FINALIZED DRAFT

AUTOMOTIVE INDUSTRY STANDARD

Approval of vehicles with regards to Cyber Security and Cyber Security management system

Date of hosting: 6th November 2023

Last date for comments: 5th December 2023

INTRODUCTION

The Government of India felt the need for a permanent agency to expedite the publication of standards and development of test facilities in parallel when the work on the preparation of the standards is going on, as the development of improved safety critical parts can be undertaken only after the publication of the standard and commissioning of test facilities. To this end, the erstwhile Ministry of Surface Transport (MOST) has constituted a permanent Automotive Industry Standards Committee (AISC) vide order No. RT-11028/11/97-MVL dated September 15, 1997. The standards prepared by AISC will be approved by the permanent CMVR Technical Standing Committee (CMVR-TSC). After approval, the Automotive Research Association of India, (ARAI), Pune, being the Secretariat of the AIS Committee, will publish this standard. For better dissemination of this information ARAI may publish this document on their Website.

Based on the discussion in the 66th meeting of AISC held on 14th July, 2023, Committee agreed to formulate an Automotive Industry Standard (AIS) for approval of vehicles equipped with Cyber Security and Management Systems (CSMS) as defined in this Standard. The purpose of this Standard is to establish uniform provisions for CSMS fitted to motor vehicles of categories M and N. It also applies to category T if fitted with at least one Electronic Control Unit (ECU) and vehicles of Categories L7 if equipped with automated driving functionalities from level 3 onwards.

The Standard cannot include all the security and threats, since the list is quite exhaustive, actual conditions and threats in the real world should not result in failure of the system and encourage the driver to opt out from such technology. While preparation of this standard considerable assistance is derived from UNR 155, date of entry into force 22 January 2021.

The AISC panel and the Automotive Industry Standards Committee (AISC) responsible for preparation of this standard are given in Annexure-F and Annexure-G respectively.

Cyber Security Management System (CSMS)

	Cyber Security and Management System (CSMS)
1.0	**SCOPE**
1.1	This Standard applies to vehicles of Categories M and N, with regard to cyber security. This Standard also applies to vehicles of Category T if fitted with at least one electronic control unit.
1.2	This Standard also applies to vehicles of Categories L7 if equipped with automated driving functionalities from level 3 onwards*.
1.3	This Standard is without prejudice to other standards, regional or national legislations governing the access by authorized parties to the vehicle, its data, functions and resources, and conditions of such access. It is also without prejudice to the application of national and regional legislation on privacy and the protection of natural persons with regard to the processing of their personal data.
1.4	This Standard is without prejudice to other standards national or regional legislation governing the development and installation/system integration of replacement parts and components, physical and digital, with regards to cybersecurity.
	* The levels of vehicle automation shall be as defined in SAE J-3016, as amended from time to time.
2.0	**DEFINITIONS**
	For the purposes of this standard the following definitions shall apply.
2.1	"Vehicle type" means vehicles which do not differ in at least the following essential respects:
	(a) The manufacturer's designation of the vehicle type;
	(b) Essential aspects of the electric/electronic architecture and external interfaces with respect to cyber security.
2.2	"Cyber security" means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components.
2.3	"Cyber Security Management System (CSMS)" means a systematic risk-based approach defining organizational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyberattacks.
2.4	"System" means a set of components and/or sub-systems that implements a function or functions.
2.5	"Development phase" means the period before a vehicle type is type approved.
2.6	"Production phase" refers to the duration of production of a vehicle type.
2.7	"Post-production phase" refers to the period in which a vehicle type is no longer produced until the end-of-life of all vehicles under the vehicle type. Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced. The phase ends when there are no longer any operational vehicles of a specific vehicle type.

2.8	"Mitigation" means a measure that is reducing risk.
2.9	"Risk" means the potential that a given threat will exploit vulnerabilities of a vehicle and thereby cause harm to the organization or to an individual.
2.10	"Risk Assessment" means the overall process of finding, recognizing and describing risks (risk identification), to comprehend the nature of risk and to determine the level of risk (risk analysis), and of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable (risk evaluation).
2.11	"Risk Management" means coordinated activities to direct and control an organization with regard to risk.
2.12	"Threat" means a potential cause of an unwanted incident, which may result in harm to a system, organization or individual.
2.13	"Vulnerability" means a weakness of an asset or mitigation that can be exploited by one or more threats.
3.0	**APPLICATION FOR APPROVAL**
3.1	The application for approval of a vehicle type with regard to cyber security shall be submitted by the vehicle manufacturer or by their duly accredited representative
3.2	It shall be accompanied by the undermentioned documents, and by the following particulars:
3.2.1	A description of the vehicle type with regard to the items specified in Annex A to this Standard.
3.2.2	In cases where information is shown to be covered by intellectual property rights or to constitute specific know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall make available sufficient information to enable the checks referred to in this Standard to be made properly. Such information shall be treated on a confidential basis.
3.2.3	The Certificate of Compliance for CSMS according to clause 6 of this Standard.
3.3	Documentation shall be made available in two parts:
	(a) The formal documentation package for the approval, containing the material specified in Annex A which shall be supplied to the Test Agency at the time of submission of the type approval application. This documentation package shall be used by the Test Agency as the basic reference for the approval process. The Test Agency shall ensure that this documentation package remains available for at least 10 years counted from the time when production of the vehicle type is definitively discontinued.
	(b) Additional material relevant to the requirements of this standard may be retained by the manufacturer, but made open for inspection at the time of type approval. The manufacturer shall ensure that any material made open for inspection at the time of type approval remains available for at least a period of 10 years counted from the time when production of the vehicle type is definitively discontinued.

