# The Key Principles of Cyber Security for Connected and Automated Vehicles

HM Government

# Contents

**Intelligent Transport System (ITS) & Connected and Automated Vehicle (CAV) System Security Principles:**

- 1. Organisational security 2
- 2. Security risks are assessed 5
- 3. Organisations product aftercare 6

**ITS/CAV System Design Principles:**

- 4. Organisations working together 9
- 5. System Defence 10
- 6. Software Security 13
- 7. Data storage and transmission 14
- 8. Resiliently designed systems 17

**Troubleshooting**

As vehicles get smarter, cyber security in the automotive industry is becoming an increasing concern. Whether we're turning cars into Wi-Fi connected hotspots or equipping them with millions of lines of code to create fully autonomous vehicles, cars are more vulnerable than ever to hacking and data theft.

It's essential that all parties involved in the manufacturing supply chain, from designers and engineers, to retailers and senior level executives, are provided with a consistent set of guidelines that support this global industry. The Department for Transport (DfT), in conjunction with the Centre for the Protection of National Infrastructure (CPNI), have created the following key principles for use throughout the automotive sector, the CAV and ITS ecosystems and their supply chains.

*Principle 1*

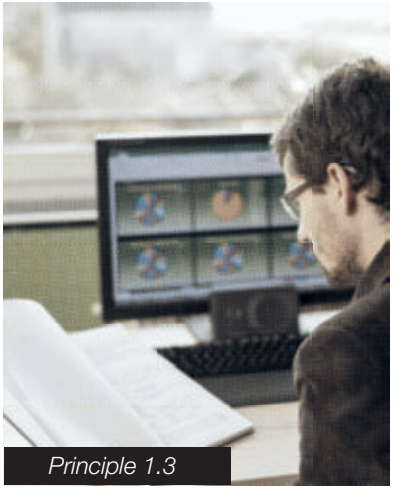
**Organisational security is owned, governed and promoted at board level.**

*Principle 1.1*

There is a **security program** which is aligned with an organisation's broader mission and objectives.

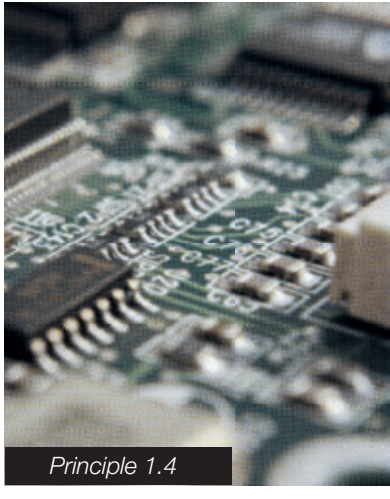
*Principle 1.2*

**Personal accountability is held at the board level** for product and system security (physical, personnel and cyber) and delegated appropriately and clearly throughout the organisation.



