PAS 1885:2018

The fundamental principles of automotive cyber security – Specification

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2018.

ISBN 978 0 580 51152 3

ICS 35.030

Publication history

First published December 2018

Contents

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.

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 It will be withdrawn upon publication of its content in, or as, a British Standard.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;

NOTE The physical aspects of security include the design, construction, operation and maintenance of the vehicle and vehicle-systems assets so as to prevent unauthorized access to, modification of, or damage which may result in safety or security incidents.

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:

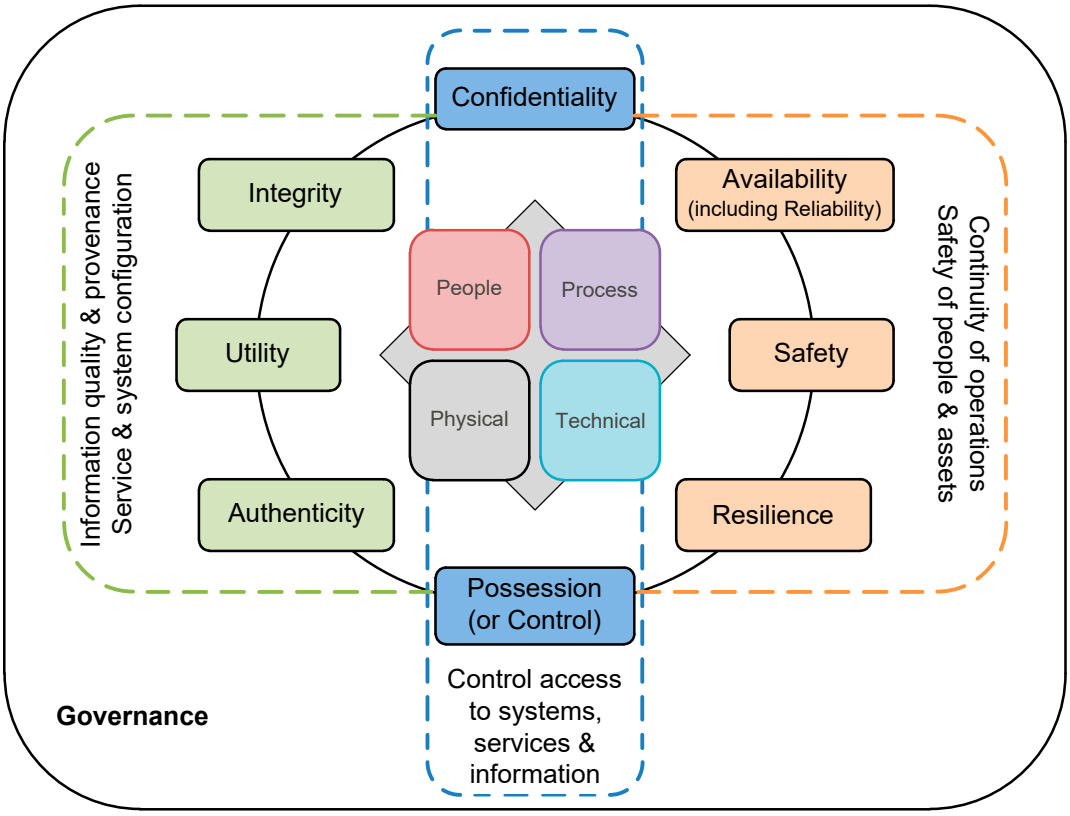
   i) the design, operation, maintenance or support, decommissioning and disposal of vehicle systems-related assets; and

   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;*

d) publication or presentation of data and/or information relating to the intellectual property, for example in white papers, conference or trade publications; and

e) disclosure of intellectual property due to accessible characteristics of a product, system or service itself.

***NOTE 4** Unauthorized modifications to intellectual property can result in economic losses through system failures, introduce vulnerabilities into a design and/or create malicious or unsafe outcomes when the product, system or service is in use.*

4.3.5 The organization's board-level management shall seek advice regarding the protection of commercially sensitive information (for example pricing, price sensitive or market sensitive data or information), especially during a tender or procurement process, and shall understand the potential consequences of the loss of, or unauthorized access to, that information.

***NOTE** In competitive markets there is a need to address the risks of commercial espionage, including measures to prevent the loss of, or unauthorized access to, pricing or price sensitive data. Failure to provide adequate protection of data or information during tendering processes can damage both purchasers and suppliers.*

4.3.6 The organization's board-level management shall be aware of the need to safeguard personally identifiable information processed by vehicle systems, in particular related to the relevant law and/or regulations, such as the Data Protection Act [1] and GDPR [2], and also when responding to requests for information under Environmental Information Regulations [7] or Freedom of Information Act [8 and 9].

***NOTE 1** Unauthorized access to personally identifiable information can enable more targeted social engineering and phishing attacks. This is potentially an issue for:*

a) intelligent transport systems, where the organization processes personal data;

b) services provided by the organization to the vehicle and/or its occupants when the vehicle is in use.

***NOTE 2** The aggregation of personally identifiable information can significantly increase the threat to individuals, or groups of individuals, and the potential impact in the event of a security breach involving unauthorized access to or disclosure of this information. (See also **4.3.8**.)*

***NOTE 3** The objectives of the Security of Network and Information Systems Directive (also known as the NIS Directive) [3] and its supporting principles are relevant when considering the protection of data and information, and/or seeking to reduce the risk and impact of cyber-attacks.*

4.3.7 The organization's board-level management shall apply due diligence to reduce the risk of obtaining counterfeit, maliciously or fraudulently sub-standard, or contaminated items when purchasing assets, including raw materials, ingredients or manufactured items that are used in its own manufactured products or systems and any vehicle related services.

***NOTE 1** The provenance of raw materials, ingredients, manufactured supplies and assets, and the integrity of the supply chain and logistics services used to handle them are both important if an organization is to reduce the risk of inferior, counterfeit or contaminated items entering their supply chain or facility. This might be as a result of the actions or inaction of a supplier or as a result of substitution in the sales and supply chain, for example where supplies are purchased as grey imports, i.e. outside of the authorized supply and distribution channels used by the original manufacturer or material supplier.*

***NOTE 2** Counterfeit supplies are those which are deliberately and fraudulently mislabelled or described with respect to their identity, composition and/or source. Counterfeiting can apply to both branded and generic materials or products and the counterfeit might include elements:*

- *with sub-standard or incorrect ingredients/components;*
- *without or with insufficient key ingredients/components; or*
- *with fake packaging*.

***NOTE 3** Contaminated supplies are those whose composition has been accidentally or deliberately altered or described with respect to their composition, for example purchasing software that has been contaminated by malicious code (malware).*

***NOTE 4** This obligation to manage the risk of counterfeit and contaminated supplies extends across the lifecycle of the vehicle and associated vehicle systems, i.e. it includes the provision of spares, software updates, etc.*

4.3.8 The organization shall consult appropriate parties to establish the increased risks and sensitivity that occurs through aggregation of data and/or information processed by and/or stored in vehicle systems-related assets and vehicle systems, and document its assessment of the risks in the organization's Security Strategy (**5.2**).

NOTE 1 *Individual facts, data or information items might not create a harmful situation, but the aggregation of data and/or information could allow a threat actor to develop a better understanding and more comprehensive picture regarding the operation of a vehicle, vehicle systems or vehicle-related services. For example, when designing a vehicle security system, there will be a need for sensors. Physical information about the size and installation requirements of individual components is unlikely to be sensitive, but the aggregated data and information comprising the detailed system design, including the location of sensors, their capability and field of view, is more sensitive as it would enable an assessment of system capabilities and physical security vulnerabilities.*

NOTE 2 *Information on sources of advice on aggregation security issues include the Centre for Protection of the National Infrastructure (CPNI), the National Cyber Security Centre (NCSC) and the Department for Transport (DfT).*

NOTE 3 *Aggregation of data and/or information can occur through manual or automated processes and refers to where data and/or information is collected and collated, and possibly analysed to allow meaningful and useful interpretation of initially isolated or independent facts, data or information. It has the potential to increase the business impact of any compromise, whether accidental or intentional. The aggregation risks can arise from:*

a) aggregation by accumulation, where the volume of data and/or information stored together increases the level of impact that would occur if the data and/or information was compromised;

b) aggregation by association, where the association of different types of data and/or information, which in themselves have little or no impact when compromised, when associated together, have a higher level of impact;

c) a combination of accumulation and association; or

d) disclosure of too much data and/or information, e.g. in response to a public access request or media enquiry, allowing a third party to draw inferences from the disclosed material or create unplanned associations.

5 Security governance

Principle 1 – Organizational security is owned, governed and promoted at board level.

5.1 Responsibility of board-level management

5.1.1 The organization's board-level management shall own, manage and govern security within the organization and in relation to its supply chain, by adopting a security-minded approach that is documented in a security strategy (**5.4.2**). It shall apply to its business operations, vehicle systems-related assets, and to the vehicles, products, systems and/or services that it delivers.

NOTE** The concept of a holistic security-minded approach is described in Clause **4.

5.1.2 To fulfil the responsibilities set out in **5.1.1**, the organization's board-level management shall establish, document and maintain a record of the organization's context, as illustrated in **Figure 2** by:

a) researching and documenting the organization's business operations, encompassing:
   i) past, present and planned future business activities, including its vehicle systems-related assets;
   ii) the scope, nature and geographic location of its supply chain; and
   iii) the current and foreseeable use of the vehicles, products, systems and/or services that it delivers;

***NOTE 1** This should consider the political, economic (both financial and competitive), social, technological, legal (including jurisdiction, legislation and regulatory) and environmental factors that affect or could affect the organization, but specifically focus on security-related aspects.*

***NOTE 2** Depending on the scope of the organization's activities the above factors might need to be addressed at international, national, regional and/or local levels.*

b) researching and documenting the operating environment of:
   i) the organization;
   ii) its supply chain; and
   iii) its vehicles, products, systems and/or services that it delivers, including post delivery services such as fleet management;

***NOTE** When considering the operating environment of the products, systems and/or services, the organization should take into account both the current environment and likely future environments, for example where products are used in new markets or territories.*

c) identifying, assessing and documenting security requirements arising from contracts and the legislation, regulations and standards applicable to its business operations, vehicle systems-related assets, and to the vehicles, products, systems and/or services that it delivers;

***NOTE 1** Some security requirements can arise from the organization's role within a supply chain, for example where an organization collects and/or processes personal data regarding customers or vehicle users there will be requirements arising from data protection legislation applicable to the territories in which the vehicles are sold and used.*

***NOTE 2** If the organization operates in, and/or its manufactured products are used in, multiple jurisdictions, there might be a complex portfolio of requirements that need to be satisfied.*

d) identifying, assessing and documenting the organization's plans and objectives, the key drivers and trends having impact on them, and the potential security implications;

e) identifying, assessing and documenting the needs and expectations of its stakeholders regarding the security of the organization and its vehicles, products, systems and/or services that it delivers;

f) identifying, assessing and documenting threat landscape, based on the organization's scope as determined in accordance with **5.2** and taking into account known and emergent (i.e. unknown and/or potential) security risks, vulnerabilities and threat actors;

g) determining, documenting and maintaining a record of the organization's:
   1) scope (**5.2**);

***NOTE** The organization's scope encompasses the nature and scale of its past, present and planned or potential future business and manufacturing activities. The scope also determines its current and future security liabilities. Past business activities are relevant as they might result in latent liabilities, for example:*

i) security liabilities arising from known or emergent vulnerabilities;

ii) safety liabilities arising from security vulnerabilities;

iii) product liabilities arising from defects in the manufacturing process, including any associated digital artefacts;

iv) service liabilities arising from failures, including non-availability of any manufacturing related services;

v) professional indemnity liabilities arising from negligent or defective delivery of design or advisory services.

2) governance approach (**5.3**);

3) security context; and

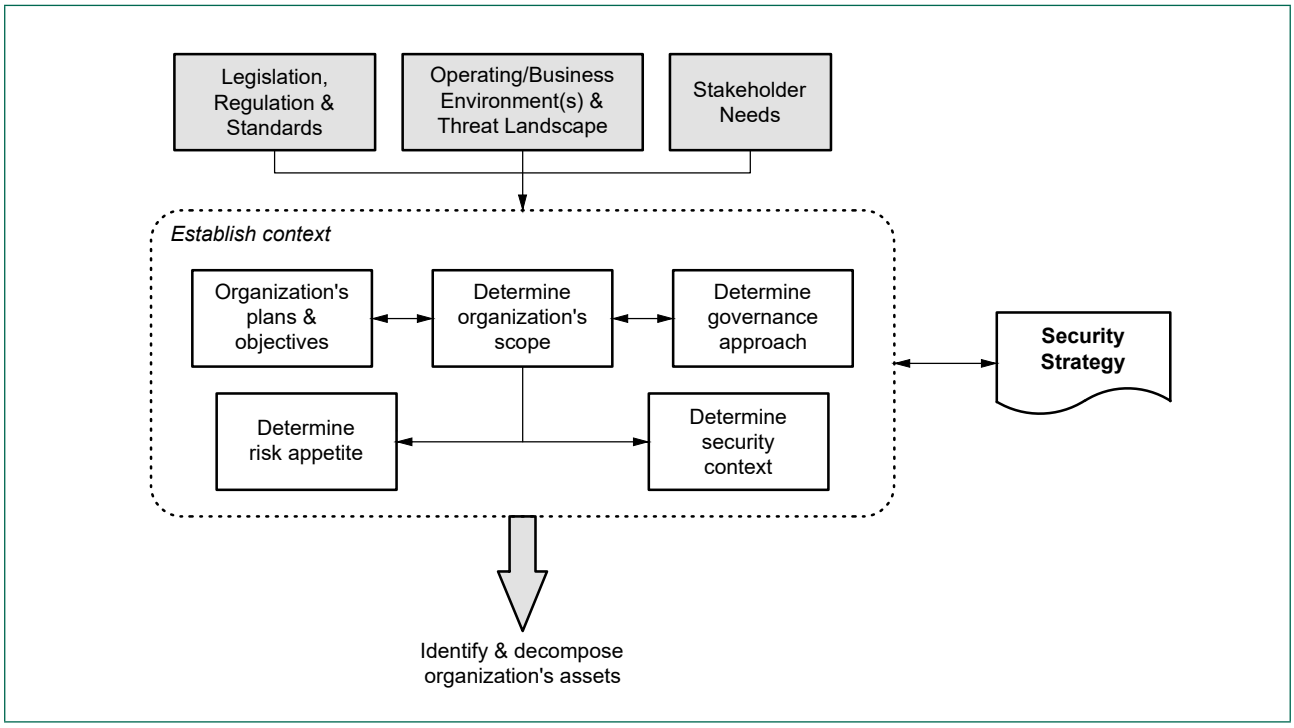
***NOTE** The security context is determined by the scope of the organization, the environment in which the organization operates, the nature and use to which its manufactured items are put, the security threats to which it and similar organizations are exposed, and the nature of vulnerabilities in the products or systems it manufactures.*

4) risk appetite (**5.4**).