4.0	**[RESERVED]**
5.0	**APPROVAL**
5.1	Test Agency shall grant, as appropriate, type approval with regard to cyber security, only to such vehicle types that satisfy the requirements of this Standard.
5.1.1	The Test Agency shall verify by means of document checks that the vehicle manufacturer has taken the necessary measures relevant for the vehicle type to:
	(a) Collect and verify the information required under this Standard through the supply chain so as to demonstrate that supplier-related risks are identified and are managed;
	(b) Document risks assessment (conducted during development phase or retrospectively), test results and mitigations applied to the vehicle type, including design information supporting the risk assessment;
	(c) Implement appropriate cyber security measures in the design of the vehicle type;
	(d) Detect and respond to possible cyber security attacks;
	(e) Log data to support the detection of cyber-attacks and provide data forensic capability to enable analysis of attempted or successful cyberattacks.
5.1.2	The Test Agency shall verify by testing of a vehicle of the vehicle type that the vehicle manufacturer has implemented the cyber security measures they have documented. Tests shall be performed by the Test Agency itself or in collaboration with the vehicle manufacturer by sampling. Sampling shall be focused but not limited to risks that are assessed as high during the risk assessment
5.1.3	The Test Agency shall refuse to grant the type approval with regard to cyber security where the vehicle manufacturer has not fulfilled one or more of the requirements referred to in clause 7.3., notably:
	(a) The vehicle manufacturer did not perform the exhaustive risk assessment referred to in clause 7.3.3.; including where the manufacturer did not consider all the risks related to threats referred to in Annex D, Part A;
	(b) The vehicle manufacturer did not protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment or proportionate mitigations were not implemented as required by clause 7.
	(c) The vehicle manufacturer did not put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data
	(d) The vehicle manufacturer did not perform, prior to the approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.
5.1.4	The assessing Test Agency shall also refuse to grant the type approval with regard to cyber security where the Test Agency has not received sufficient information from the vehicle manufacturer to assess the cyber security of the vehicle type.

5.2	Notice of approval or of extension or refusal of approval of a vehicle type pursuant to this Standard shall be communicated to vehicle manufacturer, by means of a form conforming to the model in Annex B to this Standard.
5.3	Test Agency shall not grant any type approval without verifying that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the cyber security aspects as covered by this Standard.
5.3.1	The Test Agency shall ensure, that they have:
	(a) Competent personnel with appropriate cyber security skills and specific automotive risk assessments knowledge[1]
	1. E.g. ISO 26262-2018, ISO/PAS 21448-2019, ISO/SAE 21434-2021
	(b) Implemented procedures for the uniform evaluation according to this Standard.
5.4	For the purpose of clause 7.2. of this Standard, the manufacturer shall ensure that the cyber security aspects covered by this Standard are implemented.
6.0	**CERTIFICATE OF COMPLIANCE FOR CYBER SECURITY MANAGEMENT SYSTEM (CSMS)**
6.1	Test agencies shall carry out the assessment of the manufacturer and to issue a Certificate of Compliance for CSMS.
6.2	An application for a Certificate of Compliance for CSMS shall be submitted by the vehicle manufacturer or by their duly accredited representative.
6.3	It shall be accompanied by the undermentioned documents in triplicate, and by the following particular:
6.3.1	Documents describing the CSMS.
6.3.2	A signed declaration using the model as defined in Appendix 1 to Annex A.
6.4	In the context of the assessment, the manufacturer shall declare using the model as defined in Appendix 1 to Annex A and demonstrate to the satisfaction of the Test agency that they have the necessary processes to comply with all the requirements for cyber security according to this standard.
6.5	When this assessment has been satisfactorily completed and in receipt of a signed declaration from the manufacturer according to the model as defined in Appendix 1 to Annex A, a certificate named Certificate of Compliance for CSMS as described in Annex D to this Standard (hereinafter the Certificate of Compliance for CSMS) shall be granted to the manufacturer.
6.6	The test agency shall use the model set out in Annex D to this Standard for the Certificate of Compliance for CSMS.
6.7	The Certificate of Compliance for CSMS shall remain valid for a maximum of three years from the date of deliverance of the certificate unless it is withdrawn.
6.8	The test agency which has granted the Certificate of Compliance for CSMS may at any time verify that the requirements for it continue to be met. The test agency shall withdraw the Certificate of Compliance for CSMS if the requirements laid down in this Standard are no longer met.

