

PAS 11281:2018

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



Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2018. Published by BSI Standards Limited 2018.

ISBN 978 0 539 02394 7

ICS 03.080.01, 03.220.20

No copying without BSI permission except as permitted by copyright law.

Publication history

First published December 2018

Contents

Foreword	ii
0 Introduction	iv
1 Scope	1
2 Terms and definitions	2
3 Security policy, organization and culture	5
4 Security-aware development process	9
5 Maintaining effective defences	13
6 Incident management	16
7 Secure and safe design	19
8 Contributing to a safe and secure world	24
Annexes	
Annex A (informative) Risk assessment	26
Annex B (informative) Assurance and safety cases	29
Annex C (informative) Secure versus safe coding practices	33
Annex D (informative) Approaching safety and security integration	35
Annex E (informative) Automotive networks	38
Annex F (informative) Security and safety of a composite system	40
Annex G (informative) UK Government CAV cyber security principles ..	43
Bibliography	46
List of figures	
Figure A.1 – Schematic showing the relationship between causal factors, hazards and accidents	26
Figure A.2 – Extension of Figure A.1 to include security	27
Figure B.1 – The CAE Framework	30
Figure D.1 – A schematic showing how security and safety interact in different scenarios	35
List of tables	
Table 1 – Individual roles	vi
Table B.1 – Vocabulary changes in ISO 26262	31
Table B.2 – High-level safety case requirements: changes in text of ISO 26262	31
Table D.1 – Examples of specific actions relating to the areas covered in the PAS	36
Table F.1 – Composition questions	41
Table F.2 – Example impact of security on ASILs	42
Table G.1 – UK Government CAV cyber security principles	43

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.

The British Standards Institution retains ownership and copyright of this PAS. BSI Standards Limited as the publisher of the PAS reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended PAS and publicized in Update Standards.

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.

- 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.

0.3 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];

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, it 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.