

PAS 1885:2018

The fundamental principles of automotive cyber security – Specification



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 0 580 51152 3

ICS 35.030

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

Publication history

First published December 2018

Contents

Foreword	ii
0 Introduction	iii
1 Scope	1
2 Normative references	2
3 Terms, definitions and abbreviations	3
4 Organization's security context	9
5 Security governance	14
6 Assessing and managing security risk	22
7 Security management over vehicle systems lifecycles	29
8 Working together to enhance system security	32
9 Applying a defence-in-depth approach	34
10 Software trustworthiness	37
11 Management of vehicle system data & information	39
12 Vehicle system resilience	42
13 Bibliography	43
Annexes	
Annex A (informative) Security concepts and relationships	45
Annex B (informative) Case study	47
List of figures	
Figure 1 – Holistic approach to security	10
Figure 2 – Determining the organization's security context	15
Figure 3 – Illustration of security concepts and relationships	23
Figure 4 – Risk management approach	25
Figure B1 – Electric Vehicle Charging	47

Foreword

This PAS was sponsored by the Department for Transport. 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 author Hugh Boyes and to the following organizations that were involved in the development of this PAS as members of the steering group:

- Centre for the Protection of National Infrastructure
- Defence Science and Technology Laboratory
- EP90 Group Ltd
- LDRA Ltd
- Garage Equipment Association
- HORIBA MIRA Ltd
- Independent Automotive Aftermarket Federation
- International Manufacturing Centre, University of Warwick
- Jaguar Land Rover Ltd
- McLaren Automotive Ltd
- National Cyber Security Centre
- NCC Group
- Newcastle University UK
- School of Computing Science, University of Glasgow

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 specification 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

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.

Presentational conventions

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

Commentary, explanation and general informative material is presented in 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

As the level of connectivity of vehicles increases, cyber security is becoming an increasing concern. Recent innovations have made vehicle-related systems more vulnerable to cyber security incidents. Given the constantly evolving nature of the threat environment and the all too frequent emergence of new vulnerabilities in vehicles and vehicle-related systems, there is an ongoing need to maintain awareness and sustain cyber security across the lifetime of vehicles and related infrastructure.

All parties involved in the manufacturing lifecycle, from designers and engineers to retailers and senior level executives, need to understand how to implement and maintain the security of vehicles and associated systems. This PAS is intended to be read in conjunction with “Key Principles of Cyber Security for Connected and Automated Vehicles”¹⁾, published by the UK Government in August 2017. The principles are:

- 1) organizational security is owned, governed and promoted at board level;
- 2) security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain;
- 3) organisations need product aftercare and incident response to ensure systems are secure over their lifetime;
- 4) all organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system;
- 5) systems are designed using a defence-in-depth approach;
- 6) the security of all software is managed throughout its lifetime;
- 7) the storage and transmission of data is secure and can be controlled; and

- 8) the system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail.

NOTE The above principles appear as individual sub-headings underneath the title of the relevant clauses in this document.

The principles and this PAS are intended for use throughout the automotive sector, including Connected and Automated Vehicles (CAV) and Intelligent Transport System (ITS), their supply chains and wider ecosystems.

1) <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles>

This page is deliberately left blank.

1 Scope

This PAS sets out the fundamental principles for the provision and maintenance of cyber security in relation to reducing threat and harm to products, services and systems within increasingly connected and collaborative intelligent transport eco-systems. The concept of an automotive ecosystem encompasses:

- the vehicles;
- related infrastructure, including road-side and remote systems that provide services to the vehicles, their operators, occupants and cargo; and
- the human elements, including vehicle owners and/or operators, designers, manufacturers and service providers.

This PAS is applicable to the security and functional safety aspects of the entire automotive development and use life cycle, including specification, design, implementation, integration, verification, validation, configuration, production, operation, servicing and decommissioning. A lifecycle approach is required to address the risks arising from the constantly changing threat landscape, so as to protect vehicles and vehicle-related systems once they have been delivered to the market.

NOTE PAS 11281:2018 addresses the relationship between automotive safety and security and ISO 26262 addresses the functional safety of road vehicles.

