat agents make use of misinformation tactics (e.g. to influence user behaviour to bring about hazardous situations).

6.1 Planning

6.1.1 The organization should have a documented plan to manage events that indicate potential risk to the safety of their assets, products, systems and services.

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

6.1.3 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 organization's assets, products, systems and services and on the safety of the automotive ecosystem.

***NOTE** Further guidance on security incident management is available from NCSC [26], NIST [27], BS ISO 27035 and PAS 1885, Clause **7**. Organizations might wish to implement an incident detection system compliant with ISO 27035.*

6.1.4 The plan should identify an organizational function or role (a "point of contact") with responsibility for coordinating incident response activities.

6.1.5 The plan should be exercised at least yearly.

***NOTE** Some organizations might find it appropriate to perform exercises in conjunction with others.*

6.1.6 The security of the infrastructure used to detect, respond to, and manage incidents should be protected.

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

6.2 Detection of security issues

6.2.1 The organization should have a program in place for detecting security issues in its assets, products, systems and services.

6.2.2 At least one means of contacting the organization to report a security issue should be advertised publicly and accessible to anyone.

6.2.3 The organization should enable and encourage responsible and ethical disclosure of security issues with its products, systems and services.

NOTE *Further guidance on receiving reports of vulnerabilities can be found in BS ISO/IEC 29147.*

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

6.2.5 The organization should examine reports of failures (e.g. from warranty returns/repairs) for indications that the failure might have been caused by an attack.

6.2.6 Any computer networks that the organization operates, and on which the proper operation or safety of the organization's products, systems or services depend, should be identified and actively monitored to detect security incidents.

6.2.7 The organization should subscribe to industry or government-led schemes that provide notifications of relevant incidents.

6.2.8 The organization should include contractual provisions for operators of safety-relevant services it uses to ensure that these services are monitored, and any relevant incidents are notified in a timely way.

6.3 Assessment

6.3.1 The organization should adopt a scheme for classifying security issues.

NOTE *An example of an incident categorization system can be found in the NIST Computer Security Incident Handling Guide [27].*

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

6.3.3 The plan (see **6.1**) should identify specific individuals who are responsible for and competent in assessing if any event might have a security dimension.

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.*

6.3.4 The organization should assess the impact of the security incident on the safety of their product or service.

6.4 Response

6.4.1 The organization 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.*

6.4.2 The plan should identify individuals with sufficient authority to authorize any actions needed to preserve the safety and security of the organization's products, systems or services.

6.4.3 The plan should consider the possibility of a security incident so severe as to necessitate withdrawal or recall of the organization's products, systems or services.

NOTE *ISO 10393 contains guidance on the recall of products.*

6.4.4 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 might exploit vulnerabilities that are present in products, systems or services provided by other organizations, and it is essential that such organizations are notified quickly to ensure that they can also respond as needed. It is also important to notify operators of services that might be affected by a degraded state of the organization'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.*

6.5 Post-event

6.5.1 Evidence that might 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 might need to be deployed to prevent this.*

NOTE 2 *BS EN ISO/IEC 27037 contains guidance on the identification and capture of digital evidence, while BS EN ISO/IEC 27042 contains guidance on its analysis.*

6.5.2 Following an incident, steps should be taken to identify and understand the underlying causes (e.g. vulnerabilities), and ensure that the risk management measures and risk assessment are updated if necessary.

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

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

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

7 Secure and safe design

*COMMENTARY ON CLAUSE **7***

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.

Security concerns often require inclusion of additional functionality beyond that needed to ensure safety from non-security-related hazards. Such functionality might include 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 does not directly lead to a hazardous situation (for example, authentication might be required for all messages sent over ostensibly closed networks). This Clause 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 [28] and Security Design Principles for Digital Services [29] is available from NCSC.

*PAS 1885, **5.13** also requires that organizations use a lifecycle that embraces secure-by-design.*

7.1 General

7.1.1 The measures described in Clause **7** should supplement, not replace, any measures that are specified in application-specific standards that are applied (e.g. ISO 26262 for vehicles).

7.1.2 Measures should not be applied if their application is judged to be inappropriate or disproportionate to the security benefit. The rationale for this judgement should be explicitly recorded.

***NOTE 1** A balance has to be struck between cost, complexity and risk.*

***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.*

7.2 Secure design principles

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

***NOTE** Examples of secure design principles can be found in the SAFECode "Fundamental practices for secure software development" [30] and the OWASP "Guide to building secure web applications and web services" [31], which both reference a set of secure design principles originally proposed by Saltzer and Schroeder [32] which include:*

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 is to be checked for authority;*
4) *open design: the design is not be secret;*
5) *separation of privilege: two keys are better than one;*
6) *least privilege: every program and every user of the system is to operate using the least set of privileges necessary;*
7) *least common mechanism: minimize the amount of mechanism common to more than one user and depended on by all; and*
8) *psychological acceptability: design for ease of use.*

7.3 Secure system configuration

7.3.1 A secure default configuration should be used for all hardware and software.

7.3.2 On safety-critical systems, the following measures should be applied:

a) The safety-critical function is provided by dedicated hardware that is not used for any non-safety function.

b) Any unnecessary functionality or applications are removed or disabled.

c) Any unnecessary network services are removed or disabled.

d) Unnecessary peripheral devices and removable media are removed or disabled.

e) Only authorized software is allowed to run.

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

f) Facilities to alter the configuration are protected from unauthorized users.

NOTE *Further guidance on secure configuration and recommended configurations for particular platforms is available from NCSC [33].*

7.4 Behaviour on failure

7.4.1 The system should include a mechanism to detect failures or unusual behaviour that might indicate compromise as the result of a security vulnerability.

NOTE *For simple systems that are intended for integration into a larger system that contains measures to detect or mitigate failures, application of* ***7.4.1*** *might be disproportionate.*

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

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

7.4.3 Failures or suspected compromises should be reported to the operator via an appropriate mechanism and recorded for subsequent analysis.

7.5 Defence in depth

NOTE *Further guidance on this topic can be found from ICS-CERT [34] and in PAS 1885, Clause* ***9****.*

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

NOTE 1 *For example, a measurement of vehicle speed might be derived from more than one source 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.*

NOTE 3 *ISO 26262 provides guidance on the concept of single-point failures and how they can be avoided.*

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

NOTE 1 *The degree of segmentation depends on the types and degree of connectivity in the network. Segmenting some simple networks might be infeasible or disproportionate (see* ***7.1.2****).*

NOTE 2 *IEC/ISA 62443 provides guidance on security zones and conduits for network segmentation.*

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

7.5.4 The design of the system should prevent a non-safety-related component inducing a safety-related component to take an unsafe action. If this is not possible, the non-safety-related component should be treated as safety-related.

NOTE *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.*

7.6 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 BS EN ISO 27002, Clause* ***10****.*

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

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

NOTE *In the United Kingdom, NCSC provides a list of certified cryptographic products [35].*

7.6.3 Steps should be taken to ensure that the processes and systems for securely generating, storing, archiving, retrieving, distributing and retiring cryptographic keys provide a sufficient level of protection and trust.

7.7 Protection of software

7.7.1 Steps should be taken to protect the software from unauthorized access.

NOTE *Such measures include procedural controls and prohibiting unauthorized distribution of copies of the software.*

7.7.2 Steps should be taken to protect the software from unauthorized analysis or unauthorized reverse engineering.

NOTE *Protection techniques, such as obfuscation or cryptography may be used to achieve this.*

7.7.3 Steps should be taken to protect the integrity of software and safety-relevant data.

NOTE *Integrity of data can be protected by use of secure fingerprints or checksums, or requiring an enhanced level of access to write to protected areas of memory. Techniques also exist to protect the software against interference while it is executing (i.e. control-flow integrity). More details can be found in Stavroulakis & Stamp, Handbook of Information and Communication Security [36].*

7.8 Diagnostics

7.8.1 The system should provide an interface for diagnosing faults securely.

NOTE *If the design makes provision for diagnostics, the motivation for bypassing security controls to diagnose faults is reduced. However, it is permissible to restrict access to more powerful functions or the ability to change certain sets of parameters.*

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

NOTE 1 *Physically hiding access ports is not considered adequate protection. An example of adequate protection might be requiring authentication before allowing access through the interface.*

NOTE 2 *SERMI [37] provides guidance on accreditation, approval and authorization to access security-related repair and maintenance information for third-party maintenance organisations.*

7.8.3 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 hazard.

NOTE *For example, the diagnostic action might be restricted to only act when the vehicle is moving at low speed.*

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

7.8.5 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.*

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

7.8.7 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.