6.9	The manufacturer shall inform the test agency of any change that will affect the relevance of the Certificate of Compliance for CSMS. After consultation with the manufacturer, the test agency shall decide whether new checks are necessary.
6.10	In due time, permitting the test agency to complete its assessment before the end of the period of validity of the Certificate of Compliance for CSMS, the manufacturer shall apply for a new or for the extension of the existing Certificate of Compliance for CSMS. The test agency shall, subject to a positive assessment, issue a new Certificate of Compliance for CSMS or extend its validity for a further period of three years. The test agency shall verify that the CSMS continue to comply with the requirements of this Standard. The test agency shall issue a new certificate in cases where changes have been brought to the attention of the test agency and the changes have been positively reassessed.
6.11	The expiry or withdrawal of the manufacturer's Certificate of Compliance for CSMS shall be considered, with regard to the vehicle types to which the CSMS concerned was relevant, as modification of approval, as referred to in clause 8, which may include the withdrawal of the approval if the conditions for granting the approval are not met anymore.
7.0	**SPECIFICATIONS**
7.1	General specifications
7.1.1	The requirements of this Standard shall not restrict provisions or requirements of other AIS Standards.
7.2	Requirements for the CSMS
7.2.1	For the assessment the test agency shall verify that the vehicle manufacturer has a CSMS in place and shall verify its compliance with this Standard.
7.2.2	The CSMS shall cover the following aspects:
7.2.2.1	The vehicle manufacturer shall demonstrate to an test agency that their CSMS applies to the following phases:
	(a) Development phase;
	(b) Production phase;
	(c) Post-production phase.
7.2.2.2	The vehicle manufacturer shall demonstrate that the processes used within their CSMS ensure security is adequately considered, including risks and mitigations listed in Annex D. This shall include:
	(a) The processes used within the manufacturer's organization to manage cyber security;
	(b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex D, Part A, and other relevant threats shall be considered;
	(c) The processes used for the assessment, categorization and treatment of the risks identified;

	(d) The processes in place to verify that the risks identified are appropriately managed;
	(e) The processes used for testing the cyber security of a vehicle type;
	(f) The processes used for ensuring that the risk assessment is kept current;
	(g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.
	(h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks
7.2.2.3	The vehicle manufacturer shall demonstrate that the processes used within their CSMS will ensure that, based on categorization referred to in clause 7.2.2.2 (c) and 7.2.2.2 (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.
7.2.2.4	The vehicle manufacturer shall demonstrate that the processes used within their CSMS will ensure that the monitoring referred to in clause 7.2.2.2 (g) shall be continual. This shall:
	(a) Include vehicles after first registration in the monitoring;
	(b) Include the capability to analyze and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect clause 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.
7.2.2.5	The vehicle manufacturer shall be required to demonstrate how their CSMS will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of clause 7.2.2.2.
7.3	Requirements for vehicle types
7.3.1	The manufacturer shall have a valid Certificate of Compliance for the CSMS relevant to the vehicle type being approved.
	However, for new model type approvals prior to All Model implementation date (after new model implementation date), if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned.
7.3.2	The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks
7.3.3	The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all

	the threats referred to in Annex D, Part A, as well as any other relevant risk.
7.3.4	The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex D, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex D, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.
	In particular, for new model type approvals prior to All Model implementation date (after new model implementation date), the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex D, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority.
7.3.5	The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.
7.3.6	The vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.
7.3.7	The vehicle manufacturer shall implement measures for the vehicle type to:
	(a) Detect and prevent cyber-attacks against vehicles of the vehicle type;
	(b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;
	(c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.
7.3.8	Cryptographic modules used for the purpose of this Standard shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use
7.4	Reporting provisions
7.4.1	The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the test agency the outcome of their monitoring activities, as defined in clause 7.2.2.2. (g)), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the test agency that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken
7.4.2	The test agency shall verify the provided information and, if necessary, require the vehicle manufacturer to remedy any detected ineffectiveness.
	If the reporting or response is not sufficient the test agency may decide to withdraw the CSMS in compliance with clause 6.8.
8.0	**MODIFICATION AND EXTENSION OF THE VEHICLE TYPE**

8.1	Every modification of the vehicle type which affects its technical performance with respect to cybersecurity and/or documentation required in this standard shall be notified to the test agency which approved the vehicle type. The test agency may then either:
8.1.1	Consider that the modifications made still comply with the requirements and documentation of existing type approval; or
8.1.2	Proceed to necessary complementary assessment pursuant to clause 6, and require, where relevant, a further test report by conducting the tests.
8.1.3	Confirmation or extension or refusal of approval, specifying the alterations, shall be communicated by means of a communication form conforming to the model in Annex B to this Standard. The test agency issuing the extension of approval shall assign a certificate number for such an extension and issue it to vehicle manufacturer by means of a communication form conforming to the model in Annex B to this Standard.