This PAS is intended for use by vehicle manufacturers, Tier-1 and Tier-2 supply chain suppliers, authorized service centres, aftermarket suppliers, road/highways authorities and service providers both to the vehicle and to its occupants and/or cargo. It can also be informative for other stakeholders of the automotive supply chain and the operators of automotive vehicles.

It is recognized that at the date of issue of this PAS:

- a) there is a large fleet of vehicles in use;
- b) these vehicles will have varying degrees of connectivity and automation; and
- c) the degree to which security has been considered as part of the design and manufacture will vary depending on the age, nature and complexity of the vehicle.

The PAS is intended to apply to new or modified products, systems and services and its adoption does not require vehicle manufacturers, suppliers or service providers to apply its provisions retroactively.

2 Normative references

There are no references to external documents considered indispensable for the application of this document (*see 13 for Bibliography*).

3 Terms, definitions and abbreviations

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

3.1 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 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.

3.2 asset data and/or information

data and/or information relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organization

NOTE Asset data and/or information can include design information and models, documents, images, software, spatial information, testing and task or activity-related information.

3.3 board-level management

person or group of people who directs and controls an organization at the highest level

NOTE For example, in some organizations this may be "the board" (i.e. a group of people who officially administer a company, trust, etc.).

3.4 context

circumstances that form the setting for an asset, event, data and/or information, which allows its significance and/or meaning to be better understood

3.5 cyber hygiene

conditions and practices that serve to promote or preserve cyber safety and security by individual system users

NOTE Good cyber safety and security practices are not dissimilar to good health practices related to infection and disease control, i.e. taking appropriate steps to prevent infection (e.g. malware), seeking advice in the case of a suspected infection, and when infection occurs, isolating it or taking steps to prevent further spread.

3.6 data

series of digital or analogue signals or encoded characters stored or transmitted electronically, or marks that are intended to convey information

[SOURCE: PAS 185:2017, 3.1.14, modified]

NOTE 1 Marks can include writing, printed characters or graphics.

NOTE 2 Analogue data varies continuously and relates to natural phenomena such as sounds, natural light, river levels, waves and time. It can also include images such as sketches, drawings and text which have been produced by hand rather than using digital technologies.

NOTE 3 Digital data is represented as binary digits (bits) that have only two states, 0 and 1. This data can be a digital representation of analogue data, captured through a quantization process, or data that was created in digital form, for example as a result of a computer process or by entry using a human interface device (keyboard, touchscreen, stylus, etc.)

NOTE 4 The distinction between data and information is that data does not need to have any meaning attached to it; data becomes information via context.

3.7 data and information sharing agreement (DISA)

set of rules to be adopted by the various organizations involved in a data and/or information sharing operation

[SOURCE: PAS 185:2017, 3.1.19]

3.8 data controller

person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

[SOURCE: Data Protection Act 1998 Section 1 [1]]

NOTE 1 The wording of the definition given in the Data Protection Act 1998 [1] (DPA) will be amended by General Data Protection Regulation (GDPR) [2] Article 4(7).

NOTE 2 Whilst few manufacturers may fall within the scope of the Security of Network and Information Systems Directive (also known as the NIS Directive) [3], data controllers should be aware of its objective regarding managing security risks, protecting against cyber-attacks, detecting cyber security events and minimising the impact of cyber security incidents.

3.9 data sharing

provision of data from one or more organizations to a third-party organization or organizations, the reciprocal exchange of data between organizations, or the disclosure of data between different parts and/or systems of the same organization

[SOURCE: PAS ICO's data sharing code of practice [4], May 2011, modified]

NOTE 1 There are two main types of data sharing:

- a) systematic, routine data sharing where the same data sets are shared between the same organizations, or parts of an organization, for an established purpose; and
- b) exceptional, one-off decisions to share data, for example, in unexpected or emergency situations, the provision of medical or social care data to emergency service first responders when they are responding to an incident.

NOTE 2 Data sharing might take place implicitly as well as explicitly with outsourced services via the use of cloud services where appropriate security measures are not in place.

3.10 disclosure

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

3.11 information

one or more data items that have a context and therefore convey a message or meaning

NOTE 1 A string of characters might be referred to generally as data; but if these characters are understood by a person or a computer program for example, as someone's name, then the characters convey information. Information always involves the presence of data in some format, on some medium, which could be, for example, a physical document, a document image on a screen, or the contents of an electronic file.