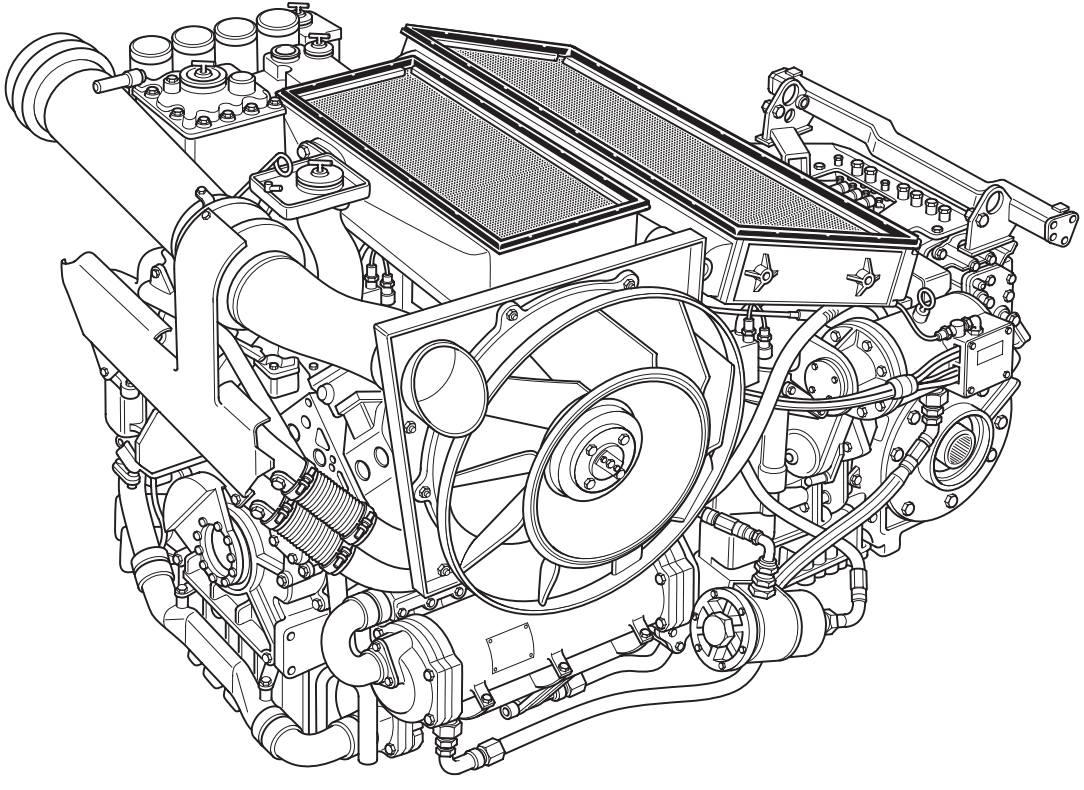
*Principle 1.3*

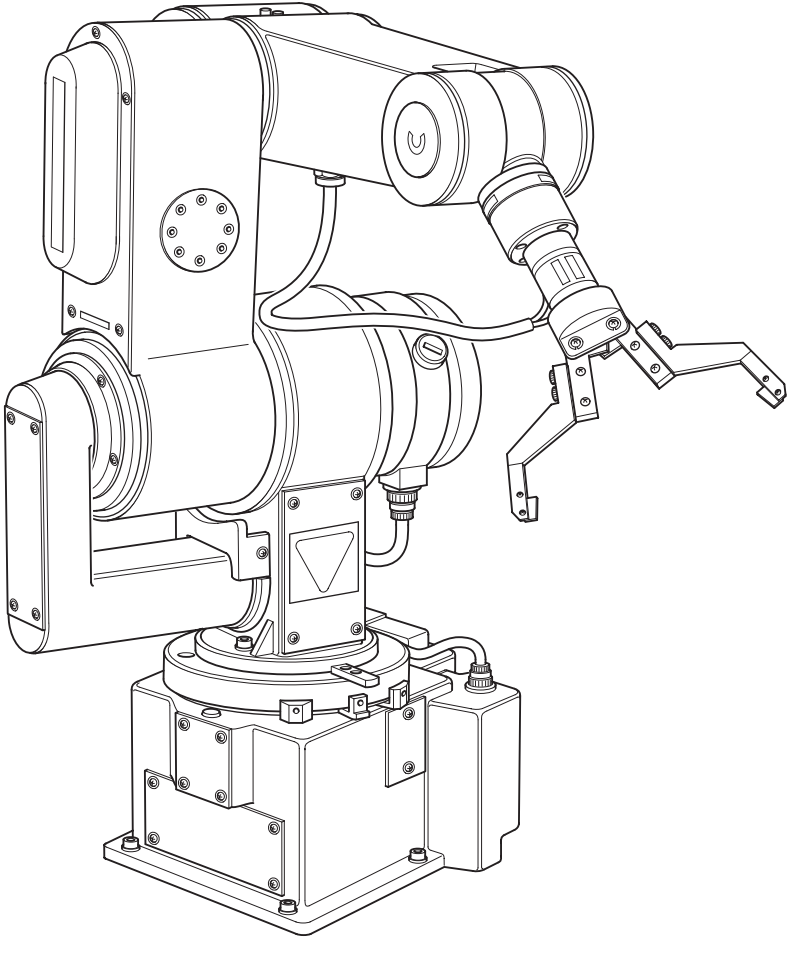
**Awareness and training** is implemented to embed a 'culture of security' to ensure individuals understand their role and responsibility in ITS/CAV System security.



