Singapore Standards Council

TR 68 : Part 3 : 2019

(ICS 35.030; 43.020)

TECHNICAL REFERENCE

Autonomous vehicles

– Part 3 : Cybersecurity principles and assessment framework

Published by

Enterprise Singapore

TR 68 : Part 3 : 2019
(ICS 35.030; 43.020)

TECHNICAL REFERENCE

Autonomous vehicles

– Part 3 : Cybersecurity principles and assessment framework

ISBN 978-981-48-3560-2

This Technical Reference was approved on 8 January 2019 by the Manufacturing Standards Committee under the purview of the Singapore Standards Council.

First published, 2019

The Manufacturing Standards Committee, appointed by the Standards Council, consists of the following members:

		Name	*Capacity*
Chairman	:	Dr John Yong	*Individual Capacity*
Deputy Chairman	:	Mr Brandon Lee	*Individual Capacity*
Secretary	:	Mr Kwok Wing Kit	*Singapore Manufacturing Federation – Standards Development Organisation*
Members	:	Ms Fong Pin Fen	*Economic Development Board*
		Mr Goh Wee Hong	*TÜV SÜD PSB Pte Ltd*
		Mr Ho Chi Bao	*Enterprise Singapore*
		Mr Steven Koh	*Singapore Precision Engineering Technology Association*
		Ms Lee Wan Sie	*Info-communications Media Development Authority*
		Dr Jim Li Hui Hong	*Individual Capacity*
		Dr Lim Ee Meng	*A*STAR National Metrology Centre*
		Mr Loh Wai Mun	*A*STAR Science Engineering Research Council*
		Er. Prof Ramakrishan Seeram	*The Institution of Engineers, Singapore*

The Technical Committee on Automotive, appointed by the Manufacturing Standards Committee and responsible for the preparation of this standard, consists of representatives from the following organisations:

		Name	Capacity
Co-Chairmen	:	Mr Lam Wee Shann	*Individual Capacity*
		Assoc Prof Marcelo H Ang Jr	*Individual Capacity*
Secretary	:	Mr Kwok Wing Kit	*Singapore Manufacturing Federation – Standards Development Organisation*
Members	:	Mr Chandrasekar s/o Palanisamy	*Land Transport Authority*
		Mr Alvin Chia	*Land Transport Authority*
		Dr Chin Kian Keong	*Land Transport Authority*
		Mr Niels de Boer	*Centre of Excellence for Testing & Research of AVs – NTU*
		Dr Jaya Shankar s/o Pathmasuntharam	*A*STAR Institute for Infocomm Research*
		Mr Lim Soon Chia	*Cyber Security Agency of Singapore*
		Mr Mahesh Tanwani	*Aptiv PLC*
		Mr Peter Quek	*Land Transport Authority*

Members	:	Mr Tan Nai Kwan	*ST Engineering Land Systems Ltd*
		Dr Vrizlynn Thing	*A*STAR Institute for Infocomm Research*
		Mr Daryl Yeo	*Ministry of Transport*

The Working Group on Cybersecurity Principles and Assessment Framework, appointed by the Technical Committee to assist in the preparation of this standard, comprises the following experts who contribute in their *individual capacity*:

		Name
Co-Convenors	:	Mr Peter Quek Ser Hwee
	:	Mr Lim Soon Chia
	:	Dr Vrizlynn Thing
Secretary	:	Mr Louis Lauw
Members	:	Mr Chew Thiam Soon
		Mr Gerry Chng
		Mr Dai Zhongmin
		Mr Huang Shaofei
		Mr Cody Kamin
		Mr Koh Ming Yang
		Mr Lai Jin Wei
		Mr Marcus Lim
		Dr Lim Woo Lip
		Dr Bekmamedova Nargiza
		Dr Ong Chen Hui
		Ms Eley Querner
		Dr Giedre Sabaliauskaite
		Mr Natarajan Somou Suresh
		Ms Andrea Teo
		Dr Yi Estelle Wang
		Mr Thomas Webster

The organisations in which experts of the Working Group are involved are:

Aptiv PLC
*A*STAR Institute for Infocomm Research*
Centre of Excellence for Testing & Research of AVs – NTU
Continental Automotive Singapore Pte Ltd
Cyber Security Agency of Singapore
DSO National Laboratories
Ernst & Young Singapore
Land Transport Authority
Nova Systems Pte Ltd
nuTonomy
NXP Semiconductors
Singapore Test Services Pte Ltd
Singapore University of Technology and Design

Singtel
StarHub
ST Engineering Land Systems
TÜV SÜD Asia Pacific Pte Ltd

Contents

Foreword

This Technical Reference (TR) was prepared by the Working Group on Cybersecurity Principles and Assessment Framework appointed by the Technical Committee on Automotive under the direction of the Manufacturing Standards Committee.

TR 68 is intended to support the development of AV technology and deployments and consists of the following parts under the generic title "Autonomous vehicles":

Part 1 – Basic behaviour
Sets out fundamental behaviours AVs should exhibit while driving on public roads in order to co-exist safely with entities on the roads such as other vehicles, cyclists, and pedestrians.