NOTE 2 There are alternative definitions of information, but from a security-mindedness perspective the context can increase sensitivity.

3.12 information management

policies, processes, procedures and tasks applied to the data and/or information across its lifecycle to ensure its accuracy, authenticity, confidentiality, integrity and utility

[SOURCE: PAS 1192-5:2015, 3.1.17, modified]

3.13 information sharing

provision of information from one or more organizations to a third-party organization or organizations, the reciprocal exchange of information between organizations, or the disclosure of information between different parts and/or systems of the same organization

[SOURCE: ICO's data sharing code of practice [4], May 2011, modified]

NOTE 1 There are two main types of information sharing:

- a) systematic, routine information sharing where the same information sets are shared between the same organizations, or parts of an organization, for an established purpose; and
- b) exceptional, one-off decisions to share information, for example, in unexpected or emergency situations, the provision of medical or other personal information to emergency service first responders when they are responding to an incident.

NOTE 2 Information sharing might take place implicitly as well as explicitly with outsourced services via the use of cloud services where appropriate security measures are not in place.

3.14 near-miss

incident in which a security incident is narrowly avoided, either by chance or through deliberate action

3.15 need-to-know

grant of access to data and/or information relating to assets for an individual or organization where such access is necessary in order for them to perform their role satisfactorily and safely

[SOURCE: PAS 1192-5:2015, 3.1.18, modified]

3.16 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, 3.1.13]

3.17 pattern-of-life

identification of habits, routines and preferences of individual(s) or group(s), which enable prediction of future actions and/or behaviour

[PAS 185, 3.1.31 modified]

3.18 pattern-of-use

identification of routine actions in the handling, operation and management of assets

NOTE The pattern-of-use of assets could facilitate malicious pattern-of-life analysis by increasing the number of data and information sources that can be combined.

[SOURCE: PAS 185:2017, 3.1.32]

3.19 personal data

data which relates to a living individual who can be identified:

a) from those data, or

b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller (3.1.11)

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

{SOURCE: Data Protection Act 1998 Section 1 [1]}

NOTE Under GDPR [2], Article 4(1), personal data means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity or that natural person”. This definition comes into force from 25 May 2018.

3.20 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, 3.1.22]

3.21 personnel security

system of policies and procedures which seek to mitigate the risk of workers (inside an organization) exploiting their legitimate access to that organization’s assets for unauthorized purposes

[PAS 185, 3.1.36]

NOTE These measures might be applied to all personnel that have access to, or use, the asset over its lifecycle, including personnel employed within the supply chain used to design, create, operate, decommission or dispose of the asset.

3.22 physical security

multi-layering of different physical measures designed to deter, detect or delay an attack or intrusion

[SOURCE: PAS 185, 3.1.37, modified]

3.23 processing

obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data, including:

- a) organization, adaptation or alteration of the information or data;
- b) retrieval, consultation or use of the information or data;
- c) disclosure of the information or data by transmission, dissemination or otherwise making available; or
- d) alignment, combination, blocking, erasure or destruction of the information or data

{SOURCE: Data Protection Act 1998 Section 1 [1]}

NOTE Under GDPR [2], Article 4(2), processing means “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”. This definition comes into force from 25 May 2018.

3.24 referential master data

set of permissible values to be used by other data fields in shared data and/or information sets

3.25 resilience

ability to recover from, or adjusts to, an incident or change

3.26 risk appetite

amount of risk that an organization is willing to seek or accept in the pursuit of its long-term objectives

{SOURCE: Chartered Institute of Internal Auditors [5]}

NOTE 1 Risk appetite might be set in relation to the organization as a whole, for different groups of risks, or at an individual risk level.

NOTE 2 In the vehicle system context, when determining the risk appetite, the needs and perspectives of the organization and vehicle stakeholders should be taken into account.

NOTE 3 Where the organization is a supplier of a component, sub-system or service that forms part of a vehicle or vehicle system, the risk appetite should be consistent with those of the organization(s) who integrate or operate the vehicle system.