Annex A – INFORMATION DOCUMENT	
A-1.0	Make (trade name of manufacturer): .....
A-2.0	Type and general commercial description(s):.....
A-3.0	Means of identification of type, if marked on the vehicle: .....
A-4.0	Location of that marking: .....
A-5.0	Category(ies) of vehicle:.....
A-6.0	Name and address of manufacturer/ manufacturer's representative:.....
A-7.0	Name(s) and Address(es) of assembly plant(s): .....
A-8.0	Photograph(s) and/or drawing(s) of a representative vehicle: .....
A-9.0	Cyber Security
A-9.1	General construction characteristics of the vehicle type, including:
	(a) The vehicle systems which are relevant to the cyber security of the vehicle type;
	(b) The components of those systems that are relevant to cyber security;
	(c) The interactions of those systems with other systems within the vehicle type and external interfaces.
A-9.2	Schematic representation of the vehicle type
A-9.3	The number of the Certificate of Compliance for CSMS: .....
A-9.4	Documents for the vehicle type to be approved describing the outcome of its risk assessment and the identified risks: .....
A-9.5	Documents for the vehicle type to be approved describing the mitigations that have been implemented on the systems listed, or to the vehicle type, and how they address the stated risks: .....
A-9.6	Documents for the vehicle type to be approved describing protection of dedicated environments for aftermarket software, services, applications or data:.....
A-9.7	Documents for the vehicle type to be approved describing what tests have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests:.....
A-9.8	Description of the consideration of the supply chain with respect to cyber security:...

ANNEX A –Appendix 1 **Model of Manufacturer's Declaration of Compliance for CSMS**
Manufacturer's declaration of compliance with the requirements for the Cyber Security Management System
Manufacturer Name: .....
Manufacturer Address:.....
……..(Manufacturer Name) attests that the necessary processes to comply with the requirements for the Cyber Security Management System laid down in clause 7.2 of this standard are installed and will be maintained.
Done at: …… (place)
Date: .....
Name of the signatory: .....
Function of the signatory: .....
..... (Stamp and signature of the manufacturer's representative)

ANNEX B - **COMMUNICATION**
Concerning:[7] Approval granted Approval extended Approval withdrawn with effect from dd/mm/yyyy Approval refused Production definitively discontinued of a vehicle type, pursuant to this Standard
Approval No.: .....
Extension No.: .....
Reason for extension: .....
1. Make (trade name of manufacturer): .....
2. Type and general commercial description(s) .....
3. Means of identification of type, if marked on the vehicle: .....
3.1. Location of that marking: .....
4. Category(ies) of vehicle:.....
5. Name and address of manufacturer / manufacturer's representative: .....
6. Name(s) and Address(es) of the production plant(s) .....
7. Number of the certificate of compliance for cyber security management system: .....
8. Test agency responsible for carrying out the tests: .....
9. Date of test report: .....

10. Number of test report: .....
11. Remarks: (if any). .....
12. Place:.....
13. Date: .....
14. Signature: .....
15. The index to the information package lodged with the test agency, which may be obtained on request is attached:
[7] Strike out what does not apply.

ANNEX C **MODEL OF CERTIFICATE OF COMPLIANCE FOR CSMS**
Certificate of compliance for cyber security management system With **AIS. No. [This Standard]** Certificate Number [Reference number] [……. Test Agency] Certifies that
Manufacturer: .....
Address of the manufacturer: .....
complies with the provisions of clause 7.2 of this Standard
Checks have been performed on:.....
by (name and address of the Test Agency): .....
Number of report:.....
The certificate is valid until […..Date] Done at [……Place] On […….Date] […….Signature]
Attachments: description of the Cyber Security Management System by the manufacturer

ANNEX D

LIST OF THREATS AND CORRESPONDING MITIGATIONS

E-1.0	This annex consists of three parts. Part A of this annex describes the baseline for threats, vulnerabilities and attack methods. Part B of this annex describes mitigations to the threats which are intended for vehicle types. Part C describes mitigations to the threats which are intended for areas outside of vehicles, e.g. on IT back ends.
E-2.0	Part A, Part B, and Part C shall be considered for risk assessment and mitigations to be implemented by vehicle manufacturers.
E-3.0	The high-level vulnerability and its corresponding examples have been indexed in Part A. The same indexing has been referenced in the tables in Parts B and C to link each of the attack/vulnerability with a list of corresponding mitigation measures
E-4.0	The threat analysis shall also consider possible attack impacts. These may help ascertain the severity of a risk and identify additional risks. Possible attack impacts may include:
	(a) Safe operation of vehicle affected;
	(b) Vehicle functions stop working;
	(c) Software modified, performance altered;
	(d) Software altered but no operational effects;
	(e) Data integrity breach;
	(f) Data confidentiality breach;
	(g) Loss of data availability;
	(h) Other, including criminality.