*Principle 1.4*

All new designs embrace **Security by Design.** Secure design principles are followed in developing a secure ITS/CAV System, and all aspects of security (physical, personnel and cyber) are integrated into the product & service development process.





*Principle 2*

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

*Principle 2.1:*

Organisations must require **knowledge and understanding of current and relevant threats** and the engineering practices to mitigate them in their engineering roles.

*Principle 2.2:*

**Organisations collaborate** and engage with appropriate third parties to enhance threat awareness and appropriate response planning.

*Principle 2.3:*

**Security risk assessment and management procedures** are in place within the organisation. Appropriate processes for identification, categorisation, prioritisation, and treatment of security risks, including those from cyber, are developed.

*Principle 2.4:*

Security risks specific to, and/or encompassing, **supply chains, sub-contractors and service providers** are identified and managed through design, specification and procurement practices.

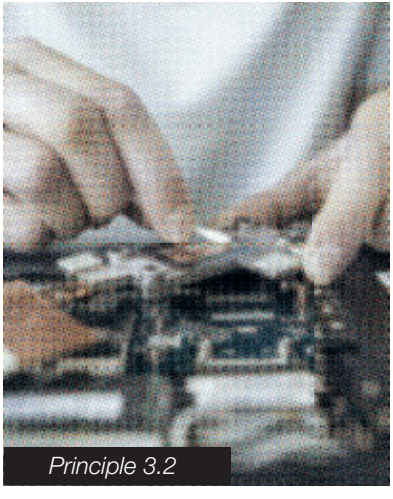
*References: Def Stan 05-138, ISO 15408, ISO 27002, ISO 27010, ISO 27034, NIST800-30, PAS 1192-5*

*Principle 3*

**Organisations need product aftercare and incident response to ensure systems are secure over their lifetime.**

*Principle 3.1*

Organisations plan for how to **maintain security over the lifetime of their systems,** including any necessary after-sales support services.

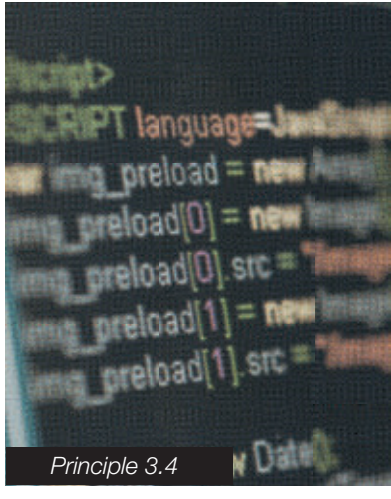


*Principle 3.2*

**Incident response plans are in place.** Organisations plan for how to respond to potential compromise of safety critical assets, non-safety critical assets, and system malfunctions, and how to return affected systems to a safe and secure state.