3.27 risk capacity

resource(s), including financial, intangible and human, which an organization is able to deploy in managing risk

{SOURCE: Chartered Institute of Internal Auditors [5]}

NOTE The organization's risk capacity is generally wider in scope than the risk appetite of the organization as it represents the limits beyond which the organization could not cope in the event that the risk(s) occur(s). For example, when seeking insurance cover, the organization it assesses what residual risk it is prepared to accept, i.e. its risk appetite which might be reflected in the excess payable if an insured event occurs, whilst the level of cover purchased reflects the risk capacity in respect of the insured risk(s). In assessing its risk appetite and risk capacity an organization considers both the gross risk and residual risk exposures, its reliance on controls and other mitigations, and the cost of implementing them in comparison to the consequences of the risk materializing.

3.28 risk universe

full range of risks which could impact, either positively or negatively, on the ability of the organization to achieve its long-term aims

{SOURCE: Chartered Institute of Internal Auditors [5]}

3.29 sabotage

deliberate, malicious action carried out with the aim of weakening, obstructing, disrupting, damaging or destroying an asset, activity, service, organization or other entity

NOTE Sabotage might also be conducted with the aim of enabling a secondary event that occurs as a result of the original action, to be targeted, for example, the evacuation of a building arising from the sabotage of a fire alarm.

3.30 security

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

{SOURCE: Engineering Council, 2016 [6]}

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.

3.31 security-by-default

adopt an approach to solving security problems at root cause rather than treating the symptoms, thus reducing the overall harm or risk to a particular product, system or service

3.32 security context

environments in which the organization seeks to achieve its objectives and in which its products or services are or may be used

[SOURCE: PAS 555:2013 2.32, modified]

3.33 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 data and/or 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.*

3.34 security-minded

understanding and routine application of appropriate and proportionate security measures in any business situation so as to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities and reduce the risk of security incidents

[SOURCE: PAS 1192-5:2015, 3.1.26 modified]

3.35 security strategy

document setting out the security approach adopted by board-level managers that applies to the organization's business operations, products, systems and services

3.36 sensitive data

data, which depending on its nature and the level of sensitivity, could in the event of unauthorized access or through its loss, misuse or modification, adversely affect the privacy, welfare or safety of an individual or individuals; compromise intellectual property or trade secrets of an organization; cause commercial or economic harm to an organization or country; and/or jeopardize the security, internal and foreign affairs of a nation

3.37 sensitive information

information, which depending on its nature and the level of sensitivity, could in the event of unauthorized access or through its loss, misuse or modification, adversely affect the privacy, welfare or safety of an individual or individuals; compromise intellectual property or trade secrets of an organization; cause commercial or economic harm to an organization or country; and/or jeopardize the security, internal and foreign affairs of a nation

3.38 service

work done to meet some administrative, general or public need

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

3.39 stakeholder

third parties such as persons, personnel, or organizations that have a legitimate interest in the organization's manufacturing activities, and/or the products, systems and any related services it delivers

NOTE *The reference to persons encompasses people affected by the manufacturing operations, customers of the manufacturer, and any vehicle operators or users, or people affected by use of the manufacturer's products, systems and any related services.*

3.40 supplies

asset or assets used to design, build, test, integrate, configure, operate or maintain an element, component, sub-assembly, assembly, unit or sub-system or system that is used by or supports a vehicle system

3.41 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 and any subsequent decommissioning and/or disposal

3.42 system

group of interacting, interrelated, or interdependent elements forming a complex whole

NOTE A system can include physical, digital, process and human elements.

3.43 threat

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

3.44 threat actor

person or organization that can adversely act on assets

3.45 vehicle

self-propelled means by which people or goods may be conveyed, carried, or transported on land, either on or off the public highway, other than those running on rails, and which has at least two wheels

NOTE 1 This encompasses means of transport that may be referred to by users as motor vehicles, motor cycles, passenger cars, goods vehicles, trucks, buses, coaches, etc.

NOTE 2 The vehicle may comprise both the physical entity and off-vehicle services provided to it as part of the vehicle operation or for the benefit of the people or goods that are conveyed, carried or transported by the vehicle.

NOTE 3 The term vehicle should be interpreted as covering connected vehicles, i.e. those where a dedicated bi-directional communications link used by a vehicle system.