Part A. Vulnerability or attack method related to the threats

1. High level descriptions of threats and relating vulnerability or attack method are listed in Table A1.

Table A1
List of vulnerability or attack method related to the threats

High level and sub-level descriptions of vulnerability/ threat			Example of vulnerability or attack method	
4.3.1 Threats regarding back-end servers related to vehicles in the field	1.	Back-end servers used as a means to attack a vehicle or extract data	1.1	Abuse of privileges by staff (insider attack)
			1.2	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			1.3	Unauthorized physical access to the server (conducted by for example USB sticks or other media connecting to the server)
	2.	Services from back-end server being disrupted,	2.1	Attack on back-end server stops it functioning, for example it prevents it

		affecting the operation of a vehicle		from interacting with vehicles and providing services they rely on
	3.	Vehicle related data held on back-end servers being lost or compromised ("data breach")	3.1	Abuse of privileges by staff (insider attack)
			3.2	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers
			3.3	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			3.4	Unauthorized physical access to the server (conducted for example by USB sticks or other media connecting to the server)
			3.5	Information breach by unintended sharing of data (e.g. admin errors)
4.3.2 Threats to vehicles regarding their communication channels	4.	Spoofing of messages or data received by the vehicle	4.1	Spoofing of messages by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)
			4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)
	5.	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	5.1	Communications channels permit code injection, for example tampered software binary might be injected into the communication stream
			5.2	Communications channels permit manipulate of vehicle held data/code
			5.3	Communications channels permit overwrite of vehicle held data/code
			5.4	Communications channels permit erasure of vehicle held data/code
			5.5	Communications channels permit introduction of data/code to the vehicle (write data code)
	6.	Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks	6.1	Accepting information from an unreliable or untrusted source
			6.2	Man in the middle attack/ session hijacking
			6.3	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway

	7.	Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	7.1	Interception of information / interfering radiations / monitoring communications
			7.2	Gaining unauthorized access to files or data
	8.	Denial of service attacks via communication channels to disrupt vehicle functions	8.1	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner
			8.2	Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles
	9.	An unprivileged user is able to gain privileged access to vehicle systems	9.1	An unprivileged user is able to gain privileged access, for example root access
	10.	Viruses embedded in communication media are able to infect vehicle systems	10.1	Virus embedded in communication media infects vehicle systems
	11.	Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	11.1	Malicious internal (e.g. CAN) messages
			11.2	Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)
			11.3	Malicious diagnostic messages
			11.4	Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)
4.3.3. Threats to vehicles regarding their update procedures	12.	Misuse or compromise of update procedures	12.1	Compromise of over the air software update procedures. This includes fabricating the system update program or firmware
			12.2	Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware
			12.3	The software is manipulated before the update process (and is therefore corrupted), although the update process is intact
			12.4	Compromise of cryptographic keys of the software provider to allow invalid update

	13.	It is possible to deny legitimate updates	13.1	Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific feature
4.3.4 Threats to vehicles regarding unintended human actions facilitating a cyber attack	15.	Legitimate actors are able to take actions that would unwittingly facilitate a cyberattack	15.1	Innocent victim (e.g. owner, operator or maintenance engineer) being tricked into taking an action to unintentionally load malware or enable an attack
			15.2	Defined security procedures are not followed
4.3.5 Threats to vehicles regarding their external connectivity and connections	16.	Manipulation of the connectivity of vehicle functions enables a cyberattack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications	16.1	Manipulation of functions designed to remotely operate systems, such as remote key, immobilizer, and charging pile
			16.2	Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)
			16.3	Interference with short range wireless systems or sensors
	17.	Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems	17.1	Corrupted applications, or those with poor software security, used as a method to attack vehicle systems
	18.	Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems	18.1	External interfaces such as USB or other ports used as a point of attack, for example through code injection
			18.2	Media infected with a virus connected to a vehicle system
			18.3	Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)
4.3.6 Threats to vehicle data/code	19.	Extraction of vehicle data/code	19.1	Extraction of copyright or proprietary software from vehicle systems (product piracy)
			19.2	Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc
			19.3	Extraction of cryptographic keys
	20.	Manipulation of vehicle data/code	20.1	Illegal/unauthorized changes to vehicle's electronic ID
			20.2	Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend