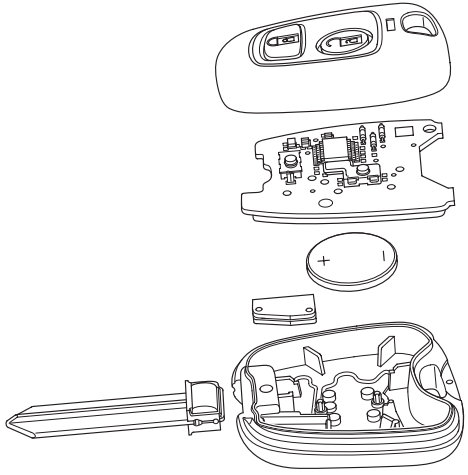
*Principle 3.3*

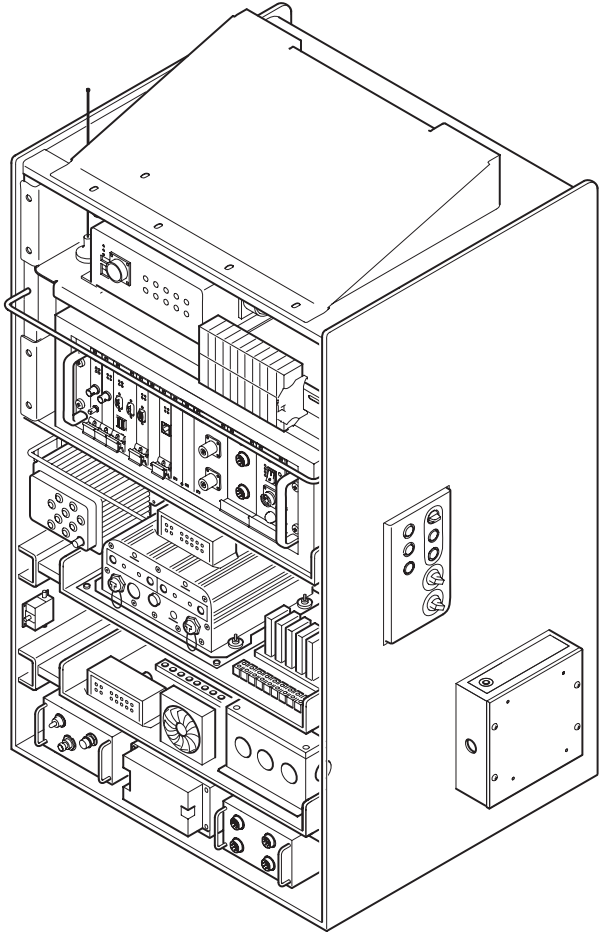
There is an active programme in place to **identify critical vulnerabilities** and appropriate systems in place to mitigate them in a proportionate manner.




*Principle 3.4*

Organisations ensure their systems are able to **support data forensics** and the recovery of forensically robust, uniquely identifiable data. This may be used to identify the cause of any cyber, or other, incident.






9 501101530 0 3
1
2
3
4
5
6
7
8
9
10
ENTER

*Principle 4*

**All organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system.**

*Principle 4.1:*

Organisations, including suppliers and 3rd parties, must be able to **provide assurance,** such as independent validation or certification, of their security processes and products (physical, personnel and cyber).

*Principle 4.2:*

It is possible to ascertain and validate the **authenticity and origin of all supplies** within the supply chain.

*Principle 4.3:*

Organisations jointly plan for how systems will **safely and securely interact with external devices,** connections (including the ecosystem), services (including maintenance), operations or control centres. This may include agreeing standards and data requirements.

*Principle 4.4:*

Organisations identify and **manage external dependencies.** Where the accuracy or availability of sensor or external data is critical to automated functions, secondary measures must also be employed.

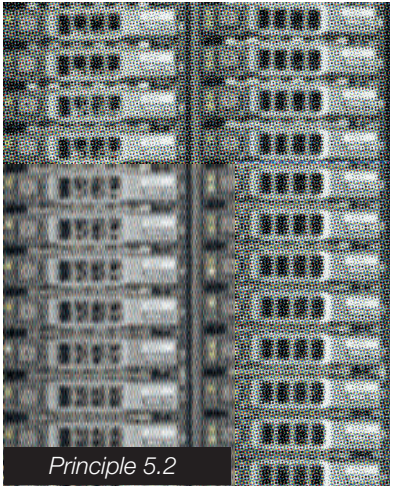
*References: Def-Con 05-138, ISO 12207, ISO 27001, ISO 27002*

*Principle 5*

**Systems are designed using a defence-in-depth approach.**

*Principle 5.1*

The security of the system does **not rely on single points of failure,** security by obscuration or anything which cannot be readily changed, should it be compromised.

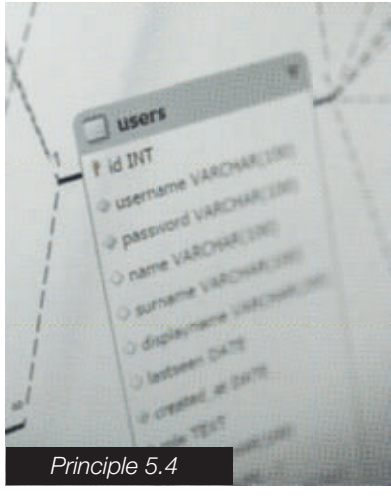


*Principle 5.2*

The security architecture applies **defence-in-depth & segmented** techniques, seeking to mitigate risks with complementary controls such as monitoring, alerting, segregation, reducing attack surfaces (such as open internet ports), trust layers/ boundaries and other security protocols.