***NOTE 1** The risk appetite in respect of a particular product, system or service should not be viewed in isolation, but treated as part of the organization's wider business and operational risk appetite.*

***NOTE 2** Where an organization has existing products, systems or services in use the security context relates to historic, current and emergent security issues. For example, where a legacy product is still in use and a security vulnerability emerges, which if exploited would have serious safety or security consequences, the organization might have a legal responsibility to mitigate the vulnerability.*

Figure 2 – Determining the organization's security context



***NOTE** The stakeholders include potential vehicle driver/operator, the public and third parties affected by the security, or insecurity, of vehicles, vehicle-related systems and any associated services.*

5.2 Determining the organization's scope

The organization's board-level management shall establish, document and maintain a record of the organization's scope, which as a minimum shall comprise an overview of the:

a) organization's current operations, to include:
   i) the locations at which it operates;
   ii) the organization's ICT equipment and systems, including any outsourced or externally hosted components;
   iii) the organization's vehicle system-related assets;
b) type of vehicles, products, systems and/or services that it:
   i) has delivered;
   ii) is currently delivering; and
   iii) that it plans to deliver;

   NOTE *The organization's scope should cover the lifecycle of the vehicles, products, systems and/or services it delivers, e.g. where a vehicle manufacturer provides fleet management services.*
c) organization's supply chain, to include suppliers of:
   i) raw materials or ingredients;
   ii) physical products (e.g. components, sub-assemblies, systems and equipment) which are:
      1) incorporated in its products, systems or vehicles;
      2) used during the design, creation, testing, storage, shipping and maintenance of its products, systems or vehicles; and
      3) used in vehicle system-related assets;
   iii) digital products/artefacts that are used by or to manufacture, shipped with or incorporated in the items listed at **5.2.1 c) ii.**

5.3 Security management and governance

5.3.1 To fulfil the responsibilities set out in **5.1.1**, board-level management shall establish a governance approach and structure to manage the organization's security-related requirements, which is commensurate with the organization's context (**5.1.2**).

NOTE *In developing the governance approach, the board-level management should be cognizant of other disciplines and considerations. For example, the interaction between safety and security, further guidance on balancing these requirements is provided in PAS 11281.*

5.3.2 The security management responsibilities within the organization's board-level management shall:

a) set out the personal accountability of board-level managers for the ownership and management of security risks;
b) where applicable, the arrangements for delegation within the organization of responsibility, but not accountability, for security of specific processes, vehicle system-related assets, products, systems and services; and
c) establish the arrangements for the periodic review and where necessary updating of security management responsibilities to reflect changes to the organization, its business processes, operations, vehicle system-related assets, products, systems and services.

NOTE *The organization's board-level management might consider that an annual or biennial review is appropriate and proportionate, but with the option to conduct ad hoc reviews in the event of serious security incidents and/or prior to any significant changes to the organization, its operations, products and/or services, and any related services.*

5.3.3 Where the organization's board-level management agrees to delegate specific security responsibilities, this shall be documented, and accountability shall remain with the board-level managers.

5.4 Determining the risk appetite

5.4.1 The organization's board-level management shall establish, document and maintain a record of the organization's risk appetite in a statement which:

a) establishes direct links to the organization's plans and objectives;
b) recognizes the organization has a portfolio of objectives, manufactured items, services and projects;
c) establishes a risk management strategy through allocation of resources, including people, the use of processes and the architecture and operation of the organization's physical and technical infrastructure;
d) provides clarity and precision to enable communication or its risk appetite throughout the organization;
e) sets acceptable tolerances and parameters for risk;
f) specifies the frequency of regularly reviews and updates to the statement to address changes in the risk universe and the organization's risk capacity; and

g) establishes the monitoring and assurance policies, processes and procedures required to ensure effective and consistent application of the risk management strategy.

***NOTE** The organization's risk appetite may vary depending on the context, nature of the risk(s), including their likelihood and potential impact.*

5.4.2 The organization's board-level management shall review the organization's risk appetite as part of the annual financial audit process to take account of changes in the organization's context.

***NOTE** Whilst the organization's risk appetite should be considered as part of the audit process, the management of security should not be considered solely in the realms of the financial audit and any associated reputational harm (i.e. impact to goodwill), but also considered in design reviews, code review, quality assurance, and thus be embedded in all aspects of operation of the organization.*

5.5 Organization's Security Strategy

5.5.1 The organization's Security Strategy shall:

a) be aligned with the organization's broader mission and objectives;

***NOTE** For example, if the organization's human resource strategy involves employment of contractors to fill certain roles or give flexibility to meet varying demand, then the Security Strategy should address the need to have appropriate plans, policies, processes and procedures in place to consistently manage personnel security, taking into account the sensitivity and security risks associated with individual roles.*

b) set out the personal accountability of board-level managers for the ownership and management of security risks and, where applicable, the arrangements for delegation within the organization of responsibility, but not accountability, for security of specific processes, assets, products, systems and services;

c) establish the security goals in respect of:

i) the business architecture and its through-life management of the organization, its products, systems, services, processes and structures;

ii) capability development through security awareness initiatives, training and development so that personnel can acquire and maintain awareness and competence to fulfil their roles in a security-minded fashion and contribute to an effective security culture; and

iii) management of security risks across the organization, its supply chain, customers and end users;

d) establish the need for and scope of a reporting system used to inform board-level managers of the effectiveness of security measures, including handling of security incidents and any subsequent mitigation activities or improvement initiatives;

e) set out the process that is to be regularly used to review and maintain the organization's security to reflect changes in the security context though:

i) implementation of new or amended legislation, regulation and standards;

ii) developments in the organization's structure, business plans and objectives;

iii) developments in stakeholder needs, the operating environment for the business and its products, systems or services;

iv) changes to the threat landscape, for example emerging risks.

f) commit the organization to adoption of industry standards as mitigation of cyber risks of connected vehicles.

5.5.2 The organization's board-level management shall ensure that the Security Strategy is reviewed at least annually or earlier:

a) if there are significant changes to any of the items listed in **5.5.1 e**); or

b) following a security incident, or a near miss (i.e. a narrow avoidance of a security incident).

5.6 Asset-based Risk Register

5.6.1 The organization's board-level management shall develop, document and maintain an Asset-based Risk Register using the approach set out in **Clause 6**.

5.6.2 The information contained in the Asset-based Risk Register, either in whole or in part, is sensitive information. The organization's board-level management shall require that access to it is managed on a need-to-know basis, with security measures implemented that are appropriate to the level of risk, with regard to its creation, storage, distribution and use.

5.7 Security Management Plan (SMP)

5.7.1 The organization's board-level management shall develop, document, implement and maintain a SMP that addresses the specific security objectives in the organization's Security Strategy and the security risks and combinations of risks identified in the organization's Asset-based Risk Register.

5.7.2 The SMP shall apply across all of the organization's activities, in particular in respect of:

a) sharing of data and information;

b) the development and delivery of new vehicle-related products, systems and/or services that will form part of a vehicle or the wider vehicle ecosystem; and

c) the operation, delivery, evolution and disposal of vehicle systems-related assets and services, whether for use as part of the organization's operations or for delivery to or use by a third party.

***NOTE** During vehicle operation there may be a range of services provided in support of its use, for example, fleet management, breakdown and recovery, asset tracking and condition monitoring. These services should be taken into account when developing the SMP, particularly where they require connectivity to vehicle systems.*

5.7.3 The SMP shall cover the people, process, physical and technological aspects of the organization's operations by addressing the following elements:

a) policies which set out the security-related business rules derived from the organization's Security Strategy;

b) processes which are derived from the security policies and provide guidance on their consistent implementation throughout the lifecycle of the asset;

c) procedures that comprise the detailed work instructions relating to repeatable and consistent mechanisms for the implementation and operational delivery of the processes;

d) the monitoring and auditing requirements that will be used to measure effectiveness of the plan and compliance with policy, processes and procedures;

e) the mechanisms for reviewing and updating the SMP and related documents;

f) a Security Incident Management Plan (**5.8**); and

g) a Supply Chain Security Management Plan (**5.9**).

***NOTE** Depending on the size and/or nature of the organization the Security Management Plan may be a single document containing all of the elements listed above or it may be an overarching document that references a suite of documents covering the elements.*

5.8 Security Incident Management Plans (SIMP)

5.8.1 The organization's board-level management shall develop, document, implement and maintain a SIMP tailored to:

a) the organization, its function and supply chain;

***NOTE 1** The SIMP should address reporting both upstream (i.e. from a supplier to the operator/user/purchaser of their products, systems and/or services) and downstream (i.e. to a supplier when an incident or potential incident arises that relates to the security of their products, systems and/or services).*

b) legal, regulatory and contractual requirements that affect the organization and its products, systems and/or services;

c) the vehicle systems-related assets over the lifecycle of any related products, services or vehicle systems;

d) the products, systems and services it delivers, as used by or embodied in vehicle systems over the lifecycle of the vehicle, service or vehicle system.

***NOTE 2** The term lifecycle refers to the period from definition of a requirement for an object (e.g. vehicle, products, or vehicle systems) or service through to its decommissioning, decomposition or destruction at the end of its useful life.*

5.8.2 The organization's board-level management shall require that the SIMP is developed, employed and maintained as described in **7.1**.

5.8.3 Access to any part of the SIMP which details sensitive information (for example, risks to the organization, its function, vehicle systems-related assets, personnel and third parties) shall be managed on a strict need-to-know basis, with the information contained within it subject to appropriate security measures with regard to its creation, storage, distribution and use. Key parts of the Security Incident Management Plan shall be widely available and shall therefore be written to enable, in the main, distribution to all personnel.

***NOTE** A balance needs to be struck regarding the implementation of a strict need-to-know. The organization needs to adopt a risk-based approach to managing the dissemination of all or parts of the SIMP, taking into account the role of the personnel, third party organizations and/or suppliers to who it is disclosed. Where some or all of the SIMP is provided to a third party, the organization should consider putting in place appropriate contractual measures or employing a Data and Information Sharing Agreement (see **5.10**).*

5.9 Supply Chain Security Management Plan (SCSMP)

5.9.1 The organization's board-level management shall develop, document, implement and maintain a SCSMP that defines the contractual and operational measures required for the adoption of an appropriate and proportionate security-minded approach throughout the organization's supply chain.

NOTE *Managing a complex supply chain and its inherited risks is challenging as there is a loss of visibility and understanding as one moves further away from the purchaser through layers of contracts/ sub-contracts. Further guidance regarding risks management in supply chains can be found in NIST 800-161 [10] and on the NCSC website[2)].*

5.9.2 The organization's board-level management shall require that the SCSMP is developed, employed and maintained as described in **8**.

5.10 Data and Information Sharing Agreement (DISA)

5.10.1 The organization's board level management shall develop, implement and periodically review an overarching policy regarding the sharing of data and/ or information, taking into account the corporate risk appetite and providing an aggregated view of the acceptable level of sharing.

NOTE *This policy shall be used to inform the development, acceptability, application, and termination or retirement of individual DISAs.*

5.10.2 The organization's board-level management shall put in place a DISA prior to sharing of any sensitive or potentially sensitive data or information that could be used to cause harm to vehicle systems-related assets, vehicle-related products, systems and/or services, vehicles and their use or occupants.