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

7.9 Patching and updates

7.9.1 There should be a mechanism for updating the system safely and securely.

NOTE 1 *For example, all updates to be checked for authenticity, and it is only possible to update the product or service when it is in a safe state.*

NOTE 2 *Additional guidance on patching and updates can be found in PAS 1885,* ***10.3****.*

7.9.2 The organization should enable the operator or owner of a product or system to identify the revision of software installed therein and determine if 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 specialized equipment.*

7.9.3 The design should facilitate updates to the product or service without compromising its overall safety and security.

NOTE *For example, the product or service could be designed in a modular fashion with an architecture that enforced strong separation between components.*

7.9.4 It should be possible to revert an update or restore the system to a known good state if the update process is not successfully completed.

7.10 Protection of communications

7.10.1 The design should take steps to verify the integrity and authenticity of data transmitted between components or received from other systems or external connections.

NOTE *While safety-related systems often use checksums or similar methods as a means of detecting accidental corruption of data, a simple checksum does not provide adequate protection against an attacker with knowledge of the checksum algorithm, who can modify both the data and the checksum. Techniques that make use of a digital signature based on a secret key can be used to establish the authenticity of data.*

7.10.2 Safety-critical data that is transmitted between components of the system should only be transmitted so that the data cannot be manipulated (spoofed, blocked) by a non-safety system.

7.10.3 Data that is transmitted between components of the system on a link that is not accessible either externally or to untrusted internal components, should be checked for integrity and validity.

NOTE 1 *Timing constraints and bandwidth limitations might 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 external source or an untrusted internal source.*

NOTE 2 *Further guidance on securing communications in automotive networks can be found in Annex E.*

7.10.4 The design should support the verification of the integrity, validity and authenticity of data it transmits.

7.10.5 The design should verify the integrity, validity and authenticity of data it receives from external sources.

NOTE *A common source of vulnerabilities is for an application to assume that data that passes an integrity check is valid. It is also important to check that the data is valid, for example, to check that the values of data fields are within range and are internally consistent.*

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

7.11 External services and devices

7.11.1 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.*

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

7.11.3 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.*

7.11.4 The system should not make safety-related decisions on the basis of information received from an external source, unless the source has an appropriate level of trust, 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.*

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

NOTE *For example, even highly-reliable services such as Global Navigation Satellite System (GNSS) can be jammed by attackers.*

7.11.6 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.*

7.12 Forensic recording

7.12.1 The system should include measures to record system activities securely to enable forensic examination and aid identification of the cause of a security incident. The record should be preserved for an appropriate time period.

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. NHTSA has produced a rule (National Highway Traffic Safety Administration 49 CFR Part 563 38]) that defines the types of data required to be recorded. This document focusses on vehicle crashes, and could be used to specify such a vehicle system, though logging other security-related data could also be considered.*

NOTE 2 *An appropriate time period is 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.*

NOTE 3 *Attention is drawn to the possibility that such records might contain personally identifiable data, and applicable legislation might impose requirements for how the data is stored and protected.*

NOTE 4 *BS EN ISO/IEC27037 contains guidance on the identification and capture of digital evidence.*

7.12.2 Where practicable, a component or subsystem that is to be integrated into a larger system should support logging in a secure manner.

7.12.3 The forensic recording facility should be designed so that it is not possible for an attacker to modify the records and conceal their actions.

7.12.4 The forensic recording facility should be designed so that actions are logged in a timely manner.

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

7.12.5 All significant actions performed by the system should be recorded, including both safety and non-safety-related actions.

7.12.6 The forensic recording system should record changes made to safety relevant and security relevant parameters, with the time and the origin of the change.

7.12.7 The forensic recording system should make use of a timestamping system that enables the actual sequence of events or actions to be reconstructed.

7.13 Secure user behaviour and interfaces

7.13.1 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.*

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

NOTE *An example is to promote the use of strong authentication methods such as two-factor authentication, or strong passwords.*

7.14 Development environment

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

NOTE *Examples of guidance on secure coding practices are MISRA-C [39], SEI CERT C Coding Standard [40] and SAFECode [30]. Further guidance on safe and secure coding practices can be found in Annex C.*

7.14.2 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 specialized 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).*

7.14.3 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.*

8 Contributing to a safe and secure world

*COMMENTARY ON CLAUSE **8***

In safety industries, lessons learned are typically shared to push good 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 (such as the NCAP scheme for crash worthiness). Accident and near-miss investigations provide a formalized route for learning from experience, especially in the regulated high-hazard industries.

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

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

*PAS 1885, Clause **8** also contains guidance on cooperating with other organizations in the context of automotive cyber-security.*

8.1 Managing risks

The organization should assess and manage risks to:

a) the wider connected automotive ecosystem; and

b) society more generally;

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

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

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

8.2 Compatibility and interoperability

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

8.3 Information sharing

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

***NOTE** To protect intellectual property, information such as detailed design documentation can be made available under a non-disclosure agreement (NDA) or DISA (see **3.8**).*

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

8.3.3 The organization should collaborate with relevant organizations to obtain knowledge and understanding of current and relevant threats.

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

8.3.4 If the organization becomes aware of vulnerabilities that affect or might affect the products, systems or services of another organization, it should responsibly disclose such vulnerabilities to those organizations.

NOTE *Vulnerabilities might be identified through post-incident analysis (see **6.5**), or have been reported by third-parties.*

8.3.5 The organization should support other organizations in the connected automotive sector to understand and manage security risks arising from the use or abuse of its services, systems or products.

8.4 Collaboration

8.4.1 The organization should collaborate with relevant organizations to share, develop and foster the adoption of good engineering practices to mitigate current and relevant threats.

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

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

Annex A (informative) Risk assessment

A.1 General

There are 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 Annex discusses some of these challenges.

A.2 Impact on the project lifecycle

This PAS considers the impact of security on safety for overall governance and for individual phases of the lifecycles of products, systems and services in the automotive ecosystem. However, it is important to recognize that safety and security currently follow different processes (e.g. ISO 26262 and SAE J3061 [23] for the safety and cybersecurity, respectively, of vehicles) 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 appropriate controls.

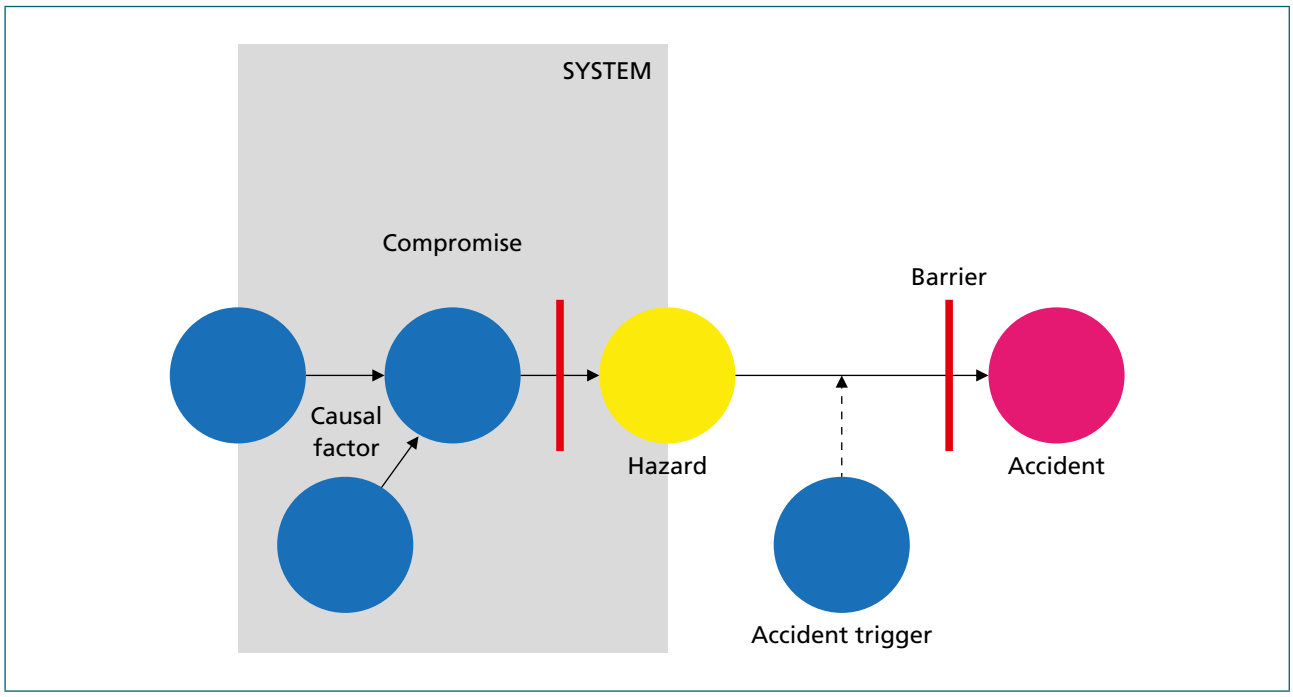
A.3 Impact on hazard identification

Security concerns could have an impact on:

a) the system boundaries;
b) what systems could potentially affect safety;
c) the stakeholders involved; and
d) the validity of design safety assumptions.