Part 2 – Safety
Sets out the safe design and continuing safety management process requirements, supported by competent personnel and organisational quality certifications that organisations should have in place so that the AVs driving on public roads are inherently safe and behave in the manner that they are designed to.

Part 3 – Cybersecurity principles and assessment framework
Sets out principles and assessment framework for organisations to support development and management of AVs. The assessment framework is intended to provide a cybersecurity safeguard for AVs to satisfy prior to on-road deployment.

Part 4 – Vehicular data types and formats
Sets out what data, resolution, capture frequency and the format in which they should be transmitted so that there is seamless communication between sending party and receiving party.

This TR is a provisional standard made available for application over a period of three years. The aim is to use the experience gained to update the TR so that it can be adopted as a Singapore Standard. Users of the TR are invited to provide feedback on its technical content, clarity and ease of use. Feedback can be submitted using the form provided in the TR. At the end of the three years, the TR will be reviewed, taking into account any feedback and or other considerations, to further its development into a Singapore Standard if found suitable.

Attention is drawn to the possibility that some of the elements of this TR may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

Technical Reference for autonomous vehicles
Part 3: Cybersecurity principles and assessment framework

0 Introduction

This TR provides a technical reference for an enhanced cybersecurity framework for autonomous vehicles (AVs) deployed on public roads. Given that Singapore is not a vehicle manufacturing country and would be dependent on the AV developer/operator to provide comprehensive documentation for a security-by-design review, an independent approach is taken instead, to conduct cybersecurity assessment of an AV before it is deployed on public roads.

Two tiers of cybersecurity safeguards are set out in this TR.

The first tier is set out in Clause 5. Cybersecurity principles are presented for AV developers/operators to manage cybersecurity for the full lifecycle of an AV, including design, development, operations, maintenance, and decommissioning. This culminates in a secure-by-design system and secure operations, which are verified by a full internal cybersecurity assessment.

The second tier is set out in Clause 6. A framework for the independent cybersecurity assessment of AV systems is presented with the purpose of providing a recommended process for:

a) Discovering further cyber vulnerabilities and exploitations which may have been overlooked by the AV developer/operator;

b) Testing the preparedness of the AV against cyber threats.

The assessment framework includes three main parts:

i. System review

ii. Threat risk analysis

iii. Cybersecurity testing of the vehicle in three areas:

- Vulnerability analysis
- Fuzz testing
- Attack simulation

This TR should be read in conjunction with the other parts of TR 68. Of particular relevance, Part 2 is referred to in this TR as it covers topics relevant to cybersecurity including QMS, hazard and risk assessment, and provides a means of relating security threats to the in-use risk impacts.

This TR is applicable to the following:

- AV operators, AV developers;
- Government agencies / local authorities;
- Assessor (e.g. testing, inspection and certification bodies);
- Engineering and consulting companies.

The meanings of automation driving levels, automated driving system (ADS), operational design domain (ODD), dynamic driving task (DDT) are as defined in SAE J3016_2018. It is noted that SAE J3016_2018 advises against using the terms “autonomous” or “autonomous vehicle” as these terms may lead to confusion. However, the use of the term “autonomous” is well established, with the terms “autonomous

motor vehicle and “autonomous system” defined in Singapore’s Road Traffic Act. Therefore, to provide consistency with established legislation the term autonomous vehicle (AV) is defined and used in this TR as described above.

1 Scope

The purpose of this TR is to provide a Technical Reference for cybersecurity assessment framework of Autonomous Vehicles deployed on public roads. Specifically, the use case of deployment in Singapore is considered.

This TR normatively references existing standards relevant to automotive safety and cybersecurity, as listed in Clause 2. Its aim is to coordinate and extend the referenced standards to cover the following areas:

- Apply methodology from existing cybersecurity standards and best practices in the context of automotive practices. Where the subject is a cyber-physical vehicle system that includes embedded control systems, and a coupling between the computational elements and physical elements. Furthermore, the subject system has close physical interactions with people and other vehicles while deployed on public roads.

- Extend existent cybersecurity standards and best practices for automotive application to provide an enhanced cybersecurity safeguard in response to the increased security threat potential which is present for vehicles deployed to level 4/5 automation (as defined in SAE J3016_2018) where a human operator is not present in the vehicle to intervene in the event that an attack has compromised it.

The assessment framework takes a threat and risk-based approach and includes a security risk assessment. However, the scope of this TR does not extend to consider risks arising due to any consequential impacts to the physical operation of the vehicle arising from cybersecurity. TR 68: Part 2 should be referred to for further discussion on AV system safety.

Specifically, with reference to Figure 1, the scope of assessment defined in this TR includes the following vehicle zones (and their connected communication channels) that are within the Vehicle Intelligence and Interface Layer:

- Vehicle intelligence zone;
- Device zone;
- HMI zone.