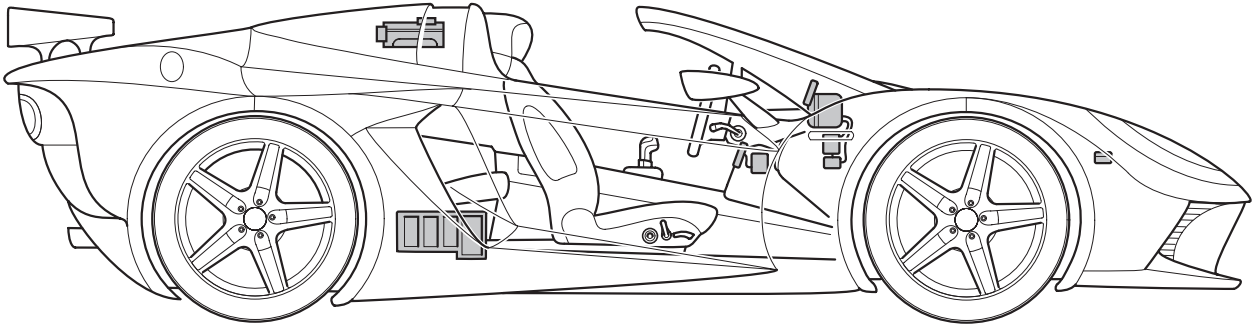
*Principle 5.3*

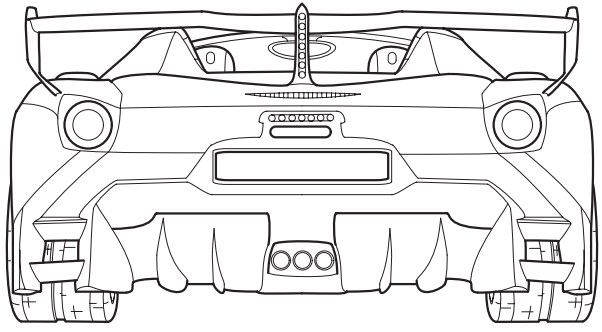
**Design controls to mediate transactions across trust boundaries,** must be in place throughout the system. These include the least access principle, one-way data controls, full disk encryption and minimising shared data storage.