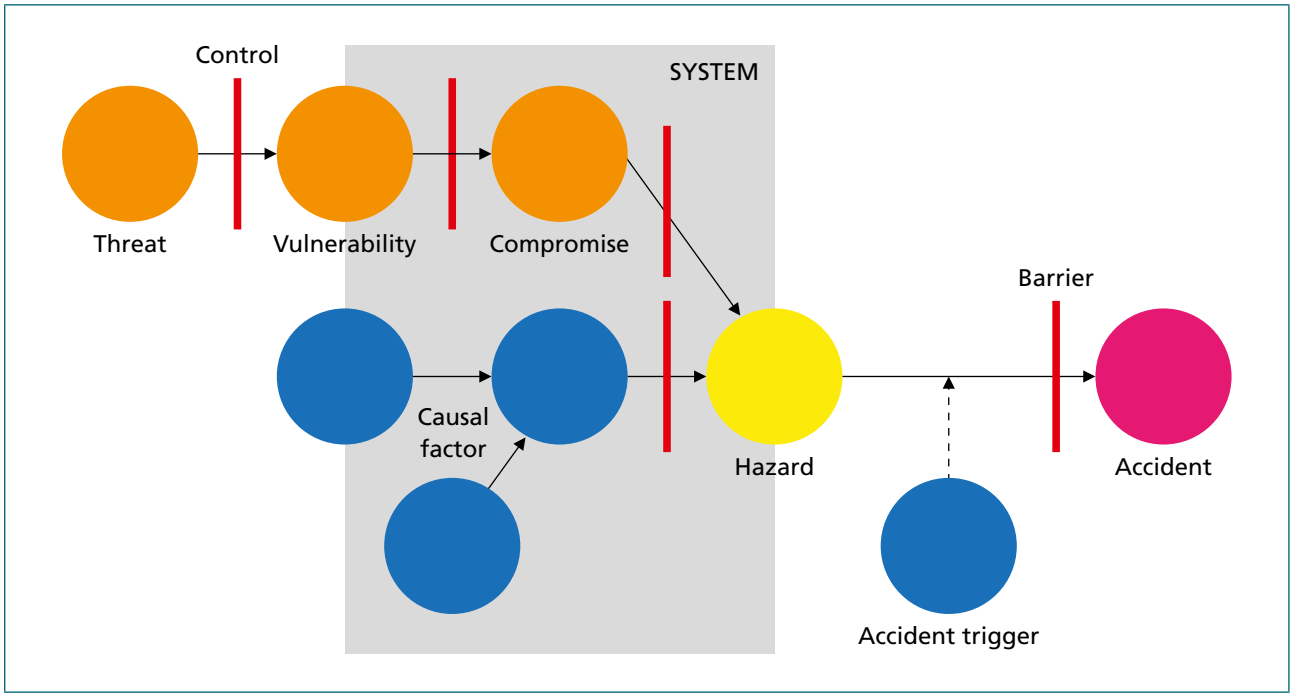
A conventional safety analysis uses a well-defined system boundary, and the analysis identifies causal factors (typically random or accidental events) that could result in a hazard. This is shown in Figure A.1. The hazard occurs on the boundary of the system being analysed. Barriers (design countermeasures)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

Figure A.1 – Schematic showing the relationship between causal factors, hazards and accidents



If security concerns are included, the organization needs 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 A.2, where security controls are shown with a red vertical line.

Figure A.2 – Extension of Figure A.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 issues 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. Schmittner, et al. [41], Fovino, et al. [42], Steiner and Liggesmeyer [43]).

A.4 Impact on risk estimation

Conventional safety analysis presumes a relatively stable environment where the initiating events are understood and relatively unchanging over time. Therefore, 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:

a) initiating event frequency;
b) event impact; and
c) controllability and mitigations.

However, in a security context, the types of attack are not necessarily known in advance and the likelihood and frequency of attack varies more over time, depending on the nature and number of attackers and changes in technology that facilitate attacks.

Furthermore, some of the assumptions that safety engineers might make (e.g. about independent failure of redundant components or of diverse "defence-in-depth" barriers) are no longer guaranteed if these elements are all vulnerable to attack. Organizations need ways of addressing these uncertainties, which might require a balance of qualitative and quantitative approaches. For example, a system might be designed to withstand attacks up to some qualitative capability level (see Bloomfield et al [44]).

One definition of capability levels can be found in NCSC, *Technical Risk Assessment and Risk Treatment* [45]. The capability levels range from 1 to 5 where, for instance:

a) Capability level 5 is classed as "formidable". The threat source is extremely capable and well resourced (for example, a hostile nation-state). It can:
   1) devote several man-years to penetrating the system or service;
   2) develop bespoke attacks;
   3) coordinate information about targeted systems or services from several sources;
   4) cultivate insiders for long-term attacks;
   5) deploy large amounts of equipment; and
   6) coordinate attacks using several threat agents.
b) Capability 4 is classed as "significant". The threat source is capable and has significant resources (for example, a well-organized terrorist or criminal group). It can:
   1) devote several man-weeks to penetrating a system;
   2) use all publicly available attack tools;
   3) influence insiders for specific attacks; and
   4) deploy modest amounts of equipment.

Threat sources at the lower levels have fewer resources and technical capabilities. Typical examples are a skilled lone hacker and a novice hacker. In general, threat sources with higher capability are more difficult to defend against, but are also fewer in number.

Threat capability, 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 capability level. 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 occurrences.

Security risk estimates might also need to be more frequently updated than risk estimates for purely safety risks. This could be prompted by developments such as the release of a tool enabling lower-capability agents to carry out attacks previously only in the reach of higher-capability agents.

A.5 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:

a) the level of uncertainty (which might be expressed qualitatively);
b) what is proportionate (given the societal impact if the attack succeeds);
c) the side effects of additional controls and complexity; and
d) what recovery measures are needed (recognising that these could also be attacked).

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.

A.6 Addressing uncertainty

As noted by the NCSC *(Critical Appraisal of Risk Methods and Frameworks* [46], *Risk Management Principles* 2016 [47] and *Security Governance: Enabling Sensible Risk Management Decisions and Communication* [48]), risk assessment has limitations. In particular, most methods fail to recognize 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.

Annex B (informative) Assurance and safety cases

B.1 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 a user 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 end-user needs to have sufficient and well-placed confidence that they 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. Therefore when we are dealing with a system whose failure can lead to danger, a safety case is the appropriate approach. For subsystems and other services with only an indirect impact on safety, or for components of a safety relevant system, then the organization needs to have confidence that the sub-system or service meets its explicit or implicit requirements in a way that leads to the safety of the overall system.

A more general approach to addressing the need for confidence in engineering decisions is assurance cases. 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" [13].

In practice, assurance cases can be very complex and might 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.

B.2 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, this is often derived from the regulation the assurance case is trying to meet. An example of a top level claim might be:

"System X is safe".

The precise meaning of "safe" and details of the system context and its environment need to be detailed in the remainder of the case.

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. Kelly and Weaver [49], ASCAD — Adelard Safety Case Development Manual [6] and Bishop, et al. [50]), and supporting standards and guidance (e.g. BS ISO/IEC 15026-2:2011 and GSN Community Standard [51]). Current assurance case practice makes use of a basic approach that can be related to ideas originally developed by Toulmin [52] – 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) (Kelly and Weaver [49]) or claims-argument-evidence (CAE) [1] (see Figure B.1). These notations [49] can be supported by tools (Emmet, et al. [53] and Rushby, "Mechanized support for assurance case argumentation," [54]) 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 Rushby, "The Interpretation and Evaluation of Assurance Cases" [55].

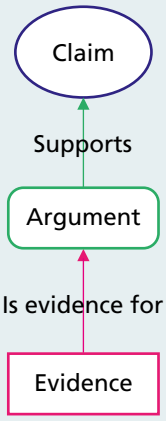
Figure B.1 – The CAE Framework

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 the "*statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established*" (Toulmin [52]) together with the validation for the scientific and engineering laws used. In an engineering context, arguments should be explicit.