NOTE *The aim of the DISA is for the party providing the data and/or information to put in place appropriate and proportionate controls on its use by the recipient, it is intended to have legal effect, i.e. the parties involved can seek legal remedies in the event of a breach of the agreement.*

5.10.3 **5.10.2** shall apply to all situations where the organization is:

a) designing, implementing or operating systems or services that process data or information relating to:
   i) vehicles and their use, location, or ownership; or
   ii) vehicle occupants; and
b) this data or information will be:
   i) shared with or processed by a third party, either:
   ii) in the organization's supply chain; or
   iii) as part of a service provided by the organization

NOTE *the term process data should be interpreted as encompassing the various aspects of data processing covered by the UK Data Protection Act and the General Data Protection Regulation (GDPR), i.e. the creation or collection, processing, storage, retrieval and deletion of data or information.*

5.10.4 A DISA shall detail, as a minimum:

a) the purpose, or purposes, of the sharing;
b) the potential recipients, or types of recipient, and the circumstances in which they may access or use the data and/or information;
c) the type of data and/or information to be shared;
d) the monitoring and auditing of the implementation of the sharing agreement;
e) the quality of the data and/or information to be shared, in particular its authenticity, coverage, accuracy, relevance and usability;
f) the requirements in relation to;
   i) where relevant, data protection;
   ii) permitted and prohibited rights of use of the data;
   iii) obligations to notify the data owner and/or data controller in the event of a security incident, or any complaints regarding the quality of the data or information

NOTE 1 *The obligations should reference the relevant security incident management policies, processes and procedures (**5.8**).*

NOTE 2 *Given the international nature of the automotive sector differences in handling of data and information arising from variations in legal and/ or regulatory requirements in different jurisdictions will need to be taken into account.*

g) data and/or information maintenance, including responding to notification of requests for erasure or correction;
h) data and information security, including the handling of security incidents and investigations undertaken by data protection authorities;

[2)] NCSC Supply Chain Collection – https://www.ncsc.gov.uk/guidance/supply-chain-security

i) the arrangements for retention and/or purging of shared data and/or information;

j) procedures dealing with data subjects' rights, including access requests, queries and complaints; and

k) sanctions for failure to comply with the agreement and/or a security incident(s) caused by an individual member of staff.

5.10.5 In the event of a security incident, or if there is evidence that data or information is not being managed and handled in accordance with the data and information sharing agreement, the organization shall have the authority to:

a) suspend the sharing agreement until the event or concerns have been investigated and any remedial measures have been agreed and implemented; or

__NOTE__ Depending on the terms of the agreement, suspension may limit or prevent:

i) further sharing of new data or information; and/or

ii) use of existing share data or information;

b) terminate the sharing agreement and require purging or secure deletion of the shared data and/or information if the matter cannot be satisfactorily remedied.

__NOTE__ Depending on the nature of the breach there may be legal and/or regulatory requirements concerning its reporting. Where such requirements exist the DISA should address the responsibilities of the parties involved to provide the necessary reporting in a timely manner.

5.10.6 The DISAs shall be periodically reviewed, to establish the effectiveness of the sharing and to confirm that:

a) the data and/or information shared is precisely what was agreed, i.e. no more data and/or information (e.g. additional attributes) has accidentally been made available;

b) there is still a legitimate purpose for the continued sharing of data and/or information;

c) the recipients of the data and/or information still need access to it, and where they do not, that access has been withdrawn;

d) the data and information quality and maintenance are to the agreed standards;

e) the data security arrangements remain appropriate and proportionate, and that any complaints have been satisfactorily resolved.

5.11 Organization's security program

To facilitate a consistent organization-wide approach to security, the organization's board-level management shall establish and maintain a security program, that:

a) is aligned to the organization's Security Strategy (**5.5**);

b) supports the SMP (**5.7**);

c) develops and periodically reviews the organization's security objectives;

d) plans and implements the steps to achieve them;

e) monitors the implementation of the plan and fulfilment of the objectives;

f) assigns and manages ownership of the objectives and any implementation plans to achieve them; and

g) monitors the threat landscape (**6.5**).

5.12 Organization's security culture

5.12.1 The organization's board-level management shall embed a security culture within its personnel and suppliers, through the provision of **5.12.2** to **5.12.4** below.

5.12.2 The organization's board-level management shall provide general security awareness training to all personnel, which as a minimum addresses the following topics:

a) cyber hygiene;

b) protection of data and information, including policies and procedures related to sharing with third parties or publication of data or information about vehicle systems; and

c) the organization's policies and procedures regarding the security of its information, communications and operational technologies.

5.12.3 The organization's board-level management shall identity high-risk roles in the lifecycle of its products, systems and/or services and any additional security training that may be required by personnel occupying these roles.

5.12.4 The organization's board-level management shall ensure that personnel occupying high-risk roles, as identified in **5.12.3** are:

a) aware of their security responsibilities;

b) accountable for their security-related behaviour; and

c) in receipt of any additional briefing or training so that they can fulfil their role in a security-minded manner.

5.13 Secure-by-Design

The organization's board-level management shall establish, document and operate policies, processes and procedures such that all new designs are conceived and implemented using a product and/or service lifecycle that embraces Secure-by-Design.

NOTE *The UK Government has published a report[3)] advocating a fundamental shift in approach: moving the burden away from consumers having to secure their devices or products and instead ensuring that strong security is built in.*

[3)] Secure by Design Report – available: http://www.gov.uk/government/publications/secure-by-design

6 Assessing and managing security risk

Principle 2 – Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain.

NOTE *When identifying potential security risks, it is appropriate to consider them from a number of perspectives, including:*

- *Operational, i.e. the potential impact on the business through disruption of business and/or manufacturing activities, reputational damage;*
- *Confidentiality and privacy, i.e. the loss of or unauthorized access to sensitive information and/or personally identifiable information;*
- *Safety, i.e. the potential harm to individuals, assets or the environment arising from the failure, in whole or in part, or misuse of manufacturing-related systems or the manufactured products and/or systems and any related services;*
- *Financial, i.e. the costs associate with managing and responding to a security incident, any subsequent legal costs, fines, etc., the potential loss of income or profit as a result of diverting resources during a security incident response, and any financial loss to individuals and/or third parties;*
- *Legal arising from non-compliance with legislation or regulations, e.g. data protection;*
- *Third parties, arising from harm caused to one or more third parties, for example spreading malware to third party products or systems, provision of inaccurate or misleading data or information leading to corruption of databases, etc.*

6.1 Security risk management approach

6.1.1 The organization's board-level management shall establish, document and operate an appropriate and proportionate approach to security risk management that takes into account the organization's risk appetite (**5.4**).

6.1.2 The organization's risk management processes shall encompass identification, categorization, prioritization and treatment of security risks.

6.1.3 The organization shall demonstrate through its policies, processes and procedures an understanding of the concepts and relationships summarized in **Figure 3**, described in **Annex A**, as they relate to the assets, particularly vehicle systems-related assets, vehicle-systems-related products, systems and services and the supply chain.

NOTE *When considering assets, the definition in **3.1** should be taken to include people, property and the environment.*

6.1.4 The organization's board-level management shall consider security risks and issues in respect of:

a) the threat landscape, for example identification of new vulnerabilities, threats or hazards, and threat actors;

   NOTE *Organizations may seek and support forums with wider ecosystem experience and peers to securely share information on the threat landscape.*

b) the organization's business objectives, scope and security context;

c) its vehicle systems-related assets, including acquisitions, decommissioning, disposals, or significant changes to their construction, configuration, operation or maintenance;

d) the nature, functional design, composition, configuration, installation, operation or maintenance of its vehicle systems-related assets, products and/or systems and services;

e) the additional risks that may arise as a consequence of integrating multiple vehicle-related products and/or systems, within a wider ecosystem;

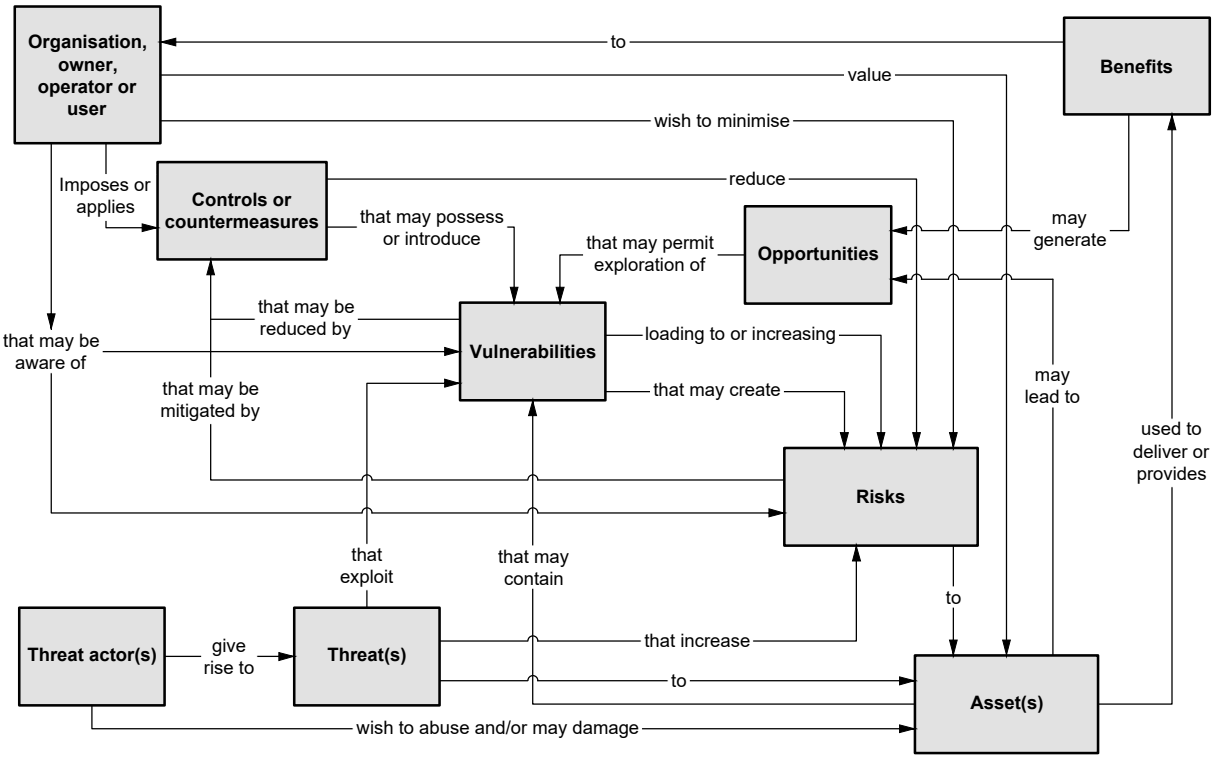
   NOTE *The wider ecosystem may encompass vehicle and/or occupant or cargo related services requiring flows of information between:*

   - *vehicles,*
   - *the vehicle and transport infrastructure,*
   - *the vehicle and external services (e.g. infotainment, road charging or logistics operations).*

f) the design, implementation, operation and delivery of any services it delivers;

g) the current, planned and potential use of vehicles, products, systems and/or services that it delivers;

Figure 3 – Illustration of security concepts and relationships



Developed from BS ISO/IEC 18408-1:2009

h) the supply chain, considering both the suppliers and the materials, products, systems or services they supply;

i) the governance, security, privacy and data protection implications of sharing data and/or information across multiple organizational and/or jurisdictional boundaries; and

j) the impact on others arising from a failure to implement appropriate and proportionate security measures in respect of **(a)** to **(i)** above.

NOTE *Products and/or systems, and any related services, are not likely to be safe if not appropriately secured. The relationship between safety and security is addressed in PAS 11281. The organization should adopt a holistic approach to risk management that takes into account the different expertise and domains needed to deal with different types of risks.*

6.1.5 The organization shall research, document and manage security risks arising from their supply chain, including sub-contractors and service providers, by employing documented and auditable design, specification and procurement practices.

6.1.6 The organization's board-level management shall be aware of the range of potential security risks, and the impact and issues that may arise in the event that a security incident occurs, including those risks which:

a) are applicable to its business, vehicle systems-related assets and personnel;

b) could involve and impact on stakeholders and other parties in respect of products or systems embodied in vehicles that are in use; and

c) are associated with the failure or impaired performance of vehicle related systems that depend on information and communications technology, both internally and within the supporting supply chain.

6.1.7 When designing vehicle-related products, systems or services, the organization shall document and maintain an up-to-date assessment of the associated security risks arising from people, process, physical and technological aspects, both individually and in combination. This assessment shall include risks arising from:

a) the technology and/or software employed, and the ease with which it can be attacked or subject to unauthorized modification;

b) the role of function of the product, system or service;

c) the vehicle systems lifecycle;
d) the through life supply chain employed; and
e) the degree to which good security practice has been employed in its design and manufacture or supply.

6.1.8 In respect of any personal data processing by a vehicle system, the organization shall identify, document and demonstrate an understanding of:

a) the risks to the data or information;
b) the risks arising from associations and behaviours that may result in disclosure, or lead to unintended release of information about, the pattern-of-life of individuals and/or pattern-of-use of the vehicle; and
c) the measures and/or actions required so that the risks can be minimized, mitigated or managed in a timely manner, in accordance with the organization's business scope, obligations and risk appetite.

6.2 Asset-based Risk Register

6.2.1 The organization's board-level management shall develop, document and maintain an Asset-based Risk Register, which encompasses the known security risks to organization's assets as defined in **6.1.3**, and where the scope of the risk assessment for the assets is consistent with:

a) the security context of the organization;
b) the Security Strategy that has been approved by board-level managers.