[SOURCE: Oxford English Dictionary, modified]

3.46 vehicle system

system that provides functionality for the vehicle its driver, occupants, operators, users or cargo

NOTE 1 The system may be a component within a larger system or system-of-systems, and may be located on or within the vehicle or involve interaction with external systems or the vehicle's environment.

NOTE 2 Vehicle systems include those required to implement smart motorways and intelligent transport systems.

3.47 vehicle system lifecycle

process comprising specification, design, development, production, delivery, installation, integration or testing, configuration, use or operation, servicing/support/repair, upgrading/updating or patching, decommissioning, and recycling or disposal of a vehicle system

NOTE The operation of the vehicle includes functionality such as telematics required to support fleet management systems, and usage monitoring for insurance purposes.

3.48 vehicle systems-related assets

assets used throughout the vehicle system lifecycle

3.49 vulnerability

weakness that can be exploited by one or more threats

3.50 Abbreviations

CPNI	Centre for the Protection of the National Infrastructure
DfT	Department for Transport
DISA	Data and Information Sharing Agreement
GDPR	General Data Protection Regulation
ICT	Information and communications technology
NCSC	National Cyber Security Centre
NIS	Network and Information Systems
OWASP	Open Web Application Security Project
SCSMP	Supply Chain Security Management Plan
SIMP	Security Incident Management Plan
SMP	Security Management Plan

4 Organization's security context

NOTE Where this document refers to activities to be carried out by board-level management, the board-level management may choose to delegate responsibility, but not accountability for performance of those activities.

4.1 Understanding the security context

The organization's board-level management shall research, document and demonstrate an understanding of the security context and the range of potential security issues that are applicable to its business, assets, personnel and the environments and ecosystems in which its products, systems and/or services are or may be used.

NOTE Security operates on a number of levels ranging from national security issues (e.g. the protection against terrorism, tackling organized crime and detecting hostile acts by nation states), to preserving the value, longevity and ongoing use of an enterprise's assets, whether tangible (e.g. a factory or physical stock), or intangible (e.g. preventing the loss or disclosure of intellectual property and nationally or commercially sensitive information). It also includes the handling of privacy issues (e.g. the protection of personally identifiable information). The security levels that need to be addressed by the organization will depend on the nature of their products, systems and/or services and the potential impact that a failure or security incident may have.