			20.3	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
			20.4	Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc)
			20.5	Unauthorized changes to system diagnostic data
	21.	Erasure of data/code	21.1	Unauthorized deletion/manipulation of system event logs
	22.	Introduction of malware	22.1	Introduce malicious software or malicious software activity
	23.	Introduction of new software or overwrite existing software	23.1	Fabrication of software of the vehicle control system or information system
	24.	Disruption of systems or operations	24.1	Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging
	25.	Manipulation of vehicle parameters	25.1	Unauthorized access of falsify the configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc.
			25.2	2 Unauthorized access of falsify the charging parameters, such as charging voltage, charging power, battery temperature, etc.
4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	26.	Cryptographic technologies can be compromised or are insufficiently applied	26.1	Combination of short encryption keys and long period of validity enables attacker to break encryption
			26.2	Insufficient use of cryptographic algorithms to protect sensitive systems
			26.3	Using already or soon to be deprecated cryptographic algorithms
	27.	Parts or supplies could be compromised to permit vehicles to be attacked	27.1	Hardware or software, engineered to enable an attack or fails to meet design criteria to stop an attack
	28.	Software or hardware development permits vulnerabilities	28.1	Software bugs. The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present
			28.2	Using remainders from development (e.g. debug ports, JTAG ports,

				microprocessors, development certificates, developer passwords, …) can permit access to ECUs or permit attackers to gain higher privileges
	29.	Network design introduces vulnerabilities	29.1	Superfluous internet ports left open, providing access to network systems
			29.2	Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages
	31.	Unintended transfer of data can occur	31.1	Information breach. Personal data may be leaked when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)
	32.	Physical manipulation of systems can enable an attack	32.1	Manipulation of electronic hardware, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack Replacement of authorized electronic hardware (e.g., sensors) with unauthorized electronic hardware Manipulation of the information collected by a sensor (for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox)

Part B. Mitigations to the threats intended for vehicles

1. Mitigations for "Vehicle communication channels"

   Mitigations to the threats which are related to "Vehicle communication channels" are listed in Table B1

Table B1
Mitigation to the threats which are related to "Vehicle communication channels"

Table A1 reference	Threats to "Vehicle communication channels"	Ref	Mitigation
4.1	Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation	M10	The vehicle shall verify the authenticity and integrity of messages it receives
4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)
5.1	Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream	M10	The vehicle shall verify the authenticity and integrity of messages it receives
		M6	Systems shall implement security by design to minimize risks
5.2	Communication channels permit	M7	Access control techniques and designs

	manipulation of vehicle held data/code		shall be applied to protect system data/code
5.3	Communication channels permit overwrite of vehicle held data/code		
5.4	Communication channels permit erasure of vehicle held data/code		
21.1			
5.5	Communication channels permit introduction of data/code to vehicle systems (write data code)		
6.1	Accepting information from an unreliable or untrusted source	M10	The vehicle shall verify the authenticity and integrity of messages it receives
6.2	Man in the middle attack / session hijacking	M10	The vehicle shall verify the authenticity and integrity of messages it receives
6.3	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway		
7.1	Interception of information / interfering radiations / monitoring communications	M12	Confidential data transmitted to or from the vehicle shall be protected
7.2	Gaining unauthorized access to files or data	M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example of Security Controls can be found in OWASP
8.1	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	M13	Measures to detect and recover from a denial of service attack shall be employed
8.2	Black hole attack, disruption of communication between vehicles by blocking the transfer of messages to other vehicles	M13	Measures to detect and recover from a denial of service attack shall be employed
9.1	An unprivileged user is able to gain privileged access, for example root access	M9	Measures to prevent and detect unauthorized access shall be employed
10.1	Virus embedded in communication media infects vehicle systems	M14	Measures to protect systems against embedded viruses/malware should be considered
11.1	Malicious internal (e.g. CAN) messages	M15	Measures to detect malicious internal messages or activity should be considered
11.2	Malicious V2X messages, e.g. infrastructure to vehicle or vehicle to vehicle messages (e.g. CAM, DENM)	M10	The vehicle shall verify the authenticity and integrity of messages it receives
11.3	Malicious diagnostic messages		
11.4	Malicious proprietary messages (e.g.		

	those normally sent from OEM or component/system/function supplier)		
2. Mitigations for "Update process"			
Mitigations to the threats which are related to "Update process" are listed in Table B2.			
Table B2 **Mitigations to the threats which are related to "Update process"**			
Table A1 reference	Threats to "Update process"	Ref	Mitigation
12.1	Compromise of over the air software update procedures. This includes fabricating the system update program or firmware	M16	Secure software update procedures shall be employed
12.2	Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware		
12.3	The software is manipulated before the update process (and is therefore corrupted), although the update process is intact		
12.4	Compromise of cryptographic keys of the software provider to allow invalid update	M11	Security controls shall be implemented for storing cryptographic keys
13.1	Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features	M3	Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP
3. Mitigations for "Unintended human actions facilitating a cyberattack"			
Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack" are listed in Table B3.			
Table B3 **Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack"**			
Table A1 reference	Threats relating to "Unintended human actions"	Ref	Mitigation
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
15.2	Defined security procedures are not followed	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions
4. Mitigations for "External connectivity and connections"			
Mitigations to the threats which are related to "external connectivity and connections" are listed in Table B4.			