***NOTE** In considering known risks this should be interpreted as encompassing the security risks which it could reasonably be judged to affect the items listed in **6.1.3**. For example, if the organization is delivering a web-based customer support service, it would be reasonable to expect that the website has addressed known technical vulnerabilities including, for example, the OWASP[4] top 10 web application vulnerabilities.*

6.2.2 The Asset-based Risk Register shall contain:

a) a list of the organization's:
   i) business assets;
   ii) vehicle system-related assets;
   iii) vehicle-related assets; and
   iv) external suppliers of the above assets and any asset related services;

   ***NOTE 1** The use of the term asset in this **6.2.2** includes asset data and/or information and inventory or stock items that are available but not yet in use.*

   ***NOTE 2** Depending on the organization and its business operations, the scope of (iv) above potentially extends to provision of services during the operational use of the vehicle. For example, the vehicle manufacture needs to be cognizant of the risks to vehicle systems that may arise from the connection of third party assets to the vehicle for fleet management or similar purposes.*

b) a cyber security maturity review of the suppliers identified in **6.2.2 a) iv**;

   ***NOTE 1** The review should consider the impact of a cyber security incident affecting an external supplier could have on the organization's operation, on vehicle system-related assets and vehicle-related assets, and any associated services.*

   ***NOTE 2** The maturity review should be conducted using a recognized methodology, model or approach.*

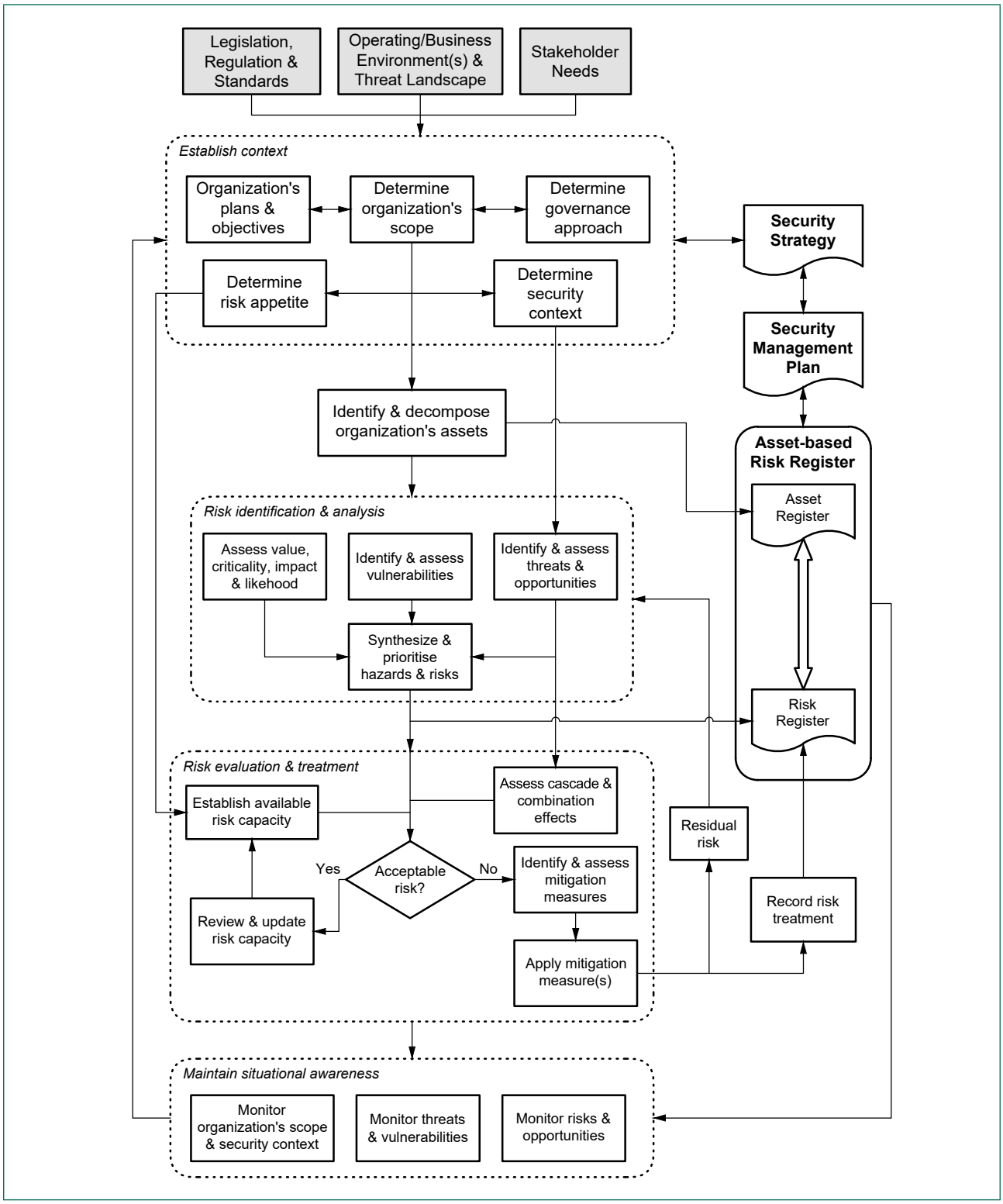
c) appropriate and proportionate decomposition of the assets listed at **a)** to the level at which they are supplied to, purchased, licensed or created by the organization;
d) contain the risks related to:
   i) the organization;
   ii) its supply chain;
   iii) vehicle system-related assets; and
   iv) the vehicles, products, system and services that it delivers;
e) allow separation and analysis of the risks by:
   i) the categories listed in **6.2.2 a)** above, taking into account the decomposition required at **6.2.2 c)** above;
   ii) individual suppliers in its supply chain;
   iii) where known, the products, systems or services in which the manufactured items, and any related services, are used or installed;
   iv) customers, where the organization is not selling its products, systems or services to the end consumer; and
   v) the compromise of vehicle safety.

***NOTE** Where the organization is selling its products, systems or services to a systems integrator, manufacturer or assembler, it is the identity of this third party that should be recorded so that they can be notified of any future security issues.*

6.2.3 Based on the scope and security context of the organization (**4.1** and **5.2**) the organization's board-level management shall require that the Asset-based Risk Register is developed using the approach outlined in **Figure 4**, applying the process described in **6.3**.

[4] See https://www.owasp.org

Figure 4 – Risk management approach



6.2.4 The organization's board-level management shall require that for each risk in the Asset-based Risk Register shall record:

a) a unique risk identifier;

b) a name or title for the risk;

c) the asset(s) affected by the risk;

d) the scope of the risk, including details of the possible risk event(s) and their size, type and number;

NOTE *The scope of the risk determines the boundaries of the impact, for example whether a risk affects multiple items as it arises from a component within them, for example a defect in an integrated circuit, circuit board or piece of software.*

e) the stakeholders, both internal and external, and their expectations in the event that a risk event occurs;

f) the risk evaluation, including the likelihood of an event occurring and its magnitude, and potential impact or consequence should the risk materialize at the assessed level;

g) any loss experience, for example information from previous incidents and any prior experience of loss events related to this risk;

h) risk tolerance or limit for the risk, i.e. the acceptable loss potential or financial impact in the event that a risk event occurs, and any targets for controlling the risk or limiting performance impact;

i) the risk response, treatment and controls, i.e. the mechanisms to be used to manage the risk and control its impact and the mechanisms to be used to monitor and review their performance;

j) the potential for risk improvement, i.e. the potential for cost-effective risk improvement or modification, timescales and responsibility for implementation; and

k) the ownership of the risk, i.e. who is responsible for monitoring compliance with any controls and the risk management strategy.

NOTE 1 *Unless explicitly delegated as part of the Security Strategy, the risk owner should be a board-level manager.*

NOTE 2 *The consequences or impact of a risk materialising can be negative (i.e. hazard risks), positive (i.e. opportunity risks) or may result in further uncertainty.*

6.3 Risk identification, analysis, evaluation and treatment

6.3.1 The organization's board-level management shall identify and decompose organization's assets to an appropriate level.

NOTE 1 *In a similar manner to techniques such as Failure Mode Effects Analysis (FMEA) there is likely to be a need to decompose complex or hybrid assets into their constituent parts. For example, in a cyber-physical system there is a need to consider the risks associate with the physical elements, the cyber (digital elements) and their combination. The decomposition might therefore consider the risk of vandalism or malicious damage so key physical components as well as the threats arising from hackers or malware that affect the digital control systems.*

NOTE 2 *When considering what is an appropriate level to decompose the assets to, the objective is to identify the lowest level at which risk is going to be managed. For example, when considering an office computer, the minimum decomposition may be applications, operating system, processing hardware and any networking or communications connectivity. Depending on the nature of its use and the sensitivity of any data or information processed on it, additional decomposition may be required to cover data storage and any access control mechanisms.*

6.3.2 For each asset the organization's board-level management shall:

a) assess and identify its criticality and the impact of:
   i) its loss, corruption or compromise;
   ii) its failure, either partially or as a whole;
   iii) its misuse or abuse (whether unintentional or malicious);
   iv) its incorrect operation on the manufactured item;

b) identify and assess its vulnerabilities; and

c) identify and assess potential threats and opportunities;

6.3.3 The organization's board-level management enumerate and assess the likely threat actors, considering their motivation, capability and priority.

6.3.4 Using the information gathered in **6.3.1**, **6.3.2** and **6.3.3**, the organization's board-level management shall synthesize and prioritize the potential risks to the organization, its vehicle systems-related assets, and to the vehicles, products systems and services that it delivers.

6.3.5 The organization's board-level management shall consider the security risks that arise through the composition and integration of components, sub-systems and systems, and where appropriate their interaction as systems-of-systems.

***NOTE** The composition and integration risks arise from the selection of elements and how they are integrated. Complementary weaknesses in two or more products that are being integrated may significantly increase the risks of exposure of the combined vulnerability and subsequent exploitation.*

6.3.6 The organization's board-level management shall consider risks arising from data and/or information aggregation:

a) within the organization; and

b) through the data and/or information generated and/or processed by its products and/or systems, and any related services.

***NOTE** See **4.3.8** for further information on data and information aggregation.*

6.3.7 The organization's board-level management shall consider risks arising from data and/or information that is critical to automated and/or safety critical functionality. As a minimum this should include:

a) assessing the impact of loss or corruption of:

   i) sensor data and/or information; and

   ii) external data and/or information;

b) the identification, assessment and recording in the Asset-based Risk Register the safety and security risks across a range of possible scenarios, and where such risks cannot be tolerated ensure that they are mitigated;

c) implementing appropriate and proportionate measures, to maintain safety critical functions where such functionality may be lost or significantly impaired in the event of a cyber-related incident.

6.3.8 Taking each of the risks in turn, as part of an iterative process, the organization's board-level management shall consider the acceptability of the risk, taking into account:

a) the available risk capacity of the organization;

b) the combinational effects of risks; and

***NOTE** Combinational effects occur where there is a linear path of negative events. In the context of a cyber incident, this is often called an 'attack path. For example, in the security incident involving loss of customer card data from Target stores, the supplier's use of a home anti-virus product failed to detect password logging malware attached to an email, which allowed capture of the login credentials for Target's supplier portal, and the poor configuration, use of default passwords and failure to apply security patches allowed the criminals to install malware on the company's point of sale systems, thus harvesting information on some 40 million consumer credit and debit cards. This combination of risks created the environment that made the attack possible.*

c) the cascading effects of risks.

***NOTE 1** Cascading effects occur where there is a non-linear path of events occurring, including amplification and subsidiary negative events or outcomes. The cascade effect is particularly likely to occur in complex systems, i.e. systems of systems, where there is not a simple linear relationship between systems or sub-systems. In these cases, rather than the effect of the risk spreading in a simple longitudinal fashion, instead the effect spreads like a ripple affecting multiple assets that may not be directly connected to each other.*

***NOTE 2** It is important that risks are not considered in isolation. In a complex manufacturing process or environment there may be considerable interaction between risks. For example, a manufacturing system may include a digital component that has a known vulnerability. A risk assessment concludes this to be of low risk as the system is behind the enterprise's firewall. However, the risk of the known vulnerability being exploited is likely also to be contingent on the protection of any remote diagnostic capability with the factory, the policies regarding the use of removable media, bring your own devices and the handling of email attachments.*

6.3.9 Where the organization's board-level management considers a risk is acceptable, the organization's risk capacity shall be reviewed and updated to reflect the risk being carried.

6.3.10 Where the organization's board-level management considers a risk is unacceptable, the organization shall:

a) identify and assess potential mitigation measures;

b) select and apply measures as appropriate;

c) record the risk treatment; and

d) return the residual risk to the identification and analysis stage.

6.3.11 Taking into account the organization's risk appetite and security strategy, the organization's board-level management shall consider for the portfolio of risks:

a) the nature of the threat environment(s);

b) an appropriate and proportionate frequency for the scheduling of risk reviews to re-evaluate the risk portfolio; and

NOTE *The board-level management may consider that annual or biennial reviews are sufficient, however the frequency should be determined by how dynamic the threat environment is.*

c) the triggers that would prompt an ad hoc review of some or all of the risk portfolio.

NOTE *Triggers may include: the emergence of a new threat actor; changes in the security context; identification of new/emerging vulnerabilities; and identification or publication of new exploits enabling easier access to vulnerabilities or increasing their impact.*

6.4 Implementing security risk management

6.4.1 The approach established in **6.3** shall be documented and maintained as a set of risk assessment and management policies, processes and procedures recorded in or referenced by the Security Management Plan (**5.7**).

6.4.2 The organization shall ensure and be able to evidence that personnel undertaking security risk management activities are suitably qualified and experienced personnel, who have an up-to-date knowledge and:

a) understanding of current and relevant threats and vulnerabilities to vehicles and vehicle-related systems; and

b) can specify workable engineering practices and/or other solutions required to mitigate them.