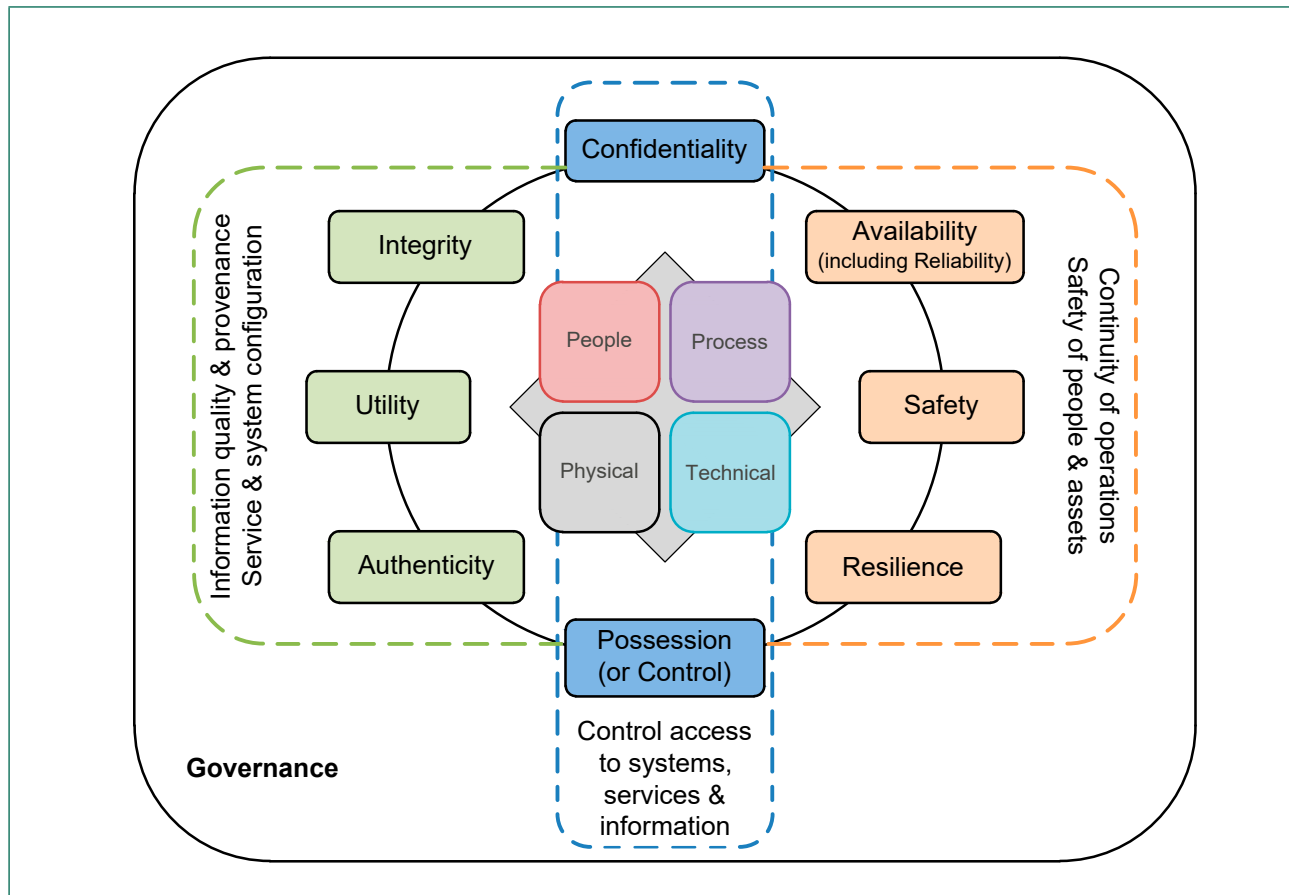
4.2 Holistic approach to security

4.2.1 The organization's board-level management shall demonstrate that effective security requires a holistic approach, as illustrated in **Figure 1**, which addresses security in respect of the following domains as a minimum:

- a) people, i.e. the personnel that have access to its vehicle systems-related assets and the vehicles, products, systems and services that it delivers;
- b) physical, i.e. the physical environment in which the organization's vehicle systems-related assets and the vehicles, products, systems and services that it delivers are designed, created, used, stored, transported and disposed of;
- c) process, i.e. the business processes used to:
 - i) acquire, transport, store, manage, maintain, and dispose of the organization's vehicle system-related assets and the vehicles, products, systems and services that it delivers;
 - ii) manage data and/or information throughout their lifecycle in both vehicle systems-related assets and the vehicles, products, systems and services that it delivers;
 - iii) manage the classification and sharing of data and information, both within the organization and with its supply chain, professional advisers, customers and potential customers; and
- d) technical, addressing security issues arising from the technology, data and/or information used in:
 - i) the design, operation, maintenance or support, decommissioning and disposal of vehicle systems-related assets; and
 - ii) the products, systems and services that the organization delivers;
- e) governance, setting the overall direction and managing the approach across the four security domains (people, physical, process and technology).

NOTE 1 Effective security reduces security risks to the lowest acceptable level having due regard for the severity and likelihood of risks both individually and in combination and their impact on both the organization and its stakeholders.

Figure 1 – Holistic approach to security



NOTE 2 The eight security goals (confidentiality, availability, safety, resilience, possession, authenticity, utility and integrity) are applicable across the four security domains (people, physical, process and technical). For example, the physical composition of a digital processing system can affect the integrity of the data and/or information it processes, which may result in a loss of availability of a safety critical process leading to potential harm to the vehicle's operator, user or occupants, or to a pedestrian.

4.2.2 The organization's board-level management shall be aware of the cyber-physical security risks that arise where digital assets and processes have an impact on the physical characteristics of a vehicle system-related asset and the vehicles, products, systems and services that it delivers.

4.2.3 The organization's board-level management shall demonstrate their understanding of the security aspects identified in 4.2.1 and 4.2.2 through production and maintenance of a security approach (Clause 5).