Evidence, that is used as the basis of the justification of the claim. Sources of evidence might 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. In practice, possible top 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 develop them into sub-claims until the final nodes of the assessment can be directly supported (or refuted) with evidence. The basic concepts of CAE are supported by BS ISO/IEC 15026-2:2011 and industry guidance (see ASCAD — Adelard Safety Case Development Manual [6]).

In the light of an empirical analysis of actual safety cases, this PAS identifies a number of basic building blocks (CAE blocks) that can form the basis for describing the assessment (Bloomfield and Netkachova [56]). The blocks are:

a) concretion blocks; This block is used where a claim needs further clarification, e.g. because part of it is too vague or general;

b) substitution blocks; This block substitutes a claim for a system and property with another claim that is easier to provide evidence for, e.g. making a simpler conservative claim, making a claim about a test system rather than the real system as evidence is available on the test system;

c) decomposition blocks; This block is 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 be divided into sub-properties (e.g. security into confidentiality, availability and integrity, or hazards into different classes of hazards);

d) calculation blocks; This block is where a claim has a value associated with it that is calculated from sub-claims; and

e) evidence incorporation blocks; This block is used to make the link between the evidence and a closely associated claim.

The resulting CAE structure supports the assessment being made, but in addition, there will be important narrative and analyses explaining and detailing the claims and arguments being made. Narrative is an essential part of the assessment.

B.3 Evolution of safety case concept in ISO 26262

In the automotive sector there has been some adoption of structured approaches and the forthcoming revision to ISO 26262 strengthens and clarifies the role of the safety case. The key changes to the terminology and requirements are provided in Table B.1 and Table B.2.

Table B.1 – Vocabulary changes in ISO 26262

Part 1 – Vocabulary	
Current wording (2011-2012 edition)	**New wording (2016 public review draft)**
safety case argument that the safety requirements for an **item** (**1.69**) are complete and satisfied by evidence compiled from work products of the safety activities during development	**safety case** argument that functional safety (**3.64**) is achieved for safety-related products, such as items (**3.82**), systems (**3.163**), elements (**3.38**), and satisfied by evidence compiled from work products (**3.183**) of the safety (**3.131**) activities during development.
NOTE *The revised version of ISO 26262 is still under development at publication so the above wording might be subject to change.*	

Table B.2 – High-level safety case requirements: changes in text of ISO 26262

Part 2 – Management of functional safety	
Clause 6 – Safety management during the concept phase and the product development	
Clause 6.1 – Objectives	
Part 1 – Vocabulary	
Current wording (2011-2012 edition)	**New wording (2016 public review draft)**
[…] The second objective of this clause is to define the requirements for the safety management during the concept phase and the development phases, including […] the creation of the safety case, and the execution of the confirmation measures	The intent of this clause is to ensure the following objectives are achieved by the organizations involved in the concept phase or the development phases at the system, hardware or software level: […] the creation of a comprehensible safety case in order to provide an argument for the achievement of functional safety;
NOTE *The revised version of ISO 26262 is still under development at publication so the above wording might be subject to change.*	

MISRA is developing guidelines [57] to support the new version of ISO 26262. These provide a number of safety case templates to support the application of the revised standard.

B.4 Addressing security issues

While the GSN and CAE notations are 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 formality into the reasoning of the cases to manage the wider scope. The development of CAE blocks addresses this to some extent (Bloomfield & Netchakova, Building Blocks for Assurance Cases [56]) as do longer term visions of automated reasoning support (Rushby, "Mechanized support for assurance case argumentation" [54]). Increased rigour also brings with it the need for approaches to structuring the detailed cases: for example, the notion of layered assurance and structuring cases in terms of "layers" of requirements and policy, architecture and implementation (Delong [58] and Bloomfield, et al. "Security-Informed Safety: If it's not secure, it's not safe" [59].

In terms of content, the provisions of this PAS provide a clear indication of the scope required in general. The (CAE) framework (ASCAD — Adelard Safety Case Development Manual [6] and Bishop, et al. "A Methodology for Safety Case Development" [50]) can be used to analyse the impact of security on existing safety assessment or safety cases and thus identify the significant changes needed to address security explicitly (Bloomfield, et al. "Security-Informed Safety: If it's not secure, it's not safe" [59] and Netkachova, et al. "Investigation into a Layered Approach to Architecting Security-Informed Safety Cases" [60]. Incorporating security into the safety assessment impacts the design and implementation process as well as the approach to verification and validation. In particular, there is a need from a security perspective to consider:

a) Integration and interaction of requirements, e.g. of safety, with security and resilience supported by security informed hazard analysis techniques.

b) Supply-chain integrity, e.g. mitigating the risks of devices being supplied compromised or having egregious vulnerabilities.

c) Post-deployment malicious events that 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.

d) Reduced lifetime of installed equipment as there is a weakening of security controls as attackers' capabilities and technologies change.

e) Threats to the effectiveness and independence of safety barriers and defence in depth.

f) Design changes to address user interactions, training, configuration, and software vulnerabilities and patching. These might lead to additional functional requirements for security controls.

g) Possible exploitation of the device/service to attack itself or other systems and the need for confidentiality of design and deployment information.

h) The trustworthiness and provenance of the evidence offered.

Annex C (informative)
Secure versus safe coding practices

C.1 Introduction

Safety standards such as IEC 61508 and ISO 26262 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 24772:2013, 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 (McGraw [61]). 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. As examples, four of which are described in this Annex.

C.2 PD ISO/IEC TS 17961, Information technology – Programming languages, their environments and system software interfaces – C secure coding rules

PD ISO/IEC TS 17961 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 at 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 organize 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 "sanitized", 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.

C.3 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 [30]. These cover design, coding and testing – in particular, eight secure coding practices are identified:

a) minimize use of unsafe string and buffer functions;
b) validate input and output to mitigate common vulnerabilities;
c) use robust integer operations for dynamic memory allocations and array offsets;
d) use anti-cross site scripting (XSS) libraries;
e) use canonical data formats;
f) avoid string concatenation for dynamic SQL statements;
g) eliminate weak cryptography; and
h) use logging and tracing.

C.4 MISRA C

The Motor Industry Software Reliability Association (MISRA) publish 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 March 2013 [39].

The publication of PD ISO/IEC 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 (Bagnara [62]). A detailed comparison of the two standards resulted in the publication of a security amendment for MISRA C:2012 [63], but demonstrated that the existing MISRA standard [39] already provided good coverage of most of the secure coding rules in PD ISO/IEC 17961 (see MISRA C:2012 Addendum 2 [63]).

C.5 AUTOSAR C++

The Automotive Open System Architecture (AUTOSAR) partnership have developed a set of guidelines for the use of the C++14 language in safety-related and critical systems [65]. These guidelines update the MISRA C++ guidelines [66] to cover a more recent version of the C++ language, but do not yet cover security.

C.6 Discussion

There is considerable overlap between safe coding standards such as MISRA C [39] and secure coding standards such as PD ISO/IEC 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 [63] 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:2012 [39] are not adequately secure without this addition.

The introduction to PD ISO/IEC 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 [30] that several classes of security vulnerability are application-specific and therefore fall outside the scope of general-purpose guidelines for safe or secure coding like MISRA C [39] and ISO/IEC 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. Therefore, it is important for the designers of safety-critical systems to be aware of these kinds of vulnerability.

One of the requirements of IEC 61508 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, one aspect necessary to consider is 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 specialized area that requires expert knowledge and the use of proprietary algorithms and implementations is actively discouraged. Instead, good practice is to build safety-critical systems using standard protocols and technologies that are known to be secure, and considering digital key management as part of the safety case.

Annex D (informative)
Approaching safety and security integration

D.1 Introduction

This PAS deals with many different aspects of considering security in the context of the safety of an automotive ecosystem. 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

a) overlapping requirements;
b) overlapping functionality;
c) the use of shared resources or platforms;
d) information flow; and
e) misuse or abuse.

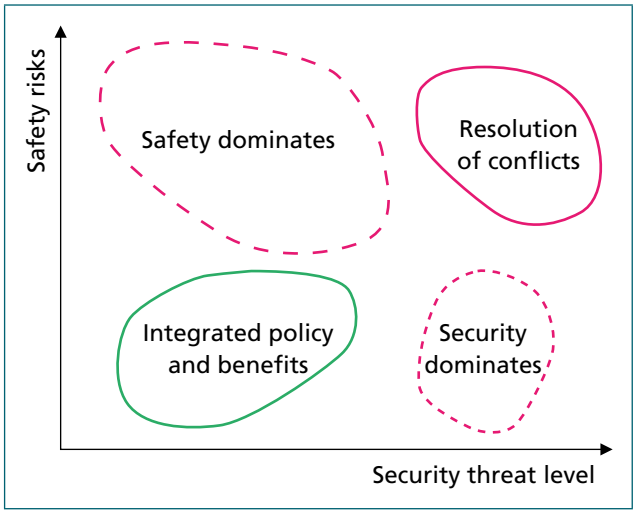
In general, these safety and security interactions might present the opportunity to make decisions that could result in trade-offs between safety and security. In some cases, they could result in direct conflicts between safety and security that cannot be easily resolved. For example, consider an access 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, e.g. 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 these holistically.