6.4.3 The organization shall consider the use of organizationally independent reviewers to assess and supplement the practices required in **6.4.2**.

6.4.4 In fulfilling the requirements of **6.1.5**, the organization shall:

a) identify and agree with their suppliers how security risks are to be managed;

b) manage access to sensitive information and systems on a need-to-know basis, so that security measures can be maintained at an appropriate and proportionate level; and

c) require personnel within its supply chain who handle sensitive information to:

i) be subject to security screening and minimum competence requirements;

ii) maintain records demonstrating that appropriate security awareness training has been undertaken; and

iii) personnel in high-risk roles shall be subject to enhanced screening or vetting.

6.5 Monitoring changes to threat landscape and emerging vulnerabilities

6.5.1 The organization's board-level management shall maintain situational awareness by monitoring:

a) risks and opportunities;

b) emerging threats and vulnerabilities; and

c) the organization's scope and security context.

6.5.2 The organization shall proactively monitor the threat landscape for new potential threats and vulnerabilities through collaboration and engagement with third parties.

NOTE *The UK NCSC has set up a Cyber Information Sharing Platform (CiSP) to facilitate sharing of information between industrial organizations, both within and between sectors. The UK Government is also setting up an Information Exchange for the automotive industry (Auto-IE) as a forum where organizations involved in road and vehicle systems can share best practice, lessons learned and threat/incident knowledge for the benefit of the industry as a whole. Organizations should consider these or similar platforms.*

7 Security management over vehicle systems lifecycles

Principle 3 – Organizations need product aftercare and incident response to ensure systems are secure over their lifetime.

NOTE *Given the changing and emergent nature or security threats and vulnerabilities organizations should provide clear and publicly accessible statements about their commitment to provide security management and incident response for their vehicle systems-related assets and vehicle-related products and or services over the lifecycle of a vehicle that may reasonably be expected by the customer/owner/operator/driver of a vehicle. Thus the provisions of this Clause should extend significantly beyond any initial warranty period for the vehicle, vehicle systems and any related services.*

7.1 Develop and maintain a Security Incident Management Plan (SIMP)

7.1.1 The organization's board-level management shall require that the SIMP is used to establish, deliver and maintain the security aftercare and incident response processes and procedures that will be employed to provide effective and coordinated to security incidents and near misses over the lifecycle of the products, systems and services that they deliver.

7.1.2 The SIMP shall also be used to respond to security incidents that affect or may affect the organization's vehicle systems-related assets.

7.1.3 The organization's board-level management shall require that the SIMP includes:

a) the incident response polices, processes and procedures detailing to be employed before, during and after an incident, including the audit arrangements and identification of the individual(s) responsible and accountable for their implementation;

b) a prepared and rehearsed communications plan to be used during the recovery from a security incident or suspected incident, that defines how information will be securely communicated in a timely manner to relevant parties;

NOTE *Consideration should be given as to who needs what information and when it is required. The parties involved may be both internal to the organization and outside it.*

c) a summary of the risk assessment of potential risks in the event of a security incident (**6.1**);

NOTE *The risks should be recorded in the Asset-based Risk Register, and only a brief summary provided in this Plan.*

d) a record of the risk mitigation measures including:

i) the measures to enable, when required, the capture of data and information about an incident for use in investigations, and/or detailed analysis of the root causes of the incidents;

NOTE 1 *This will require consideration of where the data and information may be stored and/or accessed, for example, whether it is within the organization or its supply chain, on or off the affected vehicle(s), and if off the vehicle(s) whether it is held by a service provider or within any networking infrastructure.*

NOTE 2 *There may be legal obligations arising from deployment of autonomous or communications functionality, where the organization is required to assist third parties, for example public authorities or insurers, to determine the root cause of an incident. This may require the organization to record and retain a minimum set of data or information regarding the vehicles and their systems.*

ii) the process to be followed on discovery of a security incident, including near misses;

iii) business continuity measures required in the event of failure, impairment or non-availability of the vehicle systems-related assets and any vehicle-related products, systems or services that affect vehicles outside of the organization's premises;

iv) the disaster/incident recovery actions required in the event of serious failure scenarios;

v) steps to be taken to contain and recover from the event;

e) the arrangements where applicable (**7.4**) to access data and logs on affected or potentially affected systems, including:

i) what may be accessed and why;

ii) how the data and/or logs will be used;

iii) under what circumstances they may be accessed;

iv) who is authorized to access the data and/or logs;

v) how the data and/or logs will be protected; and

vi) the arrangements for the secure deletion of the data and/or logs when no longer required;

f) the review process to be followed following a security incident, including:

i) the process for assessing any ongoing risk;

ii) the process for evaluating the scale of the incident and the effectiveness of the response to it;

iii) a review of any hosting or cloud service provider's incident management plan where applicable;

iv) the need for changes to the contractual provisions to handle security incidents caused by a professional advisor, contractor or supplier; and

v) the mechanisms for reviewing and updating the Security Incident Management Plan (SIMP).

7.1.4 The SIMP shall be regularly reviewed and updated by the organization, taking into account changes:

a) in the security context of:

i) the organization;

ii) the organization's supply chain; and

iii) the vehicles or vehicles systems that use the organization's products and/or services;

b) in the operation of the organization, which shall include:

i) operational changes, for example use of contractors or temporary staff, outsourcing and/or change of suppliers, sub-contractors, etc.;

ii) changes to existing business and technical systems; and

iii) adoption of new technologies;

c) to the vehicles, which shall include:

i) products embodied in vehicle systems;

ii) systems integrated with vehicle systems or the wider ecosystem;

iii) services used by vehicle systems;

iv) adoption of new technologies.

7.2 Testing the SIMP

7.2.1 The organization's board-level management shall require the periodic testing of the response plans that form part of their SIMP to:

a) verify that it can respond to and manage security incidents in accordance with its obligations and plans; and

b) identify and address weakness in the plans arising from organizational, personnel or technology changes.

c) **7.2.2** The organization's board-level management shall require that plans developed to test the SIMP:

a) identify possible scenarios requiring a response;

b) include the review and if necessary or appropriate update the risk management plans for them;

c) verify that the personnel, assets, policies, processes and procedures are in place to fix possible problems;

d) require the personnel involved to be appropriately briefed and/or trained to fulfil their incident response roles;

e) consider media strategies;

f) determine how affected customers (i.e. vehicle owners, operators and users) may be contacted if there are specific actions they are required to take; and

g) research and document any mandatory reporting requirements, which may vary between the territory or jurisdiction within which the affected vehicles, or vehicle systems are located.

7.3 Security update program

7.3.1 The organization's board-level management shall establish an active program to maintain security of its vehicle systems-related assets over the lifecycle of the associated products, systems or services.

NOTE *Where a vehicle system employs cloud-based functionality to deliver services, the security update program should address both the hosting and the application aspects of the cloud service.*

7.3.2 The organization's board-level management shall establish an active program to maintain security over the lifetime of the products, systems or services that it delivers

7.3.3 The programs in **7.3.1** and **7.3.2** shall:

a) encompass all relevant hardware, software, firmware, data and/or information for the in-scope items;

b) monitor the assets, products, systems and services throughout their respective lifecycles to identify, analyse consequences and criticality, and prioritize security vulnerabilities;

c) for those vulnerabilities posing intolerable safety or security risks, develop appropriate and proportionate controls or countermeasures in a timely manner; and

d) deliver the updates to implement the controls or countermeasures in a timely and effective manner as an after-sales support service.

NOTE *Where the provisions of **7.3.4** apply, the responsibility for ongoing risk management will lie with the aftermarket organizations that have taken or are taking over responsibility for ongoing development and support.*

7.3.4 Where it is no longer possible to support an asset, product, vehicle system, embedded software or service, the organization shall:

a) identify and assess the contingent safety and security risks;

b) provide sufficient notice to permit all affected parties to respond to any withdrawal or reduction of ongoing development and support;

c) if there is a significant increase in the safety or security risks, then:

   i) for vehicles that require registration or licencing notify the licencing authority and provide a public information notice for distribution to the vehicle's owner or registered keeper;

   ii) for other vehicle types notify service and maintenance organizations;

   iii) provide a searchable register for insurers and official bodies to identify obsolete products or systems and unsupportable software;

   iv) work with aftermarket organizations to enable the development of technical solutions to mitigate the risk by making available:

   - technical information about the affected product or vehicle system to suitably qualified and experienced personnel; and
   - any embedded software or source code.

NOTE *Given the relatively long lifetime of most vehicles compared to digital technology cycles it is likely that obsolescence of products and systems will become an increasingly serious issue.*

7.3.5 Where as a consequence of a supplier or service provider ceasing to trade, or as a result of a decision to discontinue support for a product, system or some embedded software, or due to technological obsolescence an organization is unable to continue to support a product or vehicle system, it shall assist vehicle owners, operators and/or users to manage any resultant risks.

7.4 Forensic readiness

7.4.1 The organization shall ensure that its systems and services are able to support data forensics and recovery of forensically robust, uniquely identifiable data.

7.4.2 If an organization is unable to fulfil the requirement in **7.4**, or it decides that this is inappropriate given the nature of its vehicle systems, the absence of the forensic capability shall be regarded as a risk and an appropriate entry provided in the organization's Asset-based Risk Register.

7.4.3 Where the organization has enabled activity logs in its vehicle systems or vehicle system-related assets, these logs shall be:

a) designed with access rights that are based on predetermined usage profiles so that is clear to all potentially affected parties who may read, or have other access rights, to the data and under what circumstances;

b) secured so as to reduce the risk of deletion or alteration during a cyber-attack;

c) of a sufficient standard that if they are produced in court the integrity and authenticity of the data can be relied upon;

d) stored for a reasonable and proportionate time, commensurate with the sensitivity and/or criticality of the system(s) to which they relate; and

e) compliant with relevant data protection laws.

7.5 Connecting to a customer or end-user's vehicle

Where the organization, including any suppliers, sub-contractors or agents, requires the connection or attachment of a cyber physical device to a vehicle the organization's board-level management shall require that:

a) the connected or attached device meets recognized minimum security requirements;

b) the risk of the device acting as a vector for a cyber-attack on the vehicle or fleet of vehicles has been assessed and where intolerable it has been mitigated; and

c) the vehicle and equipment provide appropriate logging and audit functionality for connected devices, with non-repudiation built in to the logging process.

NOTE *When vehicles are connected to a diagnostic system, or digital devices are used during maintenance, regulatory testing, etc., or telematics devices are connected for insurance or fleet management purposes, there is a risk that attacks may be propagated through malware installed on the device(s). Appropriate measures should be applied to maintain the cyber hygiene of these devices.*

8 Working together to enhance system security

Principle 4 – All organizations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system.

8.1 Working with suppliers

8.1.1 The organization's board-level management shall require that the organization works together with its supply chain, and where relevant 3rd parties, to enhance the security of its vehicle systems-related assets.

8.1.2 The organization's board-level management shall require that the organization works together with its supply chain, and where relevant third parties, to enhance the security of the vehicles, products, systems and services that it delivers, through:

a) exchange of security-related information, knowledge and experience (**6.5**); and

b) sharing information about vehicle, product, sub-system, system and service design constraints and risks.

NOTE *The collaboration to enhance vehicle system security requires a security-minded approach to the disclosure of information, balancing the need-to-know approach with a risk-based approach to addressing actual or potential vulnerabilities and delivering solutions that are secure by default.*

8.2 Develop and maintain the Supply Chain Security Management Plan (SCSMP)

8.2.1 The organization's board-level management shall require that the SCSMP is used to address the security management of:

a) suppliers (i.e. professional advisers, contractors, service providers and OEMs) across their individual lifecycles (**8.2.2**); and

b) organizations that integrate, operate, or maintain, the products, systems and services that it delivers (**8.2.3**).

8.2.2 The SCSMP shall include the policies, processes and procedures relating to:

a) the pre-contract due diligence requirements regarding the supplier's security culture and its security management strategy;

b) the auditable security requirements that are to be addressed in suppliers' contracts, for example the provision of risk management information regarding the supplier's products, systems or services;

c) guidance on the use of DISAs relating to the exchange or supply of data or information:

   i) relating to vehicle systems-related assets;

   ii) individual vehicle-related products, systems or services; and

   iii) use of vehicles;

d) auditable requirements for any further or additional security awareness training; and

e) identification of high-risk roles.

8.2.3 The SCSMP shall also detail the policies, processes and procedures to be applied when sharing sensitive information with potential or actual customers, for example when responding to an invitation to tender.

8.3 Supply chain assurance

8.3.1 The organization's board-level management shall require that the organization is able to provide assurance regarding the holistic nature of its own security measures, i.e. that the measures encompass personnel, physical, process and technical aspects of:

a) its business operations;

b) its vehicle systems-related assets; and

c) the vehicles, products, systems and services that it delivers.

NOTE *This includes products, systems or services that are embodied in or employed by vehicle systems delivered by other organizations.*

8.3.2 The organization's board-level management shall require evidence or assurance of the security measures from its suppliers, that they address the identified security risks and vulnerabilities so as to mitigate them to achieve a level of residual risk that is acceptable to the parties involved.