NOTE The security aspects identified in 4.2.1 and 4.2.2 will be affected by the organization's supply chain and this aspect should be taken into account when developing and reviewing the security approach.

4.3 Automotive security issues

NOTE Advice on the security issues outlined below can be obtained from CPNI and NCSC. This advice encompasses personnel, physical and cyber security.

4.3.1 The organization's board-level management shall research, document and demonstrate an understanding of the risks associated with the following security issues:

- a) hostile reconnaissance (4.3.2);
- b) malicious acts (4.3.3);
- c) loss or disclosure of intellectual property (4.3.4);
- d) loss or disclosure of commercially sensitive information (4.3.5);

- e) release of personally identifiable information (4.3.6);
- f) counterfeit and contaminated supplies (4.3.7); and
- g) aggregation of data and/or information (4.3.8).

4.3.2 For sensitive or potentially sensitive business and/or vehicle systems-related assets, the organization shall consult with appropriate parties to gain an understanding of the range of traditional and evolving techniques of hostile reconnaissance to which the business, its assets (including vehicle systems-related assets) and asset-related digital data and information, and its personnel, could be vulnerable.

NOTE 1 During hostile reconnaissance, the threat actor will be looking for data and/or information:

- that it can exploit about security measures (e.g. physical vulnerabilities or system configuration);
- that can be used to identify modus operandi and increase the chance of success;
- about the state of security (i.e. the chances of being detected and/or prevented);
- about the pattern of life of an individual or group of individuals;
- about the pattern of use of an individual vehicle, group or fleet of vehicles.

From the perspective of the threat actor, achieving successful attack planning depends on the reliability of this information and the ability to acquire it without being detected.

NOTE 2 While there are tools for detecting and reporting physical reconnaissance, the increasing use of digital data and information to support project modelling, digital built environments and smart asset management provides an avenue for hostile reconnaissance that might reduce or eliminate the need for physical reconnaissance prior to launching an attack.

4.3.3 The organization's board-level management shall seek advice regarding the increased business risks associated with the failure or impaired performance of vehicle systems which depend on information and communications technology, or operational technologies, or a combination of both, arising from malicious acts caused by a range of external and insider threats, such as damage caused by malware, hackers or disaffected personnel.

NOTE 1 Widespread use of digital and information technologies creates increased business risks which could manifest themselves as loss of availability, functionality or performance, or the loss or corruption of digital artefacts.

NOTE 2 The use of digital vehicle systems brings an increasing risk that errors and/or the actions of threat

actors may result in the integrity or authenticity of data and/or information being compromised, resulting in a harmful situation or malicious outcome even though the system itself is operating normally. This can affect both reference data and/or information (e.g. the configuration of products or systems) and dynamic data (e.g. routing, navigation and traffic conditions information).

4.3.4 The organization's board-level management shall seek advice regarding the protection of its own and others' intellectual property which it holds or which may be developed, and shall assess the risk and record the potential consequences of the loss of, unauthorized access to/modification of, or improper use or re-use, of that information.

NOTE 1 Intellectual property encompasses a range of material, including trade secrets, proprietary processes, technical specifications and detailed calculations or methodologies. Organizations often invest heavily in the development of intellectual property and through its use, licensing and sale can deliver significant commercial and economic benefits. The piracy, theft or unauthorized use of intellectual property can be damaging to the organization and a country's economy as a whole.

NOTE 2 Some intellectual property is sensitive information that can be used to manifest a physical result in a manufactured object, in which case it irretrievably crosses the cyber-physical boundary. This behaviour has some, but not all, of the characteristics of disclosure, and needs to be taken into account when considering the protection of intellectual property. The sensitive data and/or information might include or reflect:

- a) the composition or treatment of materials used in its manufacture;
- b) proprietary aspects of the manufacturing process; and
- c) where the object contains digital elements, the design and operation of those elements.

NOTE 3 Consideration should be given to the protection of intellectual property from loss, unauthorized access, or improper use or re-use. Scenarios to be considered include:

- a) development and use of intellectual property within the organization;
- b) collaboration with third parties, including universities and research institutes, through the lifecycle of the intellectual property;
- c) disclosure of intellectual property to third parties, including professional advisers and the organization's supply chain;