TR 68 : Part 3 : 2021
(ICS 35.030; 43.020)

TECHNICAL REFERENCE

Autonomous vehicles

– Part 3 : Cybersecurity principles and assessment framework

Singapore Standards Council

TR 68 : Part 3 : 2021
(ICS 35.030; 43.020)

TECHNICAL REFERENCE

Autonomous vehicles

– Part 3 : Cybersecurity principles and assessment framework

Published by Enterprise Singapore

ISBN 978-981-5024-07-4

The content of this Singapore Standard was approved on 14 July 2021 by the Manufacturing Standards Committee (MSC) under the purview of the Singapore Standards Council.

First published, 2019
First revision, 2021

MSC consists of the following members:

		Name	Representation
Chairman	:	Dr John Yong	*Individual Capacity*
Deputy Chairman	:	Mr Brandon Lee	*Individual Capacity*
Secretary	:	Mr Louis Lauw	*Singapore Manufacturing Federation – Standards Development Organisation*
Members	:	Dr Gavin Chua	*Science Engineering Research Council*
		Assoc Prof Goh Puay Guan	*National University of Singapore*
		Dr Andrea Hauser	*TÜV SÜD Asia Pacific Pte Ltd*
		Mr Steven Koh	*Singapore Precision Engineering Technology Association*
		Dr Jim Li Hui Hong	*Individual Capacity*
		Dr Lim Ee Meng	*National Metrology Centre*
		Mr Simon Lim	*Enterprise Singapore*
		Prof John Pang	*Nanyang Technological University*
		Dr Alpesh Patel	*McKinsey & Company*
		Ms Joyce Seow	*Singapore Manufacturing Federation*
		Assoc Prof Arlindo Silva	*Singapore University of Technology and Design*
		Mr Sze Thiam Siong	*Testing, Inspection and Certification Interest Group (TIC IG), Singapore Manufacturing Federation*
		Ms Glory Wee	*Economic Development Board*

MSC set up the Technical Committee on Automotive to oversee the preparation of this standard. The Technical Committee consists of the following members:

		Name	Representation
Co-Chairmen	:	Mr Lam Wee Shann	*Individual Capacity*
		Prof Marcelo H Ang Jr	*Individual Capacity*
Secretary	:	Mr Louis Lauw	*Singapore Manufacturing Federation – Standards Development Organisation*
Members	:	Mr Niels de Boer	*Centre of Excellence for Testing & Research of Autonomous Vehicles – NTU*
		Mr Alvin Chia	*Land Transport Authority*
		Mr Chandrasekar s/o Palanisamy	*Land Transport Authority*
		Dr Chin Kian Keong	*Land Transport Authority*

Members	:	Dr Jaya Shankar s/o Pathmasuntharam	*Institute for Infocomm Research*
		Mr Lim Soon Chia	*Cyber Security Agency of Singapore*
		Mr Ling Yuan Chun	*Economic Development Board*
		Mr Peter Quek	*Land Transport Authority*
		Mr Mark Tan	*Ministry of Transport*
		Mr Tan Nai Kwan	*ST Engineering Limited*
		Mr Mahesh Tanwani	*Motional Singapore Pte Ltd*
		Dr Vrizlynn Thing	*ST Engineering Limited*

The Technical Committee set up the Working Group on AV Cybersecurity Principles and Assessment Framework to prepare this standard. The Working Group consists of the following experts who contribute in their individual capacity:

		Name
Co-Convenors	:	Mr Lim Soon Chia
		Mr Peter Quek
		Dr Vrizlynn Thing
Secretary	:	Mr Louis Lauw
Members	:	Mr Chew Thiam Soon
		Mr Gerry Chng
		Mr Chua Teck Yeow
		Mr Dai Zhongmin
		Prof Sylvain Guilley
		Ms Rosita Jupri
		Dr Dennis Kengo Oka
		Mr Koh Ming Yang
		Mr Ian Lai
		Mr Lin Chee Kheong
		Mr Eddy Ong
		Mr Natarajan Somou Suresh
		Mr Marcus Tan
		Ms Andrea Teo
		Dr Yi Estelle Wang

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

Centre of Excellence for Testing & Research of Autonomous Vehicles – NTU
Continental Automotive Singapore Pte Ltd
Cyber Security Agency of Singapore
DSO National Laboratories
Ernst & Young Singapore
Institute for Infocomm Research
Land Transport Authority
Motional Singapore Pte Ltd

Secure-IC Pte Ltd
Singapore Test Services Pte Ltd
ST Engineering Limited
Synopsys Inc
TÜV SÜD Asia Pacific Pte Ltd
UL VS Singapore Pte Ltd

Contents

Page

Figures

Foreword

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

TR 68 series of standards is intended to support the development of Autonomous Vehicle (AV) technology and deployments. It consists of the following parts under the generic title "Autonomous vehicles":

Part 1 – Basic behaviour
Sets out fundamental behaviours AVs 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 can put 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 data types, resolution, capture frequency and the formats in which data are transmitted so that there is seamless communication between the sending party and the 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.