8.3.3 The nature of the evidence or assurance required in **8.3.1** and **8.3.2** shall be determined by a risk assessment of the consequences and impact of the vehicle, products, sub-systems, systems or services being vulnerable or compromised. This can be evidenced by:

a) for low risk items, i.e. those containing little or no digital technology and not fulfilling a safety or security critical role:
   i) by self-certification; or
   ii) provision of the organizations Security Strategy and SMP;

   NOTE *The provision of these documents should be subject to appropriate safeguards being in place, for example a confidentiality undertaking or DISA.*

b) for other items independent validation or certification can be required.

8.3.4 The organization's board-level management shall require that the organization maintain records allowing the traceability, including authenticity and origin, of all supplies delivered by its supply chain that relate to the design, deliver, operation or maintenance of products or services it supplies that are embodied in or used by a vehicle system.

8.3.5 Where the operation of a vehicle system-related asset, product, sub-system, system or service relates to, or could compromise, the safety and/or security of a vehicle, its operator, driver, occupant(s) or user(s), the organization's board-level management shall require that its supply chain maintain records allowing the traceability, including authenticity and origin, of all supplies relating to the item's design, delivery, operation, maintenance and disposal.

8.4 Security over a vehicle, system or service lifecycle

8.4.1 The organization's board-level management shall require that it works together with other parties involved in the design, delivery and support of a vehicle system to ensure that security risks and vulnerabilities have been identified and measures taken to mitigate them to achieve a level of residual risk that is acceptable to the parties involved.

8.4.2 Over a vehicle system lifecycle, where there is a need to exchange data or information with suppliers and/or third parties, the organization's board-level management shall assess the security risks associated with these exchanges and put in place appropriate and proportionate security measures to mitigate the risks.

8.4.3 The organization's board-level management shall require that where responsibility for a vehicle system is transferred to a third part, the associated security risks are considered and appropriate mitigation measures adopted to that the security of the vehicle system is maintained throughout its lifecycle.

8.5 Connected vehicles

8.5.1 Where a vehicle system, or sub-system, is or may be required to communicate with external devices or systems, the organization's board-level management shall:

a) assess the risk the connection poses to the vehicle, including potential attack vectors and identify appropriate and proportionate mitigation measures;

b) jointly plan with other parties involved with the interconnection how the safety and security of the vehicle will be maintained;

c) design the interfaces so as to minimize vulnerabilities and provides appropriate and proportionate communications security;

d) once the connectivity and interface design has been finalized:
   i) review/reassess the associated risk(s); and
   ii) confirm acceptability of any residual risk and update the Asset-based Risk Register; or
   iii) design/implement further mitigation measures and continue this process [i.e. steps **8.5.1** (d)(i) to (iii)] until an acceptable level of residual risk is achieved.

8.5.2 The organization's board-level management shall identify, document and manage external dependencies for the vehicles, products, systems and services that it delivers.

8.5.3 Where external data and/or information is relied upon by automated and/or safety critical functionality the organization's board-level management shall provide a secure method to update it so that it does not become obsolete.

9 Applying a defence-in-depth approach

Principle 5 – Systems are designed using a defence-in-depth approach.

9.1 Adopting a defence-in-depth approach

9.1.1 The organization's board-level management shall ensure that the design and implementation of the vehicles, products, sub-systems, systems and services that the organization delivers, use a defence-in-depth approach. This approach shall be implemented by ensuring that the design:

a) does not rely upon a single security mechanism; and

b) employs multiple layers of complementary defences.

9.1.2 The organization's board-level management shall ensure preparation and maintenance of documentation and evidence that the design and implementation of the vehicle system (including any vehicle systems-related asset):

a) does not incorporate single points of failure;

b) does not employ a control strategy that can be exploited as a point of failure;

c) does not rely upon security by obscurity to protect assets;

NOTE *The concept of security by obscurity assumes that a particular vulnerability is not a risk as it is not immediately apparent to a potential adversary.*

d) enables components to be easily upgraded or replaced in the event that the vehicle system design is compromised; and

e) where known vulnerabilities exist and cannot be immediately eliminated, a time bounded plan shall be developed to ensure that the risk exposure is proportionate and finite.

9.1.3 The organization's board-level management shall ensure preparation and maintenance of documentation and evidence that the design and implementation of its product, sub-system and/or vehicle system has taken into account physical security, including:

a) the location and ease of access to system components including control units, sensors, actuators, cabling, and power connections; and

b) the use of tamper protection and/or tamper evident techniques to protect critical equipment.

9.2 Security architecture

9.2.1 When designing a vehicle system, the organization's board-level management shall ensure preparation and maintenance of documentation and evidence that it has adopted a security architecture, which applies a layered defence at vehicle, vehicle system and sub-system and product levels.

9.2.2 The documented security architecture shall be made available on request, subject to agreement and signature of an appropriate DISA, to suitably qualified and experienced personnel working for:

a) organizations purchasing or integrating their own products an/or systems with the supplier's system;

b) a vehicle manufacturer utilizing the system in their design of a vehicle or vehicle system;

c) a government, public or other regulatory agency with responsibility for the safety and/or security of vehicle users, drivers or operators; and

d) security research teams, whether based in an academic or industry research organization.

9.2.3 Where a vehicle or vehicle system relies upon interaction with a system located outside the vehicle for its safe and secure operation, the security architecture shall address the impact of any loss or degradation of the connection that supports the interaction.

9.2.4 The organization's board-level management shall ensure that vehicle systems are designed to ensure that connection to the vehicle's network is actively managed, so that:

a) authorized devices are given access;

b) unauthorized and/or unmanaged devices are identified and prevented from accessing the network.

9.3 Maintaining trust within vehicle systems

Where transactions cross trust boundaries, within or between vehicle systems, the organization's board-level management shall require that the systems:

a) implement appropriate and proportionate security controls regarding the flow of data and/or information, including commands;

b) are compliant with data protection provisions;

c) limit access by operators, users, applications and devices on the basis of the least privilege principle, whilst applying fail-safe defaults, i.e. base access decisions on permissions rather than default exclusion; and

d) minimize the risk that interfaces to systems external to the vehicles are designed so as:

   i) at a minimum to implement trust boundaries between external facing vehicle systems and critical internal vehicle systems;

   ii) reduce the risk that they may be successfully exploited.

e) minimize the risk that interfaces to systems and/or end user devices within the vehicle's passenger or load area are designed so as:

   i) at a minimum to implement trust boundaries between external facing vehicle systems and critical internal vehicle systems;

   ii) reduce the risk that they may be successfully exploited.

NOTE *A trust boundary is a point where data or information passes between different sub-systems, systems or services, i.e. it is output from one process into another and therefore should be subject to some degree of checking, verification or validation. The checking may for example be:*

a) to confirm that the data is of the correct type, e.g. that a non-numeric value is not present in a numeric field;

b) to check that a numeric value is within an acceptable range.

9.4 Technical competence

The organization's board-level management shall retain sufficient technical competence to:

a) recognize and respond to threats that arise when connections to the vehicles' networks and/or the vehicle networks are or may be compromised through attacks;

b) analyse and explain safety and security implications that arise in attacks on vehicle or vehicle-related systems.

9.5 Security of connections to the vehicle

9.5.1 For remote systems that have connectivity to vehicle system, the organization's board-level management shall research, document and demonstrate an understanding of the design, function, mode of connection and operation of the connection to vehicle and vehicle system(s).

NOTE *The scope of this requirement is intentional wide, so that the system designer takes account of the full range of devices or services that could be connected to the vehicle system and that the resulting interfaces are secure by design.*

9.5.2 For each connection identified in **9.5.1** the organization's board-level management shall:

a) identify the connection and remote systems stakeholders;

b) identify the nature of any data, information, commands or transactions passed from vehicle to remote system and vice versa;

c) assess and record whether any of the data and/or information identified in (a) is sensitive information;

d) assess and record whether any of the commands or transactions identified in (b) are sensitive commands;

e) identify which vehicle systems are intended to interact with the remote system

f) understand the sensitivity of the data or information;

g) assess the impact of inaccurate or malicious data.

9.5.3 In respect of the service administrative functions, such as management and configuration, for each connection identified in **9.5.1** from vehicle to the remote system(s) and within the remote system(s) the organization's board-level management shall:

a) identify and authenticate the parties responsible for system administration;

b) record for each party involved the nature of their access to the system and what data, information, vehicle systems they have or could have access to;

c) assess the security measures in place regarding administrative and maintenance access to the systems identified in **9.5.2**.

9.5.4 Based on the understanding developed in **9.5.2** and **9.5.3**, the organization's board-level management shall:

a) assess and record the threats, vulnerabilities and residual risk, taking into account any mitigation measures already in place in the vehicle or vehicle system(s);

b) determine and document whether the level of residual risk is acceptable to the organizations and relevant connection and remote systems stakeholders; and

c) where the level of residual risk is not acceptable, provide appropriate and proportionate additional measures to:

   i) secure the data transmitted between vehicle system(s) and remote system(s);

   ii) prevent unauthorized commands or transactions being initiated by the remote system(s);

   iii) verify the provenance of the data and/or information, i.e. its authenticity, integrity and plausibility;

   iv) prevent unauthorized access to vehicle system(s) from or through the remote system(s); and

   v) provide the vehicle operator and/or user with privacy controls to enable choices to be made.

9.5.5 Where remote systems provide critical functionality for a vehicle or vehicle system, the organization's board-level management shall:

a) research, document and demonstrate an understanding of the following aspects of the remote system:

   i) physical security, including the location and protection of the system;

   ii) resilience, including the arrangements for back-ups and restoration of services;

   iii) the business continuity and disaster recovery arrangements;

b) assess the potential impact on the vehicle systems of loss of access to, use of, or performance of the remote system; Software trustworthiness;

c) taking into account the outcome of **9.5.2** and **9.5.3**, design the vehicle system so that the security and safety risks are as low as reasonably practicable;

d) where a vehicle system cannot be readily upgraded to mitigate vulnerabilities, the organization shall provide additional protection in the design so that the security and safety risks are as low as reasonably practicable.

NOTE *Guidance from the UK Health & Safety Executive (HSE) suggests that when determining that risks have been reduced to "as low as reasonably practicable level" (ALARP) involves assessing the* ***risk*** *to be avoided, the* ***sacrifice*** *(in terms of cost, time and effort) involved in implementing measures to avoid that risk, and a* ***comparison*** *of the two. This process can be implemented with varying degrees of rigour that depend on the nature of the hazard, the extent of the risk and the control measures to be adopted. The same approach can be adopted for security risks, with the level of rigour dependent on the nature of the threat and the potential impact.*

10 Software trustworthiness

Principle 6 – The security of all software is managed throughout its lifecycle.

10.1 Software development practices

10.1.1 The organization's board-level management shall require the development and maintenance of documented policies, processes and procedures that are employed to manage the software lifecycle for all software, including embedded software and firmware, use by its vehicle-systems related assets and in the products, systems and services that it delivers.

NOTE *Consideration should be given to the recommendations set out in SAE JS061 [11].*

10.1.2 When developing the software management framework required in **10.1.1**, the organization's board-level management shall require implementation of the software trustworthiness principles specified in BS10754.

NOTE *Assurance of the organization's software lifecycle processes should be available to parties higher in the supply chain.*

10.1.3 The organization's board-level management shall require the adoption of secure software design and coding practices (e.g. MISRA C) to mitigate the risks arising from known and unknown vulnerabilities:

a) in new software written or licenced by the organization and its supply chain;
b) inherited from existing code libraries and/or reuse of existing code; and
c) those that arise from interactions between the organization's software and applications provided by other organizations, whether deployed on the vehicle or accessed via networks or interfaces connected to the vehicle.

10.1.4 The organization's board-level management shall require, where practical, that the organization adopts open design practices, including:

a) ensuring that peer reviewed code is deployed wherever possible; and
b) making source code available for inspection and review where appropriate.

10.1.5 Where software developed by a third party, whether open source or proprietary, is to be employed in the design or operation of a vehicle system, the organization's board-level management shall apply due diligence to and maintain assurance of, for example by:

a) reviewing the volume and severity of known vulnerabilities in the software and other similar software created by the developer(s);
b) subjecting the software to formal code inspection reviews;
c) using automated tools to analyse the structure and security of the code; and
d) establishing the mechanisms used, or to be used, to manage vulnerability disclosure, investigation and resolution of vulnerabilities, and the provision and deployment of patches.

10.2 Configuration management and version control

10.2.1 The organization's board-level management shall establish and operate a process to enable timely identification of the status of all its vehicle systems software, including firmware and/or configuration information, that as a minimum provides:

a) version, revision and status;
b) the originator/writer/publisher of the code;
c) the software, including:
   i) the original source code;
   ii) any configuration information;
   iii) change control records;
   iv) checksum, or hash values that can be used to verify the integrity of the code;
d) dependencies, for example on specific operating systems, compilers, libraries, etc.;
e) evidence of testing, including test scenarios and results;
f) records of any unresolved test defects, deficiencies or anomalies; and
g) the vehicle systems in which the software has been deployed.

10.2.2 The organization's board-level management shall design and implement its vehicle systems so that:

a) suitably qualified and experienced personnel, including third parties can readily ascertain:
   i) the version and revision numbers of all software used within the vehicle system;
   ii) whether the software in safety and/or security critical vehicle systems is the same as that latest version approved for use in the vehicle or vehicle system;

   ***NOTE** For insurance purposes, it is likely that the driver, operator or user of the vehicle will need to be able to determine whether the vehicle's safety critical software is up-to-date.*

b) the vehicle driver/operator can easily determine if the software deployed in the vehicle is up to date.