Table B4 Mitigation to the threats which are related to "external connectivity and connections"			
Table A1 reference	Threats to "External connectivity and connections"	Ref	Mitigation
16.1	Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile	M20	Security controls shall be applied to systems that have remote access
16.2	Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)		
16.3	Interference with short range wireless systems or sensors		
17.1	Corrupted applications, or those with poor software security, used as a method to attack vehicle systems	M21	Software shall be security assessed, authenticated and integrity protected. Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle
18.1	External interfaces such as USB or other ports used as a point of attack, for example through code injection	M22	Security controls shall be applied to external interfaces
18.2	Media infected with viruses connected to the vehicle		
18.3	Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	M22	Security controls shall be applied to external interfaces
5. Mitigations for "Potential targets of, or motivations for, an attack "			
Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack " are listed in Table B5			

Table B5 Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack"			
Table A1 reference	Threats to "Potential targets of, or motivations for, an attack"	Ref	Mitigation
19.1	Extraction of copyright or proprietary software from vehicle systems (product piracy / stolen software)	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
19.2	Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.	M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Examples of Security Controls can be found in OWASP
19.3	Extraction of cryptographic keys	M11	Security controls shall be implemented for storing cryptographic keys e.g. Security Modules

20.1	Illegal/unauthorised changes to vehicle's electronic ID	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
20.2	Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend		
20.3	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information
20.4	Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.)		
20.5	Unauthorised changes to system diagnostic data		
21.1	Unauthorized deletion/manipulation of system event logs	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
22.2	Introduce malicious software or malicious software activity	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
23.1	Fabrication of software of the vehicle control system or information system		
24.1	Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging	M13	Measures to detect and recover from a denial of service attack shall be employed
25.1	Unauthorized access to falsify configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
25.2	Unauthorized access to falsify charging parameters, such as charging voltage, charging power, battery temperature, etc.		

6. Mitigations for "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened" are listed in Table B6.

Table B6
Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Table A1 reference	Threats to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"	Ref	Mitigation
26.1	Combination of short encryption keys and long period of validity enables attacker to break encryption	M23	Cybersecurity best practices for software and hardware development shall be followed

26.2	Insufficient use of cryptographic algorithms to protect sensitive systems		
26.3	Using deprecated cryptographic algorithms		
27.1	Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack	M23	Cybersecurity best practices for software and hardware development shall be followed
28.1	The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present	M23	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity testing with adequate coverage
28.2	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit an attacker to access ECUs or gain higher privileges		
29.1	Superfluous internet ports left open, providing access to network systems		
29.2	Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages	M23	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity best practices for system design and system integration shall be followed
7. Mitigations for "Data loss / data breach from vehicle"			
Mitigations to the threats which are related to "Data loss / data breach from vehicle" are listed in Table B7.			

Table B7
Mitigations to the threats which are related to "Data loss / data breach from vehicle"

Table A1 reference	Threats of "Data loss / data breach from vehicle"	Ref	Mitigation
31.1	Information breach. Personal data may be breached when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)	M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data.
8. Mitigations for "Physical manipulation of systems to enable an attack"			
Mitigation to the threats which are related to "Physical manipulation of systems to enable an attack" are listed in Table B8.			

Table B8
Mitigations to the threats which are related to "Physical manipulation of systems to enable an attack"

Table A1 reference	Threats to "Physical manipulation of systems to enable an attack"	Ref	Mitigation

32.1	Manipulation of OEM hardware, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack	M9	Measures to prevent and detect unauthorized access shall be employed

Part C. Mitigations to the threats outside of vehicles

1. Mitigations for "Back-end servers"

Mitigations to the threats which are related to "Back-end servers" are listed in Table C1.

Table C1
Mitigations to the threats which are related to "Back-end servers"

Table A1 reference	Threats to "Back-end servers"	Ref	Mitigation
1.1 & 3.1	Abuse of privileges by staff (insider attack)	M1	Security Controls are applied to back-end systems to minimise the risk of insider attack
1.2 & 3.3	Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	M2	Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP
1.3 & 3.4	Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)	M8	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data
2.1	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on	M3	Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP
3.2	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers	M4	Security Controls are applied to minimise risks associated with cloud computing. Example Security Controls can be found in OWASP and NCSC cloud computing guidance
3.5	Information breach by unintended sharing of data (e.g. admin errors, storing data in servers in garages)	M5	Security Controls are applied to back-end systems to prevent data breaches. Example Security Controls can be found in OWASP

2. Mitigations for "Unintended human actions"

Mitigations to the threats which are related to "Unintended human actions" are listed in Table C2.