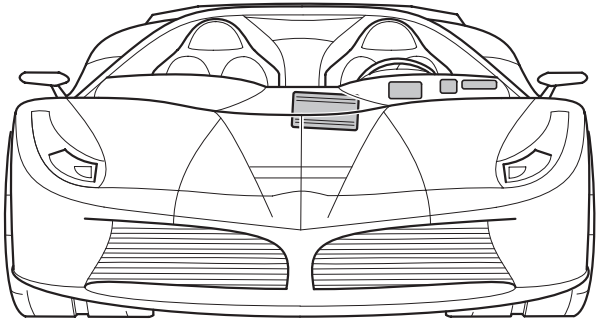



*Principle 5.4*

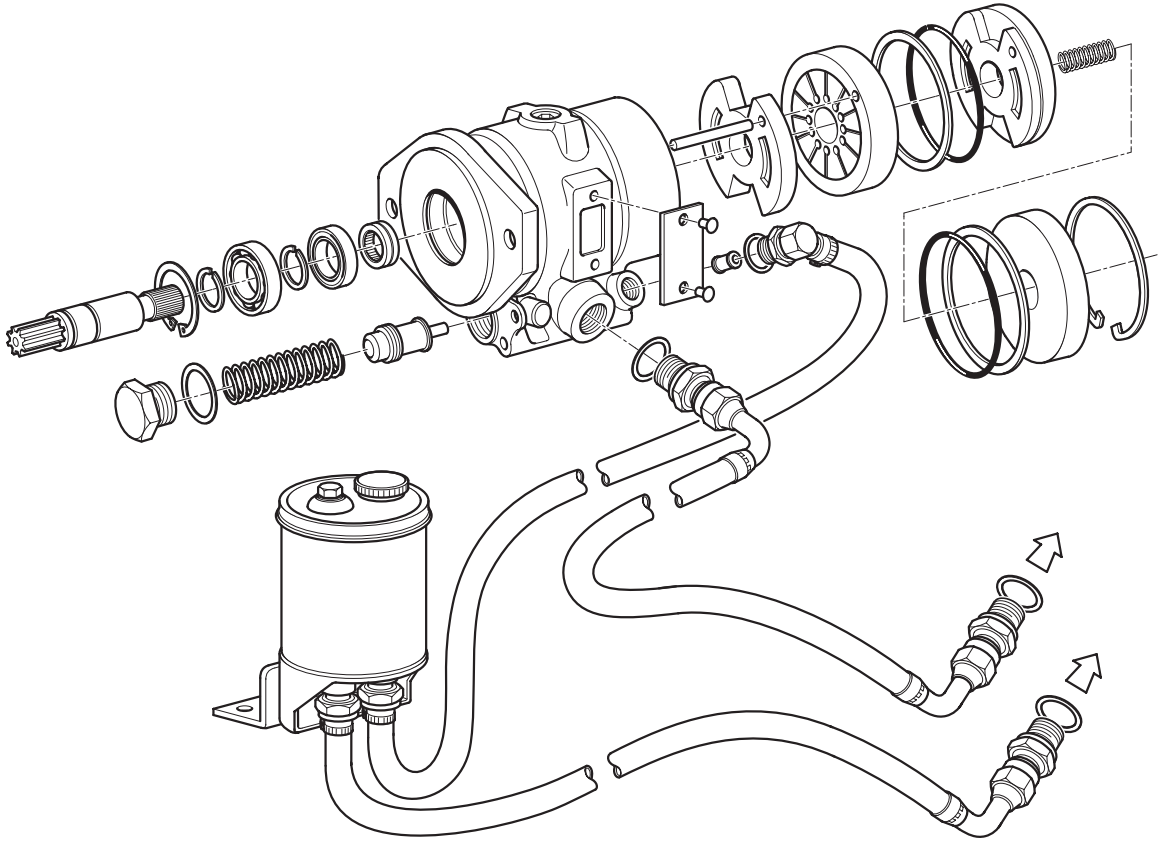
**Remote and back-end systems,** including cloud based servers, which might provide access to a system have appropriate levels of protection and monitoring in place to prevent unauthorised access.







*References: SAE J3061, SAE J3101, ISO 15408, ISO 27034, ISO 29119*



*Principle 6*

**The security of all software is managed throughout its lifetime.**

*Principle 6.1:*

Organisations adopt **secure coding practices** to proportionately manage risks from known and unknown vulnerabilities in software, including existing code libraries. Systems to manage, audit and test code are in place.

*Principle 6.2:*

**It must be possible to ascertain the status of all software,** firmware and their configuration, including the version, revision and configuration data of all software components.

*Principle 6.3:*

It is possible to **safely and securely update software** and return it to a known good state if it becomes corrupt.

*Principle 6.4:*

Software adopts **open design practices** and peer reviewed code is used where possible. Source code is able to be shared where appropriate.

*References: Microsoft SDL, SAFE Code best practices, OWASP CLASP, ISO 12207, PAS 754*

*Principle 7*

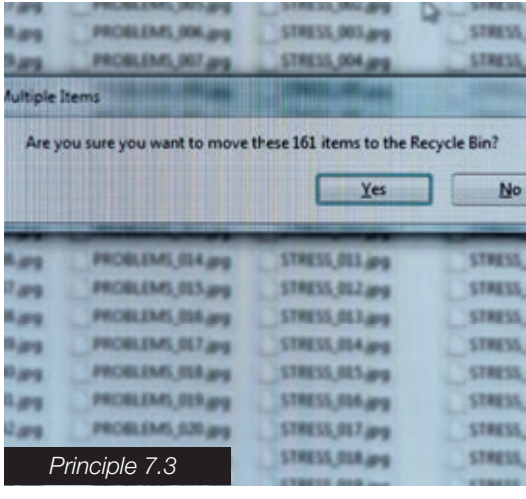
**The storage and transmission of data is secure and can be controlled.**

*Principle 7.1*

**Data must be sufficiently secure** (confidentiality and integrity) when stored and transmitted so that only the intended recipient or system functions are able to receive and/or access it. Incoming communications are treated as unsecure until validated.