10.2.3 For transfer of software and software updates from/to its suppliers and customers within the automotive and vehicle systems supply chains, the organization's board-level management shall establish and use secure mechanisms for:

a) software transfer;
b) verifying the authenticity and integrity of the software, both in transit and at rest; and
c) checking the latest version, revision and status of the software.

10.2.4 Where the use of machine learning or artificial intelligence is being considered for application in vehicle systems, the organization's board level management shall consider what measures are available to assure and describe the application of these technologies in the automotive ecosystem.

10.3 Software updates

10.3.1 Software employed in safety and/or security critical applications or operations shall be digitally signed and the organization's board-level management shall employ assured key management practices.

10.3.2 The organization's board-level management shall require that the vehicle system is designed so that it is possible to safely and securely:

a) update software; and
b) restore the software and system data/information to a known good state if it becomes corrupted, or in the event that the update or installation fail.

***NOTE** Where software is capable of being remotely upgraded or patched, the design of the update mechanism needs to take in to the account the requirement to roll-back the update or upgrade to a known good state. If the upgrade or update can be installed automatically without specialist support, for example whilst the vehicle is parked on the street or at the home of the user/owner, the reversion should also be handled automatically without the need for specialist assistance or advice.*

10.3.3 When designing the processes required by **10.3.2**, the organization's approach shall provide a well-defined, tested and documented process for delivering patch updates or new software version, that:

a) requires the update and restore processes to be executed in a safe manner;

***NOTE 1** Depending on the nature of the system and software being updated it may not be safe to apply an update when the vehicle is for example in motion. In which case the update should be designed and deployed in such a way that it can only be installed/ applied when the vehicle is stationary.*

***NOTE 2** In exceptional circumstances there may be a requirement for an update to only be applied under the control and/or direction of a suitably qualified and experienced person, in which case the vehicle driver or operator should be directed to seek support from an approved service or support agent.*

b) secures the delivery mechanisms for any updates or restoration images to prevent unauthorized modification;
c) validates the authenticity and completeness of the update or restoration package;
d) takes account of intra-vehicle and inter-vehicle systems dependencies to prevent development of unsafe or insecure situations developing; and
e) seeks to minimize the duration of any patch window, particularly for all safety and security related updates.

11 Management of vehicle system data & information

Principle 7 – The storage and transmission of data is secure and can be controlled.

11.1 Data and information security

11.1.1 The organization's board-level management shall develop, record, implement and manage appropriate and proportionate policies, processes and procedures relating to security-minded data and information management which are based on an understanding of the security implications associated with the loss, compromise, unauthorized manipulation or change of data and/or information, as set out in the Introduction (Clause **0**).

11.1.2 The organization's board-level management shall ensure that the storage, transmission and processing of data and information is secured and can be controlled.

11.1.3 To evidence compliance with the requirements in **11.1.1** and **11.1.2**, when designing or modifying a vehicle system, and any related service(s), the organization's board-level management shall require that the following aspects are assessed and documented:

a) what data and/or information needs processing by the vehicle system;
b) whether the data and/or information:
   i) needs to be stored by the vehicle system;
   ii) how long it needs to be stored;
   iii) whether an authorized person should be able to delete it;
   iv) whether it will be shared with other vehicle systems, and if so identify which system(s) and the rationale for sharing it;
c) the value and sensitivity of the data and/or information; and
d) the potential for personal data to be extracted from data sets or sets or messages.

11.1.4 To evidence compliance with the requirements in **11.1.1** and **11.1.2**, when designing or modifying a vehicle system-related asset, and any related service(s), the organization's board-level management shall require that the following aspects are assessed and documented:

a) what data and/or information needs processing by the vehicle system-related asset; and
b) whether the data and/or information:
   i) needs to be stored by the vehicle system-related asset;
   ii) how long it needs to be stored;
   iii) whether an authorized person should be able to delete it;
   iv) whether it will be shared with other vehicle system-related asset, and if so identify which system(s) and the rationale for sharing it.

11.1.5 The documentation produced in **11.1.3** and **11.1.4** shall be maintained under configuration control and updated as necessary to reflect developments in the design and integration of the vehicle system over the lifecycle of the vehicles in which it is used and the systems to which it is connected.

11.1.6 Taking into account the analysis specified in **11.1.3** and **11.1.4**, the organization's board-level management shall require that vehicle systems are designed so that data and information is protected and appropriately secured:

a) in transit, i.e. when being transferred between different vehicle systems and/or vehicle system-related assets;
b) in use, i.e. during processing or display; and
c) at rest, i.e. when stored in a vehicle system, whether on or off the vehicle.

11.1.7 When designing and implementing the measures to protect and secure the data and/or information identified in **11.1.3**, the organization's board-level management shall require that the security goals identified in **Figure 1** are addressed:

a) confidentiality, i.e. the control of access, and prevention of unauthorized access to vehicle systems, and to data or information which may be sensitive data, sensitive information or personal data, in isolation or in aggregate;

b) possession, i.e. vehicle systems and associated processes or services are designed, implemented, operated and maintained so as to prevent unauthorized control, manipulation or interference, and to ensure that data and/or information are only used in accordance with the obligations, licence or contractual rights;

c) availability (including reliability), i.e. ensuring the data, information, vehicle systems and associated processes are consistently discoverable, accessible, usable and, where appropriate, can be disclosed in an appropriate and timely fashion;

d) safety, i.e. vehicle systems and related processes are designed, implemented, operated and maintained so as to prevent the creation of harmful states, which might lead to injury or loss of life, or unintentional environmental damage, or damage to assets;

e) resilience, i.e. the ability of data, information, vehicle systems and any associated processes or services to transform, renew and recover in a timely way in response to adverse events;

f) integrity, i.e. maintaining the completeness, accuracy, consistency, coherence and configuration of data, information and vehicle systems;

g) utility, i.e. ensuring that data, information and vehicle systems remain usable and useful across the lifecycle of the data and information, and any associated asset, individual, organization or vehicle system; and

h) authenticity, i.e. ensuring that data and/or information input to, and output from vehicle systems, the state of the systems and any associated processes, data and/or information are genuine.

NOTE *The security goals are applicable to systems both on the vehicle and remote from the vehicle, for example in road-side cabinets or remote data processing centres.*

11.1.8 When designing and implementing the measures to protect and secure the data and/or information identified in **11.1.4**, the organization's board-level management shall require that the security goals identified in **Figure 1** are applied to its vehicle systems-related assets and any related service(s).

11.1.9 The organization's board-level management shall require that the design and implementation of the products, systems and services it delivers support the forensic recovery of data and information following any safety or security related incident.

11.2 Processing of personal data

11.2.1 Where a vehicle system will process or store personal data, the organization's board-level management shall require that documentation and evidence is produced and maintained to demonstrate that the design complies with the following requirements:

a) the processing of personal data shall minimized;

b) processes shall be in place to allow data subjects:

   i) to establish what personal data is held by the organization;

   ii) to ascertain for what purpose it is being held; and

   iii) to exercise the data subjects' right to be forgotten;

c) personal data shall be stored for the shortest practicable period;

d) a data retirement plan shall be in place, so as to ensure, and demonstrate, the secure destruction of all personal data when it is no longer required;

e) wherever practicable the design shall reduce privacy risks though use of techniques such as anonymization, sanitization and tokenization;

f) any personal data stored within the vehicle shall be afforded enhanced technical and physical protection to prevent unauthorized access:

   i) by personnel servicing or maintaining vehicle systems;

   ii) by third parties in the event of the theft of the vehicle, removal of vehicle system components or connection to vehicle systems.

g) any personal data stored outside the vehicle shall be afforded protection commensurate with its sensitivity and good industry practice relevant to the prevailing data protection legislation of the jurisdiction in which the vehicle is registered and normally used.

11.2.2 Where a vehicle system stores personal data the organization's board-level management shall require the system to be designed so that an operator or user may permanently delete their personal data from the vehicle system(s).

11.3 Data and information sharing

11.3.1 Where the design and/or operation of a vehicle system is intended to facilitate data sharing or information sharing the organization shall put in place a Data and Information Sharing Agreement (**5.10**) prior to sharing the data and/or information.

11.3.2 Where a vehicle system in a vehicle connects to an external vehicle system such as an Intelligent Transport System or a road charging system, the organization's board-level management shall require that the connections and exchange of data and/or information are designed so that the identity and trustworthiness of the end-user/systems can be established using appropriate secure authentication schemes and the communications channel secured throughout the exchanges of messages.

12 Vehicle system resilience

Principle 8 – The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail.

12.1 Understanding the need for system resilience

12.1.1 The organization's board-level management shall require that the design of a vehicle system, sub-system or product be resilient to attacks and will respond in an appropriate and proportionate manner if its defences or sensors fail, taking into account the immediate threat to the safety and/or security of the vehicle's operator, users, occupants and/or cargo.

12.1.2 The organization's board-level management shall require that those responsible for designing vehicle systems shall identify and document those systems, sub-systems, components and sensors that are safety and/or security critical.

12.1.3 For each of these items identified in **12.1.2** the organization shall:

a) assess and document the potential failure modes of the item, including any common mode failures;

b) assess and document the impact that each of the item's failure modes would have on the vehicle, its occupants or cargo, and on the environment outside the vehicle;

c) assess and document what compensatory measures may be appropriate to reduce the threat and harm to as low as reasonably practicable level; and

d) implement those measures that are appropriate and proportionate to reducing the risks to a level that is commensurate with the organization's security strategy and risk appetite.

12.2 System resilience in vehicle and vehicle system design

12.2.1 When designing or modifying vehicle systems the organization's board-level management shall require that those responsible:

a) be aware of and regularly review the range of potential attacks on vehicle systems;

b) design and implement safety critical systems, sub-systems and components, and any modifications to them, so as to be resilient to:

   i) attacks, whether initiated within or outside the vehicle;

   ii) failure of individual sub-systems, components and/or sensors;

c) design and implement systems, and modifications to systems, so as to be resilient to:

   i) attacks, whether initiated within or outside the vehicle;

   ii) failure of sub-systems and/or sensors;

d) design systems to respond to threats in a manner that is:

   i) appropriate and proportionate to the magnitude of the risk to the safety and security of vehicle occupants, other road users and pedestrians;

   ii) can be executed in a timely and safe fashion;

e) design and implement systems, and modifications to systems, so far as is practicable, to enable the system to remain available for its primary use and to continue to operate in a safe and secure manner:

   i) on receipt of corrupt, invalid or malicious data, information or commands via its interfaces;

   ii) when encountering denial of service attacks, for example through jamming, interference or overloading.

12.2.2 The organization's board-level management shall require that vehicle systems are designed and implemented so that:

a) when appropriate, alert the vehicle operator and/or user to system failures, interference and attacks;

b) they enable the vehicle to be brought to a stop in a safe manner at a safe location;

c) if the affected function or system is safety or security critical prevent the vehicle being driven unless safe operation is assured; and

d) where the affected function or system is neither safety nor security critical, allow control and operation to be returned to the driver/operator in a safe manner with the function or system disabled until it is restored to a trustworthy state.

12.2.3 The organization's board-level management shall require that vehicle systems are designed and implemented so that they are resilient and fail-safe if safety critical functions are compromised or cease to work, with the mechanism and immediacy of response proportionate to the risk.

12.2.4 The organization's board-level management shall require that vehicle systems are designed and implemented such that the installation of vehicle user and/or operator applications, and/or after-market products or software does not compromise the integrity, safety and/or security of the vehicle systems.

13 Bibliography

13.1 Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 10010:2017, *Information classification, marking and handling – Specification*

BS ISO 26262, *Road Vehicles – Functional Safety*

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

BS ISO/IEC 15408-1:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Introduction and general model*

BS ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

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

BS EN ISO 15118-1:2015, *Road vehicles – Vehicle to grid communication interface – General information and use-case definition*

PAS 183:2017, *Smart cities – Guide to establishing a decision-making framework for sharing data and information services*

PAS 185:2017, *Smart Cities – Specification for establishing and implementing a security-minded approach*

PAS 555:2013, *Cyber security risk – Governance and management – Specification*

PAS 754:2014, *Software Trustworthiness – Governance and management – Specification*

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

PAS 11281:2018, *Connected automotive ecosystems – Impact of security on safety – Code of practice*

13.2 Other publications and websites

[1] GREAT BRITAIN. *Data Protection Act 1998*. London: The Stationery Office.

[2] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN [viewed December 2018].

[3] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures for a high common level of security of network and information systems across the Union. (NIS Directive) Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN [viewed December 2018].

[4] INFORMATION COMMISSIONER'S OFFICE. Data sharing code of practice. ICO: Cheshire, 2011. Available from: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf [viewed December 2018].

[5] CHARTERED INSTITUTE OF INTERNAL AUDITORS. Risk appetite and internal audit. London. Available from: https://www.iia.org.uk/riskappetite?downloadPdf=true [viewed December 2018].

[6] ENGINEERING COUNCIL. Guidance on Security. Available from: http://www.engc.org.uk/security [viewed December 2018].

[7] GREAT BRITAIN. *Environmental Information Regulations 2004*. London: The Stationery Office.

[8] GREAT BRITAIN. *Freedom of Information Act 2000*. London: The Stationery Office.

[9] GREAT BRITAIN. *Freedom of Information (Scotland) Act 2002*. Edinburgh: The Stationery Office.

[10] US DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Special Publication 800-161. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, Maryland, USA, 2015. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf [viewed December 2018].

[11] SAE INTERNATIONAL. J3061-201601 *CybersecurityGuidebook for Cyber-Physical Vehicle Systems.* Available from https://www.sae.org/standards/content/j3061_201601/ [viewed December 2018].