Table C2
Mitigations to the threats which are related to "Unintended human actions"

Table A1 reference	Threats relating to "Unintended human actions"	Ref	Mitigation
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
15.2	Defined security procedures are not	M19	Organizations shall ensure security

	followed		procedures are defined and followed including logging of actions and access related to the management of the security functions
3. Mitigations for "Physical loss of data"			
Mitigations to the threats which are related to "Physical loss of data" are listed in Table C3.			
Table C3 Mitigations to the threats which are related to "Physical loss of data loss"			
Table A1 reference	Threats of "Physical loss of data"	Ref	Mitigation
30.1	Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft	M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. Example Security Controls can be found in ISO/SC27/WG5
30.2	Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues		
30.3	The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example)		

ANNEXURE E

(See Introduction)

COMPOSITION OF AISC PANEL ON APPROVAL OF VEHICLES WITH REGARDS TO CYBER SECURITY AND MANAGEMENT SYSTEMS (CSMS)

Panel Convener	**Representing**
Mr. Rejin Sathianesan	Robert Bosch Engineering and Business Solutions Private Limited (ACMA)
Members	
Mr. A. A. Badusha	The Automotive Research Association of India
Mr. Manoj M. Desai	The Automotive Research Association of India
Mr. Girish S. Tanawade	The Automotive Research Association of India
Mr. U. Sreekumar	The Automotive Research Association of India
Mr. Kamalesh Patil	The Automotive Research Association of India
Ms. Sneha R. Pawar	The Automotive Research Association of India
Mr. Pratik R. Nayak	The Automotive Research Association of India
Mr. Rohit Yadav	International Centre for Automotive Technology
Dr. Madhusudan Joshi	International Centre for Automotive Technology
Ms. Vijayanta Ahuja	International Centre for Automotive Technology
Mr. Amit Kumar	The Society of Indian Automobile Manufacturers (SIAM)
Mr. Ved Prakash Gautam	SIAM (Ashok Leyland Ltd.)
Mr. S. Parthiban	SIAM (Ashok Leyland Ltd.)
Mr. Hari Sai Krishna M	SIAM (Hyundai Motors India Engineering)
Mr. Abhijit Dhotre	SIAM (Mahindra & Mahindra Ltd.)
Mr. Priyanto Deb	SIAM (Mahindra & Mahindra Ltd.)
Ms. Pushpanjali Pathak	SIAM (Mahindra & Mahindra Ltd.)
Mr. Alok Jaitley	SIAM (Maruti Suzuki India Ltd)
Mr. Gururaj Ravi	SIAM (Maruti Suzuki India Ltd)

Mr. Das Subham Kant	SIAM (Maruti Suzuki India Ltd)
Mr. Sumit Kumar	SIAM (Maruti Suzuki India Ltd)
Mr. Arun Kumar	SIAM (Maruti Suzuki India Ltd)
Mr. Vijay DinakaranN	SIAM (Renault Nissan India Pvt. Ltd.)
Mr. Rajendra Khile	SIAM (Renault Nissan India Pvt. Ltd.)
Mr. Milind Jagtap	SIAM (Skoda Auto Volkswagen India Private Ltd.)
Ms. Aditi Deshpande	SIAM (Skoda Auto Volkswagen India Private Ltd.)
Mr. Uday Salunkhe	SIAM (Tata Motors Ltd.)
Mr. Manoj Shukla	SIAM (Tata Motors Ltd.)
Mr. V. Vaisakh	SIAM (Tata Motors Ltd.)
Mr. Uday Harite	The Automotive Component Manufacturers Association of India (ACMA)
Mr. Noel Peters	ACMA (Denso International India Pvt. Ltd.)
Mr. Pawar Khushwant	ACMA (ETAS)
Mr. Saurabh Pathak	ACMA (Minda Group)
Mr. Ashutosh Telang	ACMA (Minda Group)
Ms. Devayani Jayant Kulkarni	ACMA (Robert Bosch Engineering and Business Solutions Private Limited)
Mr. Avinash Sathyanarayana Jayam	ACMA (Robert Bosch Engineering and Business Solutions Private Limited)

* At the time of approval of this Automotive Industry Standard (AIS)

ANNEXURE F
(See Introduction)

COMMITTEE COMPOSITION *
Automotive Industry Standards Committee

Chairperson	
Dr. Reji Mathai	Director, The Automotive Research Association of India, Pune
Members	**Representing**
Representative from	Ministry of Road Transport and Highways
Representative from	Ministry of Heavy Industries
Representative from	Office of the Development Commissioner, MSME, Ministry of Micro, Small and Medium Enterprises, New Delhi
Shri Shrikant R. Marathe	Former Chairman, AISC
Shri P. V. Srikanth	Bureau of Indian Standards
Director	Central Institute of Road Transport
Director	Global Automotive Research Centre
Director	International Centre for Automotive Technology, Manesar
Director	Indian Institute of Petroleum, Dehra Dun
Director	Vehicles Research and Development Establishment
Director	Indian Rubber Manufacturers Research Association
Representatives from	Society of Indian Automobile Manufacturers
Representative from	Tractor Manufacturers Association
Representative from	Automotive Components Manufacturers Association of India
Representative from	Indian Construction Equipment Manufactures' Association (ICEMA)
Member Secretary	
Shri Vikram Tandon	The Automotive Research Association of India, Pune

* At the time of approval of this Automotive Industry Standard (AIS)