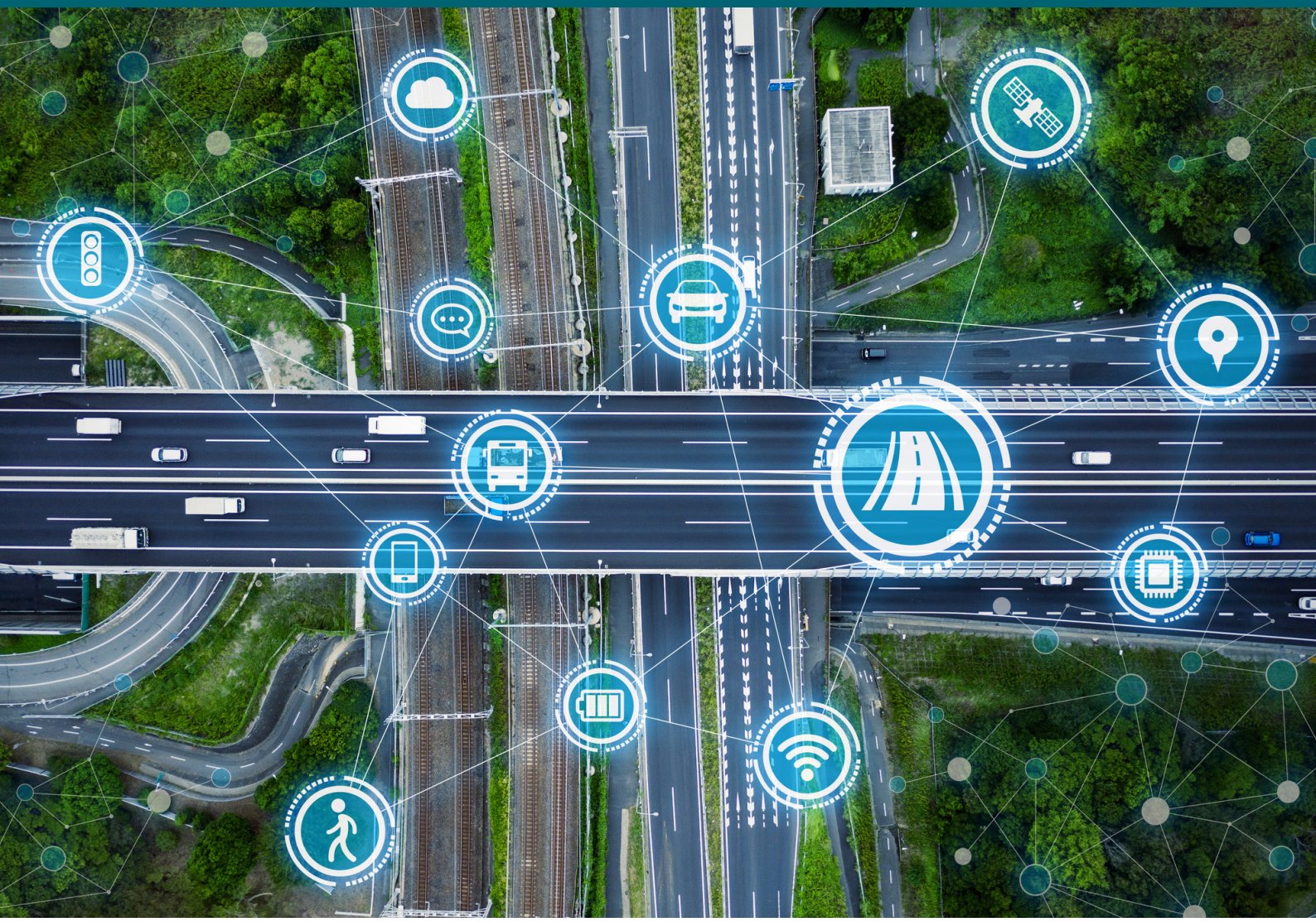
PAS 11281:2018

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



CPNI®
Centre for the Protection of National Infrastructure

bsi.

Publishing and copyright information

ISBN 978 0 539 02394 7

ICS 03.080.01, 03.220.20

Publication history

First published December 2018

Contents

Foreword

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

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

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

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

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

Use of this document

As a code of practice, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this PAS is expected to be able to justify any course of action that deviates from its recommendations.

It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Information about this document

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

Presentational conventions

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

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

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

Contractual and legal considerations

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

Compliance with a PAS cannot confer immunity from legal obligations.

0 Introduction

0.1 The connected automotive ecosystem

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

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

CAV technology is seen as potentially enabling increased:

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

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

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

0.2 Security-informed safety

Security-informed safety is the consideration of the impact of security risks on safety. Traditionally, security and safety have been treated as separate disciplines, with their own regulations, standards, culture and engineering. Safety can be seen as protecting against harm due to unintentional actions, while security is often seen as preventing harm due to the intentional actions of malicious actors. However, there is a growing realization that security and safety are closely interconnected and interdependent: it is no longer acceptable to assume that a safety system is immune from attack because it is built using bespoke hardware and software, or because it is separated from the outside world by an air gap. A safety justification, or safety case, is incomplete and unconvincing without a consideration of the impact of security. This can be succinctly summarized as "if it's not secure, it's not safe".

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

0.3 The approach taken for this PAS

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

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

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

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

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

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

0.4 How this PAS helps

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

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

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

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

Table 1 – Individual roles

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

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

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

1 Scope

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

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

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

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

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