For safety, the most important considerations are ensuring that systems provide the required functionality with a given level of reliability (comprising integrity and availability). When the security perspective is included, confidentiality also becomes a concern. In this PAS we have recommended measures to protect the confidentiality of information that could be used by a threat agent to identify vulnerabilities or conduct an attack. The privacy of individuals is outside the scope, 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 D.1, taken and generalized from Netkachova, et al. "Investigation into a Layered Approach to Architecting Security-Informed Safety Cases" [60], shows different scenarios where security and safety interact:

1) In the bottom left corner is an area of maximum operational benefit, where with low levels of threat and no significant safety challenge, it is relatively straightforward to satisfy both aspects.
2) In the bottom right there is an area where security concerns might dominate due to the threat level. (e.g. with 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.
3) A corresponding zone in the top left corner, where safety issues dominate and the security policy is the same or weakened. In this case, the security analysis must show that identified security threats are satisfactorily mitigated by other means during this time.
4) The top right hand corner is a very uncertain area where some special capabilities might be needed, e.g. in the form of a manual override to security policy.

Figure D.1 – A schematic showing how security and safety interact in different scenarios



An organization has a clear legal and ethical responsibility to deliver a safe product, system or service. This PAS 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.

However,

- the organizational, technical and resourcing advantages that security brings are to be recognized and encouraged.

D.2 Examples of specific actions

Table D.1 highlights some specific areas where actions can be taken to minimize the need to trade-off safety and security.

Table D.1 – Examples of specific actions relating to the areas covered in this PAS

Topic	Actions
Security policy, organization 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. Manage the risk that an increased number of personnel with access to security information and system specific security knowledge might have on overall security. Such information might be valuable to any attackers.
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. Recognize and encourage the safety benefit from building security in (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 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 required architectures and controls to deliver both the safety benefit and high security. For example, an integrated forensics capability for both security and safety.
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 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 securing a product does not lead to safety issues for others in the eco-system, e.g. by restricting recovery, information flows. Ensure forensics and incident analysis can identify issues in sufficient detail to enable learning.

In expressing the need to prioritize safety, this PAS has 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 the case of a system in a vehicle 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 is called if the vehicle is in a crash, but it might also enable flooding or denial-of-service attacks on the emergency system, being detrimental to the safety of the ecosystem as a whole. Increasing security controls (by, for example, blacklisting sources of calls) could increase the chance that a valid call is rejected.

Such a situation calls for consideration of resilience. 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. Forms of resilience can be the preparation of fall-back modes of operation and a plan to adapt to and recover from, unforeseen circumstances.

Annex E (informative) Automotive networks

E.1 General

In recent years, a number of security researchers (e.g. Koscher, et al. [67], Checkoway, et al. [68], Foster, et al. [69] and Miller & Valasek [70]) have demonstrated that it is possible to launch a cyber-attack on a vehicle and override its safety features. Such attacks can either be launched locally or remotely and typically exploit the fact that the various subsystems connected to the in-vehicle network are trusted to behave in a safe fashion. As a consequence, any device connected to the in-vehicle network can send a safety-related message to any other device, and this message is acted upon, regardless of the consequences. Local cyber-attacks rely on the ability to attach a malicious device to the in-vehicle network via the mandatory on-board diagnostic (OBD) port, whilst remote attacks use a wireless connection to access and compromise a device connected to the in-vehicle network, such as the infotainment system or telematics box.

E.2 Securing in-vehicle communication

There are three basic approaches that can be used to secure communications over the in-vehicle network Hoppe, et al. [71], Ueda, et al. [72] and Palanca [73]:

a) Partition the network into trusted and untrusted domains.

b) Add a security protocol that requires knowledge of a secret (e.g. a cryptographic key or certificate).

c) Install network and host intrusion detection mechanisms.

Network partitioning is probably the optimal solution but is not something that can easily be retrofitted to an existing vehicle. However, many vehicles are already designed with the in-vehicle network partitioned between safety and non-safety related devices, and this is likely to become increasingly common in the future now that the cyber security threat to vehicles has been recognized. Unfortunately, partitioning the network is not as straightforward as it might seem. For example, the infotainment system needs to be aware of the vehicle speed and road noise in order to ensure that music is audible within the driving compartment. A possible solution to the need for this kind of connectivity between safety and non-safety related devices would be for the safety component to broadcast the required information through a one-way gateway, thus ensuring that the information was accessible to the non-safety related device, without allowing that device to access safety functions of the vehicle. Another approach would be to configure the network gateway with a "white list" that only allowed specific interactions between safety and non-safety devices, with any other attempted interaction being blocked.

The introduction of security protocols is problematic because of timing and bandwidth constraints. The packet size on a CAN network is only 8 bytes, so it would not be feasible to add a digital signature to every packet. Although it is possible to use an end-to-end security protocol for a bulk data transfer such as uploading a new version of the firmware, it would not make sense to batch up real-time control messages in this way, which are relatively short and need to be delivered in a timely fashion. However, standards such as BS ISO 14229, which defines a unified diagnosis service, recognize the need for security controls. The standard includes provision for certain diagnostic operations such as uploading firmware to require the use of a security protocol to "unlock" the required functionality in the target device. Similarly, BS ISO 26021, which deals with end-of-life activation of pyrotechnic devices such as airbags, includes a number of protective features, including the requirement for the necessary software to be loaded into memory before it can be unlocked and activated.

The third approach is the least intrusive, at least at the network level, and a number of companies now offer network intrusion products for automotive in-vehicle networks. These rely on the fact that in order to override the safety function, an attacker needs to send messages at a much higher rate than usual, so anomalous traffic on the network can be readily identified. Responding safely in this situation is more difficult. One possibility might be to attempt to suppress the anomalous messages, allowing only the genuine messages to get through. However, if this is not possible, the intrusion detection device must somehow alert the other devices on the network or the driver that there is a problem, without disabling the vehicle, which could be travelling at speed.

E.3 Securing remote-access to the vehicle

In order to prevent remote attacks on the vehicle, it is necessary to secure the devices that are used as the entry point for such attacks. A defence in depth approach is recommended to guard against the wide range of vulnerabilities that security researchers have discovered with existing devices. Examples of measures that could be deployed to comply with some of the recommendations in Clause **7** are listed below:

a) Requiring end-to-end authentication from caller to vehicle (for example, using public-key cryptography for mutual recognition).

b) Imposing limitations on who is allowed to call the vehicle and what kind of services they are allowed to access remotely.

c) Making the address (phone number) of the vehicle inaccessible to unauthorized parties (for example, the vehicle's network address might only be accessible via a virtual private network).

d) Only accepting incoming connections from authorized parties and only connecting out to authorized known parties.

e) Hardening devices that accept incoming connections against attack – in particular, disabling any unnecessary services or functions so that its attack surface is reduced (this is particularly important if the device contains an embedded operating system).

f) Configuring the system for production mode and disabling any features used for debugging during development.

g) Designing the device in accordance with secure design principles (for example, secure coding guidelines should be followed).

h) Checking all external input for validity to guard against buffer overflow attacks.

i) Including proactive security measures to check that the integrity of the device's firmware or execution state in memory has not been compromised.

j) Requiring an appropriate degree of authorization for performing safety-related functions.

k) Only allowing remotely accessible devices to send a limited number of "white listed" messages to specified devices on the vehicle, and blocking, logging and alerting unauthorized messages.

Note that the ISO 20077 series of standards on Road Vehicles – Extended Vehicle Methodology will contain requirements that automotive manufacturers consider the safety and security implications of any remote service to their vehicles.

E.4 Layered approach to automotive cyber attacks

The most effective protection against automotive cyber-attacks is to adopt a layered approach and assume that all entry points to the vehicle, whether wireless or physical, are potentially vulnerable. Measures are then taken to harden each access point against attack but also to detect successful attacks and limit their propagation within the in-vehicle network. This is the approach advocated by the National Highway Traffic Safety Administration (NHTSA) in the USA, who recommend focusing on four main areas [74]:

a) protective/preventative measures and techniques – reducing the likelihood and impact of a successful attack by isolating safety-critical systems and networks using hardware and software solutions such as network gateways and encryption;

b) real-time intrusion detection measures – continuously monitoring the network for potential intrusions;

c) real-time response methods – measures to mitigate the potential adverse effects of a successful attack, preserving the driver's ability to control the vehicle; and

d) assessment of solutions – information sharing and analysis of potential vulnerabilities and hacking techniques by affected parties, development and dissemination of solutions to other stakeholders.