[12] SAE INTERNATIONAL. J2836/1_201004. *Use Cases for Communication Between Plug-In Vehicles and the Utility Grid.* Available from https://www.sae.org/standards/content/j2836/1_201004/ [viewed December 2018].

13.3 Further reading

BS 7858, *Security screening of individuals employed in a security environment – Code of practice.*

BS ISO 55001:2014, *Asset management – Management systems – Requirements.*

BS ISO 55002, *Asset management – Management systems – Guidelines for the application of ISO 55001.*

BS EN ISO/IEC 27001:2017, *Information technology – Security techniques – Information security management systems – Requirements.*

BS ISO/IEC 29100, *Information technology – Security techniques – Privacy framework.*

BS ISO/IEC 38500:2015, *Information technology – Governance of IT for the organization.*

BS ISO/IEC 38505-1:2017, *Information technology – Governance of IT – Governance of data – Application of ISO/IEC 38500 to the governance of data.*

Elliot, M., Mackey, E., O'Hara, K. and Tudor, C. *The Anonymization Decision-Making Framework*. Manchester: UKAN Publications, 2016.

Floridi, L. *Information – A Very Short Introduction*. 2010. Oxford: Oxford University Press.

IEC 62443 series, *Industrial communication networks – Network and system security.*

PAS 555, *Cyber security risk – Governance and management – Specification.*

ETSI TR 102 893, *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)* Available: http://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.02.01_60/tr_102893v010201p.pdf [viewed December 2018].

Annex A (informative)
Security concepts and relationships

When considering the cyber security of a vehicle and/or vehicle system there is a need to evaluate whether the product, or service it provides, fulfils the security needs of its owner, operator and users. BS ISO/IEC 15408-1:2009 provides a guide for the development, evaluation and/or procurement of information technology products with security functionality. It seeks to address protection of assets from unauthorized disclosure, modification, or loss of use, these security failures relate to three of the eight security goals shown in Figure 1, i.e. confidentiality, integrity, and availability.

This Annex draws upon the security concepts and relationships described in BS ISO/IEC 15408-1 to provide a model that is relevant to complex cyber-physical systems, such as the automotive ecosystem and its constituent vehicles, vehicle systems and infrastructure. The concepts and relationships have been summarized in Figure 3. The model can be applied to the eight security goals and is applicable to personnel, physical, process and technical risks.

The automotive ecosystem comprises an increasingly complex range of assets, including physical assets such as the vehicles, and digital assets such as the software used in the ecosystem and the data and/or information that is processed by the vehicle systems. The assets are valued by their owner, operator and/or user as they may be used to provide a benefit to one or more organizations and/or individuals. Actual or potential threat actors may also place some value on the assets and through adverse actions seek to harm the interests of those who receive benefits from the assets. The threat actors may be:

- acting maliciously, for example criminals, hackers or malicious users; or
- non-malicious, where their actions or inactions may be accidental or deliberate, for example user errors, mistakes or misunderstandings, failure of automated processes and accidents caused by third parties.

The actions or inactions of threat actors gives rise to threats to the asset and increase the risks to the that the use and/or enjoyment of the asset and the benefits it delivers may be impaired or denied.

Often threats relate to potential exploitation of a vulnerability contained in the asset that may arise through a weakness in the design or incorrect implementation, operation or maintenance of it. Potential sources of vulnerabilities include accidental errors made during development, poor design, intentional addition of malicious code, poor testing, configuration or maintenance, or incorrect operation. For example, weaknesses in the design of remote vehicle locking and keyless entry and ignition systems have been exploited by criminals to steal vehicles. Vulnerabilities may also arise from use of a vehicle in an operating environment for which it was not specified or designed. Given the complex nature of vehicles and vehicle systems, previously unknown errors or vulnerabilities may emerge throughout the vehicle system lifecycle.

The presence of a vulnerability can lead to a new risk or may increase the likelihood, probability or impact of an existing risk. It may also create a hazard, i.e. a source of potential harm to people, other assets or the environment. Where an organization, owner or user is aware of a potential hazard, risk or vulnerability they may evaluate it and consider steps need to be taken to reduce the risk or vulnerability, or to mitigate the hazard. This is typically achieved by imposing security or safety control or applying countermeasures. For example, a temporary procedural security control may require that a vulnerable vehicle is parked in a secured location or to be fitted with physical anti-theft devices to prevent criminals exploiting a weakness in its remote locking system. The vehicle manufacturer may subsequently seek to reduce the risk of theft by implementing design changes to the locking system and retrofitting or patching existing vehicles.

The ownership of a risk and therefore the responsibility for managing it will depend on the nature of the risk and associated threat(s), and its impact on the asset(s) and the benefit(s) delivered. When defending the decision to accept the risks associated with a specific threat or vulnerability the responsible party should be able to demonstrate that:

- any countermeasures are *sufficient*, i.e. that if they do what they claim to do, the threats to the assets are reduced to an acceptable level; and
- the countermeasures are *correct*: i.e. they do what they claim to do.

When applying a new control or countermeasure an organization, owner or user should be aware that this may possess or introduce a new vulnerability, increase the severity of an existing vulnerability or make it more accessible. Experience in both the IT and automotive sectors indicates that patching systems is not infallible, and in both sectors, there have been instances of patches causing loss of availability of systems and vehicles, and the potential for introducing new vulnerabilities.

The creation or use on new and/or upgraded assets, or access to new or enhanced benefits, may create new opportunities both for the intended organization, owner or user, and for threat actors seeking to exploit vulnerabilities. For example, the introduction of smartphone-based applications that allow remote interaction with a vehicle provide benefits to an owner or user but may also create opportunities for unauthorized access to the vehicle, thus allowing malicious actions that affect the vehicle, its user or its contents.

NOTE *Further guidance on handling the relationship between safety and security will be provided in the forthcoming PAS 11281.*

Annex B (informative) Case study

The case study highlights the interactions between products, systems and services in connected automotive environment, and is based on the communications protocols and use cases provided in BS EN ISO 15118-1:2015 and SAE J2836/1 [11]. It illustrates elements that may make up a vehicle system or vehicle service, where a security-minded approach is required to protect sensitive information.

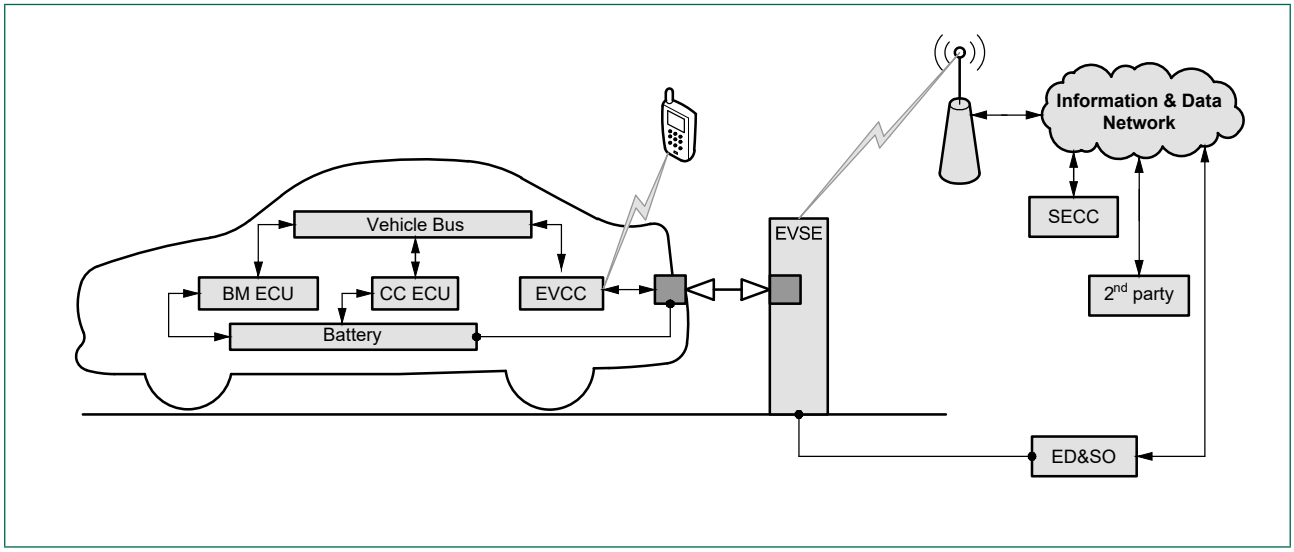
In Figure B1 the following products that have been integrated by the vehicle manufacturer to operate as the vehicle's energy storage system:

- battery – the on-vehicle energy storage device;
- Battery Management ECU (BM ECU) – manages the overall health of the battery and the charge/discharge of individual battery cells;
- Charge Control ECU (CC ECU) – manages the charging battery over the charge cycle taking into account customer settable preference, the total energy requested, the energy supplied and applicable tariffs during current charging event and the total cost of the energy supplied;
- Electric Vehicle Communications Controller (EVCC) – provides communications between the vehicle and the charging service providers via the EVSE, using power line communications (PLC) via the charging cable, and a user interface via a Bluetooth connection to the vehicle user's smartphone when within range of the vehicle.
- Each of the above products may have been delivered to the vehicle manufacturer by different suppliers, who in turn may have integrated products (i.e. components and sub-systems) or manufactured the entire product themselves.

The vehicle itself is a system-of-systems, with the vehicle energy system communicating over the vehicle data bus that is shared with other systems and sub-systems. Within the vehicle, data and information about the charging state and health of the energy system potentially crosses a number of trust boundaries, for example between the BM ECU, CC ECU and EVCC as it is transferred via the vehicle bus.

For a vehicle's user to charge the vehicle, the vehicle's energy storage system is connected to a product, the Electric Vehicle Supply Equipment (EVSE), which is part of a complex systems-of systems – the electric vehicle charging ecosystem.

Figure B1 – Electric Vehicle Charging



The charging ecosystem, comprises an on-vehicle component, the EVCC, the off-vehicle component, the EVSE, and the systems and services provided by the SECC and the EDSO. The functions of the off-vehicle elements are:

- the EVSE is a product used to deliver the charging electricity supply to the vehicle, includes power, communications and control functionality, so that users/vehicles can be identified, authorized and draw metered energy from the electricity supply network.
- the Supply Equipment Communications Controller (SECC) controls multiple EVSEs within a distribution area, managing connections and limiting supply to a level that can be safely delivered by the local electricity infrastructure.
- the Electricity Distribution and Supply Organization (ED&SO) is responsible for managing the supply of electricity to the EVSE and the demand within the local electricity distribution network. It may be the local electricity distribution network operator (DNO) or a third party that is providing connectivity from the DNO's supply network to a portfolio of EVSEs located roadside, in carparks, etc.

To control the charging ecosystem in public places, i.e. where multiple users have access to an EVSE and individual users' accounts need to be billed for energy consumed, connectivity is required as a minimum between the EVSE and the SECC. This is likely to be achieved using the cellular (mobile) telephone network.

The charging ecosystem will contain a number of trust boundaries, for example between:

- the EVCC and the EVSE
- the vehicle user or user's mobile phone and the EVSE, for authorization of charging;
- the EVSE and SECC for charging authorization and billing purposes
- the SECC and the ED&SO for charging and billing purposes; and
- provision of data and information to third parties regarding the use of individual EVSEs, operational and billing data and/or information.

As these boundaries involve transfer of data and/or information over the public telecommunications network and/or Internet, there are security issues related to the protection of these flows, the continuity of operations and the provenance of the data and/or information.

The products and systems identified above will be used to deliver a range of vehicle-related services, that potentially include:

- provision of charging information, EVSE locations and access, and tariff information to an application running on the vehicle user's smart phone;
- managing the supply of electricity via the EVSE by the system operator, including the billing of the vehicle user or an account associated with the vehicle; and
- where the vehicle is not owned by the vehicle user, provision of information to second parties for fleet management and accounting purposes.

The provision of such services introduces further trust boundaries, requiring privacy and security issues to be considered as data and/or information flows across organizational boundaries, for example from the EVSE/SECC operator to the provided to the operator of the smart-phone application.

From a systems and security engineering perspective the scenario illustrated in Figure A1 involves a complex information sharing environment, where implementation of security-by-default requires a detailed understanding of the flow and nature of information used, where it is being generated, stored and processed, and the degree to which this it proportionate to the needs of specific products, systems and/or service providers.

For example:

- the battery, BM ECU and CC ECU may store information about the vehicle's pattern of use, including energy demand profiles, times and dates of charging;
- the CC ECU and EVCC may store information about times, dates and locations of charging and the identity of the user and/or account that is being billed for charging, or, in the case of electricity to grid, credited for energy usage;
- the EVCC storing vehicle (e.g. vehicle identification number – VIN) and user account information for transmission to the EVSE and SECC as part of the identification and authentication process prior to commencing charging;
- the EVSE and SECC processing personally identifiable information (VIN and user account data) to authorize charging and enable energy billing;
- the EVSE and SECC communicating with 2nd parties for fleet management or billing consolidation purposes, and with the ED&SO regarding supply/demand for electricity;
- collecting user data from smartphone apps regarding the user's locations, vehicle, charging needs and account/billing arrangements.

The above information could be used to build a detailed profile of vehicle use, including the identity or affiliation of users, frequently used charging location, home or office locations if the vehicle is routinely charged at either.

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 978-0-580-51152-3