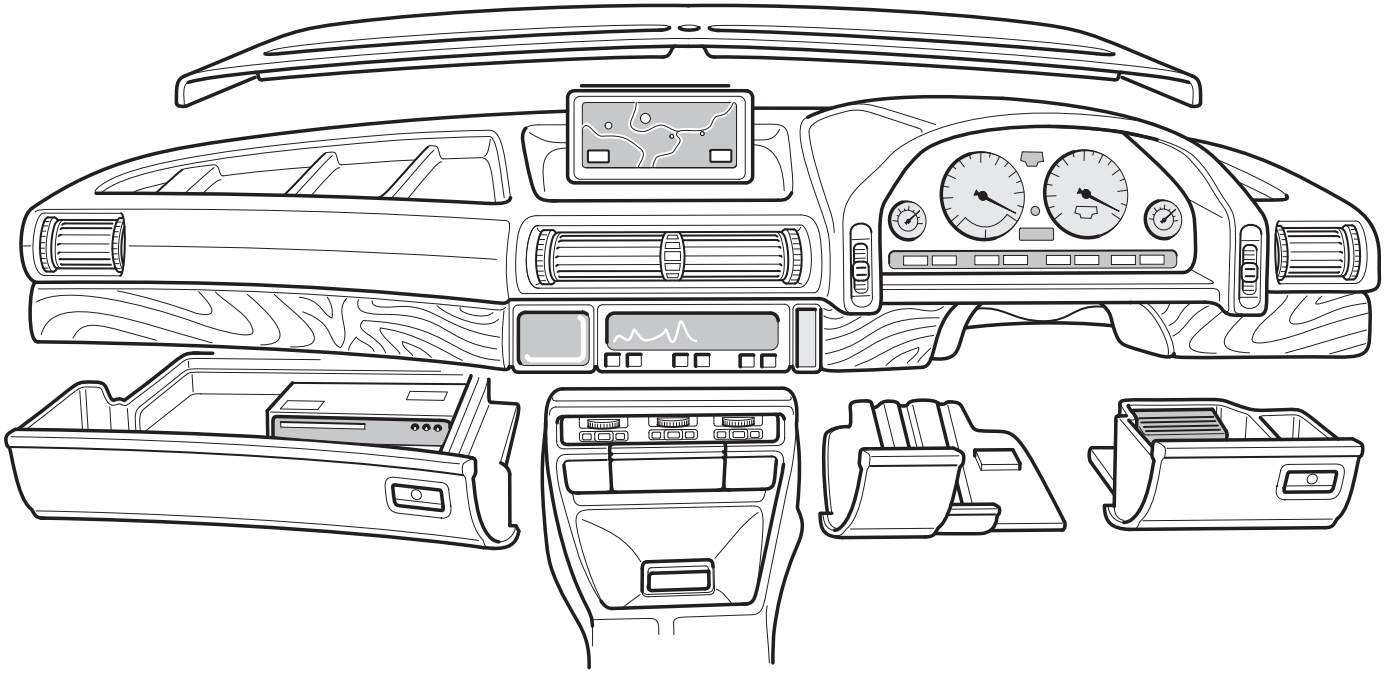
*Principle 7.2*

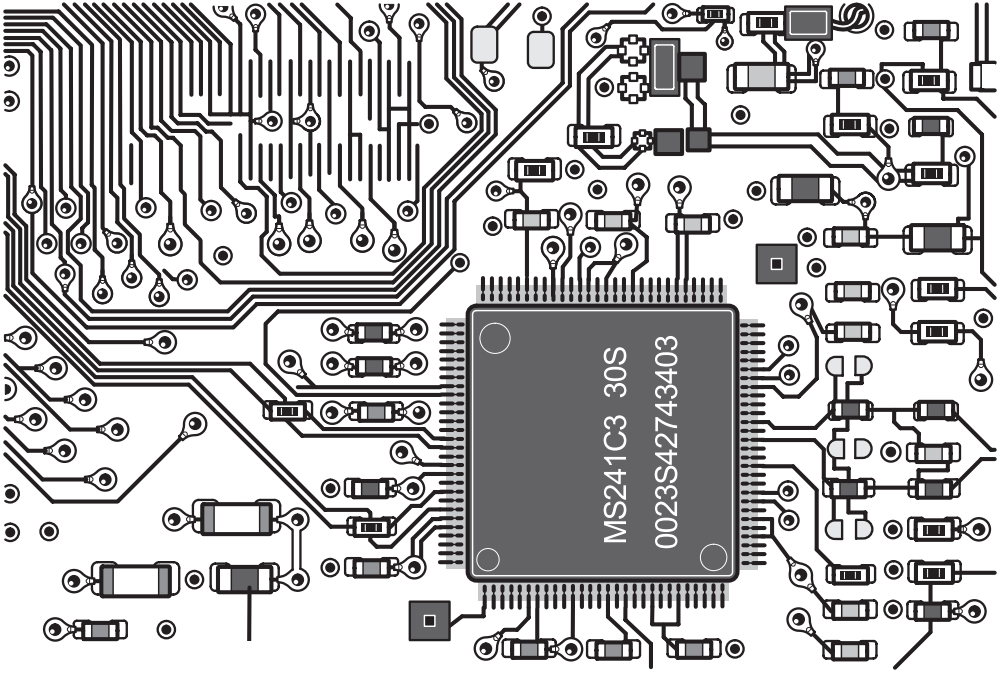
**Personally identifiable data must be managed appropriately.** This includes: what is stored (both on and off the ITS/CAV System); what is transmitted; how it is used and the control the data owner has over these processes. Where possible, data that is sent to other systems is sanitised.




*Principle 7.3*

**Users are able to delete sensitive data,** such as personally identifiable data, held on systems and connected systems.




MS241C3 30S
0023S42743403

*Principle 8*

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

*Principle 8.1:*

The system must be able to **withstand receiving corrupt, invalid or malicious data or commands** via its external & internal interfaces while remaining available for primary use. This includes sensor jamming or spoofing.

*Principle 8.2:*

**Systems are resilient and fail-safe** if safety-critical functions are compromised or cease to work.
The mechanism is proportionate to the risk. The systems are able to respond appropriately if non-safety critical functions fail.


*Reference: ISO 9797-1*

## Troubleshooting | Applicable Standards and Guidance*:

**SAE**

- J3061 - Cybersecurity guidebook for cyber-physical vehicle systems.
- J3101 - Requirements for hardware protected security for ground vehicle applications.

**ISO**

- 9797-1 – Security techniques: Message authentication codes – specifies a model for secure message authentication codes using block cyphers and asymmetric keys.
- 12207 – Systems and software engineering – software lifecycle processes.
- 15408 – Evaluation of IT security – specifies a model for evaluating security aspects within IT.
- 27001 – Information security management system.