Annex F (informative)
Security and safety of a composite system

F.1 General

Systems are nearly always developed by the integration of existing products with new ones, by integrating components or subsystems from a supply chain to form the overall 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. Rather, a justification for the overall system is needed.

Sometimes the development of composite systems follows a formalized path – as recommended in ISO 26262, BS EN IEC 62443 and other standards, which tend to focus on physical systems. However, composition involving intangible assets such as information and data is also important, particularly when security issues such as confidentiality is considered. While strict confidentiality concerns are outside the scope of the PAS, it should be borne in mind that threat agents can make use of information to identify vulnerabilities or otherwise aid attacks.

The system structure is defined by an architecture that describes how the components are brought together to form the system. Those parts of the connected automotive ecosystem that use ISO 26262 are familiar with the rather specific terminology it uses. It clarifies distinctions between systems and components:

a) system – set of components that relates at least a sensor, a controller and an actuator with one another;
b) component – non-system level element that is logically or technically separable and is comprised of more than one hardware part or of zero or more software units;
c) hardware part – portion of a hardware component at first level of hierarchical decomposition; and
d) software unit – atomic level software component of the software architecture that can be subjected to stand-alone testing.

Evidence can be provided for components. For ISO 26262 this can be provided in the form of a safety case, for other parts of the ecosystem it could be other forms of evidence (e.g. compliance to BS ISO 27001). In addition to considering how the various attributes of the components behave under composition, how to compose the assurance artefacts is also to be considered. To use this evidence for the assurance case of the overall system, the validity, accuracy, completeness, trustworthiness and comprehensibility of this evidence are to be assessed (e.g. does the evidence relate to the correct product version? Is there enough detail? Is the terminology inconsistent or confusing?).

ISO 26262 does not deal with composition of safety cases directly, but it does define two situations that involve some form of composition. The first situation is a distributed development, where responsibility for developing an item in accordance with ISO 26262 is shared between a customer and one or more suppliers. The details of this collaboration are specified in a development interface agreement. Although there is a shared responsibility and a common objective, the functional safety assessment provided by the supplier is limited in scope and the overall functional safety assessment for the item must be provided by the customer.

The other situation is the use of a safety element out of context (SEooC). In this case, there is no formal relationship or agreement between the customer and supplier. Instead, the supplier develops a general-purpose SEooC under a specific set of assumptions, and it is the responsibility of the customer to decide whether these assumptions are applicable and therefore whether the safety element can be reused or needs to be adapted for a specific context.

F.2 The behaviour of a combined system

The attributes of a composite system are related to the attributes of the component systems or services, but it is not necessarily a one to-one relationship. The composite system can:

a) share some of the attributes of its component systems;
b) have additional attributes due to, e.g. emergent behaviour; and/or
c) mitigate unwanted behaviour of components, e.g. vulnerabilities in one component that are mitigated by another.

In order to assess whether the composite system has the desired properties in a security context, the organization typically considers:

1) initiating events (or attacks);
2) vulnerabilities;
3) potential faults and error conditions;
4) hazards;
5) failures or consequences; and
6) controls, mitigations or barriers.

Table F.1 illustrates analysis of these aspects of the combined system that might be affected by composition. A rigorous approach to approaching issues associated with assuring a composite system is to address questions given in this table.

Table F.1 – Composition questions

Composition question	Security related example
What is the impact on the frequency and nature of attacks?	Do increased attack surfaces or 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? Does the combined system limit the impact of vulnerabilities in individual components?
What is the impact on faults of the overall system?	Is the reliability of the system impacted adversely by the unreliability of a security control?
What is the impact on the nature and consequences of the hazards?	Would a security attack or compromise make different hazards credible or increase the consequences of an accident?
What is the impact on controls, barriers and mitigations?	Are the controls in the different components compatible or interact in an unfortunate way? Does security make any independence or common assumptions invalid? Are there covert channels between the components? Are there common vulnerabilities across components increasing chances of common mode failure?
What is the impact on recovery?	How would an attack on the recovery mechanisms and communication mechanisms impact recovery and the system resilience? Are the mechanisms compatible?

F.3 Impact on ASILs and SILs

The generic safety standard IEC 61508 has the concept of safety integrity level (SIL) and ISO 26262 has a variant of this, known as automotive safety integrity level (ASIL). An ASIL is established by performing a risk analysis of a potential hazard by looking at the severity, exposure and controllability of a vehicle-operating scenario. In particular, combinations of events that can be dismissed as improbable for random failure events become credible if there is a malicious attack. Security issues that impact the assignment and use of ASIL-rated components are illustrated in Table F.2.

Table F.2 – Example impact of security on ASILs

ASIL factor	Example of impact of security
Severity – estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous event.	Greater scope for fleet wide impact and systemic failure. Simultaneous failures become credible, e.g. spontaneous acceleration when brakes fail.
Exposure – state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis.	Unrevealed compromises. Component failure increased due to vulnerabilities (e.g. interactions, resource depletion, memory corruption, message flooding on buses). Greater number of situations become credible due to possible multiple failures or misinformation.
Controllability – ability to avoid a specified harm or damage through the timely reactions of the persons involved.	Use of infotainment to distract and stress driver, confusion with multiple failures, alarm flooding can both reduce controllability or be reason that exposure increased and forces driver error.

As a result, an ASIL assigned to a component from a conventional random failure perspective might be insufficient when potential attacks are taken into account.

F.4 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 can be used as a component in a particular 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.

Annex G (informative)
UK Government CAV cyber security principles

Table G.1 reproduces the CAV principles given in the recent UK Government publication "The key principles of cyber security for connected and automated vehicles" [1] and indicates where they are covered in the main clauses of this PAS.

***NOTE** The CAV principles given in Table G.1 are reproduced from "The key principles of cyber security for connected and automated vehicles" [1] and contain public sector information licensed under the Open Government Licence v.3.0.*

Table G.1 – UK Government CAV cyber security principles

CAV Principle	Relevant Clause in this PAS
1 – Organisational security is owned, governed and promoted at board level.	**3.2.1, 3.2.2**
1.1 – There is a security program which is aligned with an organisation's broader mission and objectives.	**3.1.1, 3.1.2**
1.2 – Personal accountability is held at the board level for product and system security (physical, personnel and cyber) and delegated appropriately and clearly throughout the organisation.	**3.2.1, 3.2.4**
1.3 – Awareness and training is implemented to embed a 'culture of security' to ensure individuals understand their role and responsibility in ITS/CAV system security.	**3.6.1**
1.4 – All new designs embrace security by design. Secure design principles are followed in developing a secure ITS/CAV system, and all aspects of security (physical, personnel and cyber) are integrated into the product and service development process.	**4.3**, Clause **7**
2 – Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain	**3.3, 3.5, 4.2, 4.7**
2.1 – Organisations must require knowledge and understanding of current and relevant threats and the engineering practices to mitigate them in their engineering roles.	**4.2, 5.1, 5.4**
2.2 – Organisations collaborate and engage with appropriate third parties to enhance threat awareness and appropriate response planning.	**8.3**
2.3 – Security risk assessment and management procedures are in place within the organisation. Appropriate processes for identification, categorisation, prioritisation, and treatment of security risks, including those from cyber, are developed.	**3.3, 4.2, 5.8**
2.4 – Security risks specific to, and/or encompassing, supply chains, sub-contractors and service providers are identified and managed through design, specification and procurement practices.	**3.5, 4.7**