Other zones are considered to be adequately covered by existing standards, or not critical to the safe operation of the AV. As such, zones falling within the following layers are excluded from the scope, but currently not limited to the following:

- Traffic infrastructure layer;
- Vehicle actuation layer.

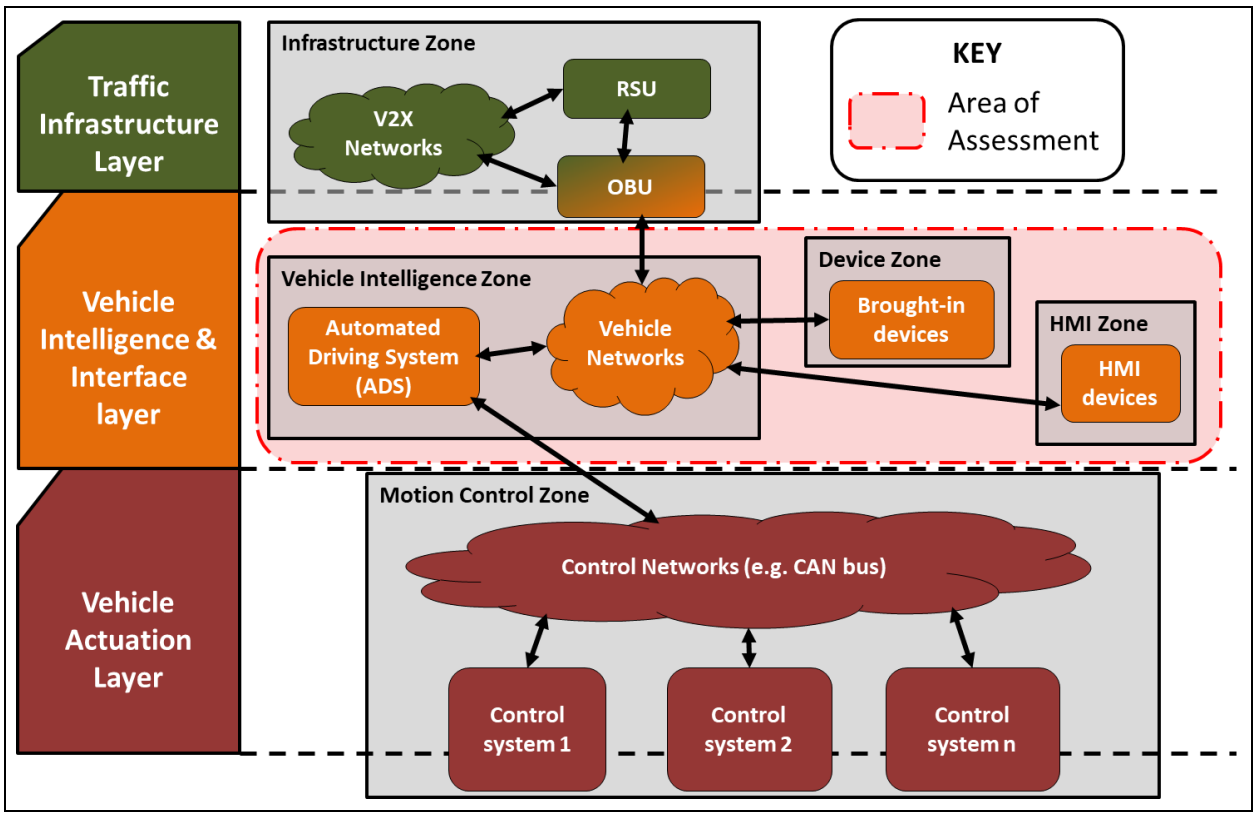

Figure 1 – AV security zone

Key areas of focus for this TR include:

- Approach of an enhanced AV cybersecurity assessment framework;
- Identify potential attack surfaces and threat scenarios; and
- Framework and methodology for AV security testing.

Two tiers of cybersecurity safeguards are set out in this TR. The first tier is set out in Clause 5 where cybersecurity principles are presented for AV developers/operators to manage cybersecurity for the full lifecycle of the AV. The second tier is set out in Clause 6 where a framework for the independent cybersecurity assessment of AV systems is presented.

The fields of automated vehicles and cybersecurity are both experiencing intensive development with new standards and technology developments being released regularly. Therefore, it is likely that this TR will be regularly reviewed and updated to align with industry developments.

2 Normative references

The following documents are referenced for the application of this standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendment) applies.

GSMA CLP.11	IoT security guidelines and CLP.17 IoT Security Assessment.
ISO/IEC 19790:2012	Information technology – Security techniques – Security requirements for cryptographic modules.

ISO/IEC 26262 series	Road vehicles – Functional safety
ISO/IEC 27000 series	Information technology – Security techniques – Information security management systems – Overview and vocabulary
ISO/SAE 21434	Road vehicles – Cybersecurity Engineering (under development)
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment, 2008
OWASP	Open Web Application Security Project
SAE J3016	Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
WP.29	UNECE ITS/AD CS/OTA
TR 64: 2018	Guidelines for IoT Security for Smart Nation