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 It will be withdrawn upon publication of its content in, or as, a British Standard.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