Table G.1 – UK Government CAV cyber security principles *(continued)*

CAV Principle	Relevant Clause in this PAS
3 – Organisations need product aftercare and incident response to ensure systems are secure over their lifetime.	Clause **6**
3.1 – Organisations plan for how to maintain security over the lifetime of their systems, including any necessary after-sales support services.	Clause **5**
3.2 – Incident response plans are in place. Organisations plan for how to respond to potential compromise of safety-critical assets, non-safety-critical assets, and system malfunctions, and how to return affected systems to a safe and secure state.	**6.1**
3.3 – There is an active programme in place to identify critical vulnerabilities and appropriate systems in place to mitigate them in a proportionate manner.	**5.4, 5.6, 6.2**
3.4 – Organisations ensure their systems are able to support data forensics and the recovery of forensically robust, uniquely identifiable data. This may be used to identify the cause of any cyber, or other, incident.	**6.5.1, 7.9**
4 – All organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system.	**3.5, 9.4**
4.1 – Organizations, including suppliers and 3rd parties, must be able to provide assurance, such as independent validation or certification, of their security processes and products (physical, personnel and cyber).	**4.4.2, 4.5, 8.3.2**
4.2 – It is possible to ascertain and validate the authenticity and origin of all supplies within the supply chain.	**4.7.1**
4.3 – Organisations jointly plan for how systems will safely and securely interact with external devices, connections (including the ecosystem), services (including maintenance), operations or control centres. This may include agreeing standards and data requirements.	**8.2**
4.4 – Organisations identify and manage external dependencies. Where the accuracy or availability of sensor or external data is critical to automated functions, secondary measures must also be employed.	**3.5, 7.11**
5 – Systems are designed using a defence-in-depth approach.	**7.5**
5.1 – The security of the system does not rely on single points of failure, security by obscuration or anything which cannot be readily changed, should it be compromised.	**7.5.1**
5.2 – The security architecture applies defence-in-depth and segmented techniques, seeking to mitigate risks with complementary controls such as monitoring, alerting, segregation, reducing attack surfaces (such as open internet ports), trust layers / boundaries and other security protocols.	**7.3, 7.5**
5.3 – Design controls to mediate transactions across trust boundaries, must be in place throughout the system. These include the least access principle, one-way data controls, full disk encryption and minimising shared data storage.	**7.5.2**
5.4 – Remote and back-end systems, including cloud based servers, which might provide access to a system have appropriate levels of protection and monitoring in place to prevent unauthorised access.	**6.2.6**

Table G.1 – UK Government CAV cyber security principles *(continued)*

CAV Principle	Relevant Clause in this PAS
6 – The security of all software is managed throughout its lifetime.	Clause **5**
6.1 – Organisations adopt secure coding practices to proportionately manage risks from known and unknown vulnerabilities in software, including existing code libraries. Systems to manage, audit and test code are in place.	**7.14**
6.2 – It must be possible to ascertain the status of all software, firmware and their configuration, including the version, revision and configuration data of all software components.	**7.9.2**
6.3 – It's possible to safely and securely update software and return it to a known good state if it becomes corrupt.	**7.9.4**
6.4 – Software adopts open design practices and peer reviewed code is used where possible. Source code is able to be shared where appropriate.	**8.4.2**
7 – The storage and transmission of data is secure and can be controlled.	**7**
7.1 – Data must be sufficiently secure (confidentiality and integrity) when stored and transmitted so that only the intended recipient or system functions are able to receive and / or access it. Incoming communications are treated as unsecure until validated.	**7**
7.2 – Personally identifiable data must be managed appropriately.	Out of scope
7.3 – Users are able to delete sensitive data held on systems and connected systems.	Out of scope
8 – The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail	**7.4.1**
8.1 – The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external and internal interfaces while remaining available for primary use. This includes sensor jamming or spoofing.	**7.11.6**
8.2 – Systems are resilient and fail-safe if safety-critical functions are compromised or cease to work. The mechanism is proportionate to the risk. The systems are able to respond appropriately if non-safety-critical functions fail.	**7.2**

Bibliography

Standards publications

PAS 1085, *Manufacturing. Establishing and implementing a security-minded approach – Specification*

PAS 1885, *The fundamental principles of automotive cyber security – Specification*

PAS 1192-5:2015, *Specification for security-minded building information modelling – digital built environments and smart asset management*

BS 10754, *Information technology – Systems trustworthiness – Governance and management specification*

IEC 61508:2011, *Functional safety of electrical/ electronic/ programmable electronic safety related systems*

IEC 61511-1, *Functional safety – Safety instrumented systems for the process industry sector* – Framework, definitions, system, hardware and application programming requirements

BS EN IEC 62443, *Security for industrial automation and control systems*

PD ISO/IEC TS 17961:2013, *Information technology – Programming languages, their environments and system software interfaces – C secure coding rules*

PD ISO/IEC TR 24772:2013, *Information technology – Programming languages – Guidance to avoiding vulnerabilities in programming languages through language selection and use*

PD ISO/IEC GUIDE 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

BS ISO/IEC 15026-2:2011, *Systems and software engineering – Systems and software assurance – Part 2: Assurance case*

BS ISO/IEC 27035, *Information technology – Security techniques – Information security incident management*

BS ISO/IEC 27032:2012, *Information technology – Security techniques – Guidelines for cybersecurity*

BS ISO/IEC 29147, *Information technology – Security techniques – Vulnerability disclosure*

BS ISO/IEC/IEEE 15288, *Systems and software engineering – System life cycle processes*

ISO 10393, *Consumer product recall*

BS ISO 26262, *Road Vehicles – Functional Safety*

BS ISO 14229-1:2013, *Road Vehicles – Unified diagnostic services (UDS)*

BS ISO 20077-1, *Road Vehicles – Extended Vehicle (ExVe) methodology – Part 1: General information*

BS ISO 26021-2:2008, *Road Vehicles – End-of-life activation of on-board pyrotechnical devices – Communication requirements*

BS ISO 28000, *Specification for security management systems for the supply chain*

BS ISO 55000, *Asset management – Overview, principles and terminology*

BS EN ISO 22300:2018, *Security and resilience – Vocabulary*

BS EN ISO/IEC 27002:2017, *Information technology – Security techniques – Code of practice for information security controls*

BS EN ISO/IEC 27037, *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*

BS EN ISO/IEC 27042, *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*

Other publications

[1] HM GOVERNMENT. The Key Principles of Cyber Security for Connected and Automated Vehicles, August 2017. https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles. Accessed October 2018.

[2] EUROPEAN COMMISSION. Cooperative, connected and automated mobility (C-ITS), https://ec.europa.eu/transport/themes/its/c-its_en. Accessed October 2018.

[3] HOUSE OF LORDS SCIENCE AND TECHNOLOGY SELECT COMMITTEE, CONNECTED AND AUTONOMOUS VEHICLES. The future?, 2nd Report of Session 2016-17, March 2017.

[4] UNITED KINGDOM. HM GOVERNMENT. Industrial Strategy: Automotive Sector Deal, January 2018.

[5] UNITED KINGDOM. HM GOVERNMENT. National Cyber Security Strategy 2016-2021, 2016.

[6] BLOOMFIELD, R. E, BISHOP, P.G., JONES, C.C.M., FROOME, P.K.D. ASCAD — Adelard Safety Case Development Manual, Adelard 1998, ISBN 0-9533771-0-5.

[7] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). Cyber security and resilience of smart cars – good practices and recommendations, December 2016. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars. Accessed October 2018.

[8] UNITED STATES NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION. Cybersecurity best practices for modern vehicles. Report No. DOT HS 812 333, October 2016.

[9] NATIONAL CYBER SECURITY CENTRE. Networks and Information Systems (NIS) Directive: Security objectives and principles Guidance. https://www.ncsc.gov.uk/guidance/nis-guidance-collection. Accessed October 2018.

[10] RAIL INDUSTRY CYBER SECURITY ASSURANCE GROUP. Cyber Security Assurance Principles, Issue 7, November 2016.

[11] OFFICE FOR NUCLEAR REGULATION. Security Assessment Principles for the Civil Nuclear Industry, v1.0, 2017.

[12] HEALTH AND SAFETY EXECUTIVE. HSG96. The costs of accidents at work. HSE Books, 1993.

[13] BISHOP, P.G. BLOOMFIELD, R.E., GUERRA, S. 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.

[14] ENGINEERING COUNCIL. Guidance on Security. https://www.engc.org.uk/security. Accessed October 2018.

[15] EUROPEAN COMMISSION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[16] EUROPEAN COMMISSION. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[17] NATIONAL CYBER SECURITY CENTRE. The Risk Management Collection, https://www.National Cyber Security Centre.gov.uk/guidance/risk-management-collection. Accessed October 2018.

[18] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. Physical Security, https://www.Centre for the Protection of National Infrastructure.gov.uk/physical-security. Accessed October 2018.

[19] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. Personnel and People Security https://www.Centre for the Protection of National Infrastructure.gov.uk/personnel-and-people-security. Accessed October 2018.

[20] NATIONAL CYBER SECURITY CENTRE. Published Guidance, https://www.National Cyber Security Centre.gov.uk/index/guidance. Accessed October 2018.

[21] NATIONAL CYBER SECURITY CENTRE. Supply Chain Security Collection, https://www.National Cyber Security Centre.gov.uk/guidance/supply-chain-security. Accessed October 2018.

[22] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. Supply Chain, https://www.Centre for the Protection of National Infrastructure.gov.uk/supply-chain. Accessed October 2018.