The main changes made in this revision are as follows:

- Updated the definitions;
- Added the following topics:
  - "Security-by-design as 5.1.2
  - "Defence-in-depth as 5.1.3
  - "Continuous operational management and oversight" as 5.1.4
  - "Resiliency" as 5.1.5
  - "Recommendations of Security Requirements for OTA update" as 5.4
  - "Cybersecurity interface agreement" as 6.2
  - "Risk-based approach testing" as 6.6.2
  - "Threat scenario for security risk based testing" as 6.8
  - Annex C and D

Acknowledgement is made to the following for their kind permission to reproduce materials from their documents:

Mr Aljoscha Lautenbach and Mr Mafijul Islam for the reproduction of Table 4-2 "Mapping between STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege) threats and security attributes" from the "HEAling Vulnerabilities to ENhance Software Security and Safety", 2.0, (released on March 18, 2016).

International Organization for Standardization (ISO) for the reproduction of Table I.10 “Attack vector based approach”, Table E.1 “Example CAL determination based on impact and attack vector parameters” and Table E.9 “Component testing methods ([RC-10-03])” from ISO/SAE FDIS 21434 “Road vehicles – Cybersecurity engineering” as Tables 6, 7 and 8 respectively of this TR. ISO standards can be purchased from Enterprise Singapore.

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. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as “Mature Standards”. Mature Standards will not be subject to further review, unless there are requests to review such standards.*

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 and the Singapore Standards Council 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. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*

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

Given that Singapore is not a vehicle manufacturing country and would be dependent on AV developers or operators to provide comprehensive documentation for a security-by-design review, an independent approach is taken instead, to conduct cybersecurity assessment of an AV as an additional safeguard prior to its deployment on public roads.

Two tiers of cybersecurity safeguards are set out in this TR as follows:

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

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

- Discovering further cyber vulnerabilities and exploitations which may have been overlooked by an AV developer or operator; and
- Testing the preparedness of the AV against cyber threats.

The assessment framework includes three main parts:

a) System review;
b) Threat risk assessment; and
c) Cybersecurity testing of the vehicle in four areas:
   - Vulnerability analysis;
   - Fuzz testing;
   - Attack simulation;
   - Vulnerability scanning.

This TR is to 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 quality management system (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 stakeholders:

a) Public or private entities which design and/or manufacture and/or procure and/or install and/or test and/or commission AV technologies, systems and/or solutions;

b) Public or private entities which use AV and/or are in charge of operations and/or maintenance of AV and provide transportation services in public areas; and

c) Independent bodies which check and/or assess AV technologies, systems and/or solutions and/or the operation and maintenance of AVs.

The meanings of driving automation levels, automated driving system (ADS), operational design domain (ODD), dynamic driving task (DDT) are as defined in SAE J3016.

NOTE – SAE J3016 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

1.1 The TR provides the technical provisions for cybersecurity assessment framework of autonomous vehicles deployed on public roads. Specifically, the use case of deployment in Singapore is considered.

This TR covers the following areas:

a) 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.

b) 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 or level 5 automation (as defined in SAE J3016) where a human operator is not present in the vehicle to intervene in the event that an attack has compromised it.

c) Include UNECE R155 and R156, where for future type approval with regard to cybersecurity, the AV developer can conduct exhaustive risk assessment and perform proportionate mitigations to the threats in considering all the risks related to threats referred to Annex A and Annex B.

The assessment framework takes a threat and 6.6.2 risk-based approach and includes a security risk assessment (SRA). 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.

1.2 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 is within the vehicle intelligence and interface layer:

a) Vehicle intelligence zone: In the automated driving system (ADS), operational design domain (ODD), dynamic driving task (DDT) includes perception sensors as mentioned in the following:

- Environmental perception sensors consisting of sensors cluster to capture all relevant external information. Examples of such sensors are camera, Light Detection and Ranging (LIDAR), ultrasonic, radar, etc.

- Global navigation satellite system (GNSS) provides absolute position to the automated vehicle system. High definition (HD) map contains processed a-priori information to detect features such as road marking, lanes that not easily detectable by on-board sensors or to provide a redundant source of information if the on-board sensors fail.

- Motion planning is an object list with specified attributes and parameters as part of trajectory planning. Motion control is to implement the desired vehicle motion; precise actuator commands are derived from the output of motion planning. Motion controller generates set of lateral and longitudinal commands.

- This approach may consists of GNSS, odometry and correction services to achieve precise global coordinates and matching GNSS measurements to a HD map to obtain a relative position on the map.

- Environment mapping using HD map to “detect” features that are not easily detectable by on-board sensors, or to provide a redundant source of information for the environmental perception sensors.

b) Device zone: Brought-in devices connected to the vehicle. Some examples are:

- Backend servers (connecting via USB sticks or other portable media);

- GSM-enabled devices, for example, mobile phones.

c) Human Machine Interface (HMI) zone: A user interface or dashboard that connects a person to a machine, system, or device for the purpose of displaying event information of software stacks, on-board equipment and map navigation displays for the safety of the driver onboard;

d) External interface communications layer is needed to support ADS in allowing retrieving external data information such as GNSS or data measurement such as tyre pressure monitoring system. Some examples of external interface communications are short-range or long-range Wi-Fi communication.

1.3 Other zones are considered to be adequately covered by existing standards, or are 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:

a) Traffic/infrastructure layer; and

b) Vehicle actuation layer.

1.4 The key areas of focus for this TR include:

a) Approach of an enhanced AV cybersecurity assessment framework;

b) Identify potential attack surfaces and threat scenarios; and

c) Framework and method for AV security testing.

The fields of autonomous 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.