- 27002 – Code of practice – security – provides recommendations for information management. Contains guidance on access control, cryptography & supplier relationship.
- 27010 – Information security management for inter-sector and inter-organizational communications.
- 27018 – Code of practice – handling PII / SPI (Privacy) – Protection of Personally Identifiable Information (PII) in public clouds.
- 27034 – Application security techniques – guidance to ensure software delivers necessary level of security in support of an organisations security management system.
- 27035 – Information security incident management.
- 29101 – Privacy architecture framework.
- 29119 – Software testing standard.

**DEFSTAN**

- 05-138 – Cyber security for defence suppliers.

**NIST**

- 800-30 - Guide for conducting risk assessments.
- 800-88 - Guidelines for media sanitization.
- SP 800-50: Building an information technology security awareness and training program.
- SP 800-61: Computer security incident handling guide.

**Other**

- Microsoft Security Development Lifecycle (SDL).
- SAFE Code best practices.
- OWASP Comprehensive, Lightweight Application Security Process (CLASP).
- HMG Security policy framework.
- PAS 1192-5 – BSI publication on security-minded building information modelling, digital built environments and smart asset management.
- PAS 754 – BSI publication on Software Trustworthiness, governance and management.
- NCSC Cyber Essentials and 10 steps.
- To download a copy visit gov.uk.
- For further info contact cyber@dft.gsi.gov.uk.

**This list is not intended to be exhaustive. Further standards and guidance may be applicable. It is recommended that for specific technologies or processes corporations should check for any applicable standards or guidance that might be of relevance and for any new standards that have been developed in the field.*