[23] SAE INTERNATIONAL. J3061-201601 *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,* https://www.sae.org/standards/content/j3061_201601/. Accessed October 2018.

[24] NIST, Digital Identity Guidelines, Special Publication 800-63B, June 2017.

[25] GREAT BRITAIN. Automated and Electric Vehicles Act 2018.

[26] National Cyber Security Centre, 10 Steps: Incident Management, https://www.National Cyber Security Centre.gov.uk/guidance/10-steps-incident-management. Accessed October 2018.

[27] US NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Computer Security Incident Handling Guide, Special Publication 800-61, Rev. 2, 2012.

[28] NATIONAL CYBER SECURITY CENTRE. Secure Development and Deployment, https://www.National Cyber Security Centre.gov.uk/guidance/secure-development-and-deployment. Accessed October 2018.

[29] NATIONAL CYBER SECURITY CENTRE. Security Design Principles for Digital Services, https://www.National Cyber Security Centre.gov.uk/guidance/security-design-principles-digital-services-main. Accessed October 2018.

[30] SAFECode, Fundamental practices for secure software development, Third edition, March 2018.

[31] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). Guide to building secure web applications and web services, https://www.owasp.org/index.php/Guide_Table_of_Contents. Accessed October 2018.

[32] SALTZER, J.H., AND SCHROEDER, M.D. 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).

[33] NATIONAL CYBER SECURITY CENTRE. End User Device Security Collection, https://www.National Cyber Security Centre.gov.uk/guidance/end-user-device-security. Accessed October 2018.

[34] ICS-CERT. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, September 2016.

[35] NATIONAL CYBER SECURITY CENTRE. Certified Products, https://www.National Cyber Security Centre.gov.uk/index/certified-product. Accessed October 2018.

[36] STRAVROULAKIS, P. AND STAMP, M. Handbook of Information and Communication Security. https://www.springer.com/gp/book/9783642041167. Accessed October 2018.

[37] SERMI. Scheme for accreditation, approval and authorization to Access Security-related Repair and Maintenance Information (RMI), May 2016.

[38] US DEPARTMENT OF TRANSPORTATION. National Highway Traffic Safety Administration 49 CFR Part 563 [Docket No. NHTSA-2006-25666] RIN 2127-AI72 Event Data Recorders.

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

[40] CERT. SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems. Software Engineering Institute, Carnegie Mellon University, 2016 edition, 2016.

[41] SCHMITTNER, C., ZHONG, M., SCHOITSCH, E. AND GRUBER, T. A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber Physical Systems. In: Proceedings of the 1st ACM Workshop on Cyber Physical System Security (CPSS), pp. 69-80, 2015.

[42] FOVINO, I.N., MASERA, M. AND DE CIAN, A. Integrating Cyber Attacks within Fault Trees. Reliability Engineering and System Safety. vol. 94, no. 9, pp. 1394 – 1402, 2009.

[43] STEINER, M. AND 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.

[44] BLOOMFIELD R., BENDELE, M., BISHOP, P., STROUD, R. AND TONKS, S. The risk assessment of ERTMS-based railway systems from a cyber security perspective: Methodology and lessons learned. In Proc. First International Conference on Reliability, Safety and Security of Railway Systems, RSSRail 2016, Lecture Notes in Computer Science, Vol 9707, Springer, Cham. https://www.adelard.com/resources/reports/papers/#pa-411. Accessed October 2018.

[45] NATIONAL CYBER SECURITY CENTRE. Technical Risk Assessment and Risk Treatment (IS1 & 2 Supplement), April 2012, https://www.National Cyber Security Centre.gov.uk/guidance/technical-risk-assessment-and-risk-treatment-is1-2-supplement. Accessed October 2018.

[46] NATIONAL CYBER SECURITY CENTRE. Critical Appraisal of Risk Methods and Frameworks, 2016. https://www.National Cyber Security Centre.gov.uk/guidance/critical-appraisal-risk-methods-and-frameworks. Accessed October 2018.

[47] NATIONAL CYBER SECURITY CENTRE. Risk Management Principles, 2016. https://www.National Cyber Security Centre.gov.uk/guidance/risk-management-principles. Accessed May 2018.

[48] NATIONAL CYBER SECURITY CENTRE. Security Governance: Enabling Sensible Risk Management Decisions and Communication, 2016. https://www.National Cyber Security Centre.gov.uk/guidance/security-governance-enabling-sensible-risk-management-decisions-communication. Accessed October 2018.

[49] KELLY, T.P. AND R A WEAVER, R.A. "The Goal Structuring Notation – A Safety Argument Notation", Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, July 2004.

[50] BISHOP, P.G. AND BLOOMFIELD, R. E. A Methodology for Safety Case Development. In: Redmill, F. and Anderson, T. (eds.) Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-Critical Systems Symposium, Birmingham 1998, pp. 194–203. Springer, London, 1998.

[51] SCSC ASSURANCE CASE WORKING GROUP. GSN Community Standard, https://scsc.uk/r141B:1?t=1. Accessed October, 2018.

[52] TOULMIN, S.E. "The Uses of Argument" Cambridge University Press, 1958.

[53] EMMET, L., AND CLELAND, G. 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.

[54] RUSHBY, J. "Mechanized support for assurance case argumentation," in Proc. 1st International Workshop on Argument for Agreement and Assurance (AAA 2013), Springer LNCS, 2013.

[55] RUSHBY, J. The Interpretation and Evaluation of Assurance Cases, Technical Report SRI-CSL-15-01, July 2015.

[56] Bloomfield, R. E. and Netkachova, K. Building Blocks for Assurance Cases. 2nd International Workshop on Assurance Cases for Software-intensive Systems (ASSURE), International Symposium on Software Reliability Engineering, Naples, Italy, 2014.

[57] MOTOR INDUSTRY SOFTWARE RELIABILITY ASSOCIATION (MISRA). Guidelines for Automotive Safety Case Arguments V5, MISRA for public review, Nov 2016.

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

[59] BLOOMFIELD, R.E., NETKACHOVA, K. AND STROUD, R. 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.

[60] NETKACHOVA, K., MÜLLER, K., PAULITSCH, M. AND BLOOMFIELD, R.E. 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.

[61] MCGRAW, G. Software Security – Building Security In, Addison-Wesley, 2006.

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

[63] HORIBA MIRA. MISRA C:2012 Amendment 1 — Additional security guidelines for MISRA C:2012. Nuneaton, Warwickshire, UK, April 2016.

[64] HORIBA MIRA. MISRA C:2012 Addendum 2 — Coverage of MISRA C:2012 against ISO/IEC TS 17961:2013 "C Secure". Nuneaton, Warwickshire, UK, April 2016.

[65] AUTOSAR, Guidelines for the use of the C++14 language in critical and safety-related systems, AUTOSAR AP Release 17-10, 2017.

[66] MOTOR INDUSTRY SOFTWARE RELIABILITY ASSOCIATION (MISRA). MISRA C++:2008 Guidelines for the use of the C++ language in critical systems, 2008.

[67] KOSCHER, K., et al. Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, Oakland, CA, May 16–19, 2010. http://www.autosec.org/pubs/cars-oakland2010.pdf. Accessed October 2018.

[68] CHECKOWAY S., et al. Comprehensive experimental analyses of automotive attack surfaces, USENIX Security, August 10–12, 2011, http://www.autosec.org/pubs/cars-usenixsec2011.pdf. Accessed October 2018.

[69] FOSTER I., et al. Fast and vulnerable: a story of telematics failures, WOOT, August 10–11, 2015, http://www.autosec.org/pubs/woot-foster.pdf. Accessed October 2018.

[70] MILLER, C., AND VALASEK, C. Remote exploitation of an unaltered passenger vehicle, August 2015, http://illmatics.com/Remote%20Car%20Hacking.pdf. Accessed October 2018.

[71] HOPPE, T., et al. Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures, Reliability Engineering and System Safety 96 (2011) 11–25, http://www.sciencedirect.com/science/article/pii/S0951832010001602. Accessed October 2018.

[72] UEDA, H., et al. Security authentication system for in-vehicle network, SEI Technical Review, No 81, October 2015, http://global-sei.com/technology/tr/bn81/pdf/81-01.pdf

[73] PALANCA, A. A Stealth, Selective, Link-layer Denial-of-Service Attack Against Automotive Networks, Department of Computer Engineering, Politecnico di Milano University, 2006, http://hdl.handle.net/10589/126393. Accessed October 2018.

[74] US NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION. NHTSA and Vehicle Cybersecurity, 2016, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/nhtsavehiclecybersecurity2016.pdf. Accessed October 2018.

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com

ISBN 978-0-539-02394-7