Date of hosting on website: 4th December 2018
Last date of comments: 19th December 2018

CHECK LIST FOR PREPARING AMENDMENT TO AUTOMOTIVE INDUSTRY STANDARD(AIS)

Amd. No 02 to AIS-140 : Intelligent Transportation System (ITS)- Requirements for Public Transport Vehicle Operation

SR. NO.	PARTICULARS	REMARKS
1.0	Is the amendment related to : i) Changes in technical requirements; ii) Corrigendum iii) Any other (Pl. specify)	Changes in Technical Requirement. 1. Revision in IRNSS implementation date 2. Details of Backend server added 3. CoP Requirements for Devices/Server added.
2.0	Indicate details of base reference standard (amendments).	Nil
3.0	Add an explanatory note indicating deviations from the above base referred standard (amendments) in Sr. 2.	NA
4.0	If amendment is for provisions in technical requirements :	Yes
4.1	a) Does amendment call for re-type approval of component / vehicle, which is already type approved? b) Is amendment applicable to fresh type approval of component / vehicle c) Do components / vehicles manufacturers / Test agencies require lead time to meet requirements of amendment?	No No No
4.2	If amendment is related to corrigendum : a) Whether changes are required in previous approvals	NA
5.0	What are the test equipments for establishing compliance to amendment?	NA
6.0	If possible, identify such facilities available in India.	NA
7.0	Are there any points on which special comments or information is to be invited from AISC/ CMVR-TSC If yes, are they identified?	No
8.0	Recommendation of date for implementation of amendment.	With Date of adoption in CMVR TSC

Explanatory note based on ECE/EEC Directive practices:

1. Amend.X = an amendment issued to the text of the AIS .
2. Rev.X = a Revision of the text comprising all previous text(s) of the AIS.
3. Corr.X = a Corrigendum consists of editorial corrections of errors in the issued texts.

Draft Amendment 2
To
AIS-140: Intelligent Transportation Systems (ITS) - Requirements for Public Transport Vehicle Operation

1.	**Page 5** Clause 3.1.1.1. a, Substitute the following text for the existing text: a. Device shall be capable for operating in L and/or S band and include support for NAVIC/IRNSS (Indian Regional Navigation Satellite System) for devices installed on vehicles on or after 1st April 2019. However VLT devices shall be compliant as per other GNSS constellation in the interim period.
2.	**Page 16/17** Clause 5.3, Substitute the following text for the existing text: The VLT system shall be mounted in a suitable location such a way that it is not easily accessible /exposed to passengers. This requirement shall not be applicable in case of combined systems VLT with HMI (Human Machine Interface) display in front of driver. ~~Test agency to verify this on vehicle level approval.~~ Emergency button(s) shall be fitted in such a way that every passenger including driver shall be able to access the Emergency button(s). Passenger Car shall have at least one emergency buttons on each passenger row easily accessible by each of the passenger. There shall also be one dedicated emergency button for the driver row. Passenger Transport bus shall have emergency buttons at locations easily visible & accessible to all the passengers such as every 2 meters on both the sides on passenger seating area. For seats reserved for ladies there shall be a dedicated panic button for each row. It shall be permissible to have a single emergency button for two successive ladies' rows on both sides of the vehicle provided each lady passenger in either rows are able to reach and operate the emergency button. **In case of passenger transport bus which has a glass window covered between two pillars having pitch 2m or more, the emergency buttons shall be provided on each pillar** **Commercial Vehicles shall have one dedicated emergency button for the driver row**. ~~Test agency to verify this on vehicle level approval.~~
3.	**Page No 31/40**

	Clause No 7.0 DEVICE TO BACKEND COMMUNICATION MECHANISM Add Below Text at the end of first paragraph The Communication from Device to backend should happen on a Secure channel over TCPIP protocol preferably on socket based connections where sessions are managed to send commands over the same connection to the device and are authenticated, identifiable, so as to prevent spoofing on IMEI/ Unique ID.
4.	**Page No 3/40** **Clause No 2.2.1, Replace the clause as below** **Device Approval**: Approval provided at Device level for compliance to this standard. These approved devices can be fitted / retro-fitted by manufacturer/ dealer/ permit holder/system integrator in any vehicle model provided it shall meet installation requirements as mentioned in Clause No. 5 of this standard. ~~For manufacturers seeking vehicle level approval with approved VLT with Emergency Buttons fitted shall only require installation approval as per the provisions of Clause 5 and Sub-Clause 6.1 of Clause 6.~~
5.	**Page No 16/40** Clause No 5.0 Replace as below **CONSTRUCTION AND INSTALLATION** (To be verified on component level ~~and target vehicle level approval~~)
6.	**Page 17/40** Clause No 6.1 :Delete this clause ~~6.1 Vehicle Level Functional Tests~~
7.	**Page 17/40** **Clause No. 6.1.1 : Delete this clause** ~~**6.1.1 AUTOMATIC VEHICLE LOCATION TRACKING AND EMERGENCY BUTTON**~~ ~~6.1.1.1 Vehicle OEM shall only provide/ installed devices approved under component level testing.~~ ~~6.1.1.2 System transmits PVT information to back office control center (2 different IPs) at user configurable frequency (5 seconds or less) via GSM/GPRS.~~ ~~6.1.1.3 .System to communicate to control center on the occurrence of the alerts captured in Communication Protocol Section 4.~~
8.	**Page 18/40** **Clause No 6.1.2: Delete this clause** ~~6.1.2 **EMERGENCY REQUEST**~~ ~~Emergency request function- When any of the emergency buttons placed anywhere in the vehicle is pressed, by any passenger / crew, make sure emergency request message has send and received at the control center.~~
9.	**Page 18/40** **Rename clause 6.2, 6.2.1,6.2.1.1, 6.2.1.2 , 6.2.1.3, 6.2.1.4, 6.2.1.5 to**

	6.1, 6.1.1,6.1.1.1, 6.1.1.2 , 6.1.1.3, 6.1.1.4, 6.1.1.5
10.	**Page 18/40** **Clause No 6.1.2.3 Replace with below** **6.1.2.3** ~~6.2.2.3 Vehicle Location data transmission to back office control center~~. System shall transmits PVT information to backend Control Center (2 different IPs) at user configurable frequency (minimum 5 seconds) via GSM/Cellular.
11.	**Page 18/40** **Add below new clause.** 6.1.1.6 System shall communicate to control center on the occurrence of the alerts captured in Communication Protocol Section 4.
12.	**Page 18/40** **Add below new clause.** **6.1.1.7** When Emergency Button is pressed, emergency request message shall be sent from the system and received at the control center.
13.	**Page 18/40** **Rename clause 6.3, 6.3.1, 6.3.2, 6.3.3, 6.3.4 to 6.2, 6.2.1, 6.2.2, 6.2.3, 6.2.4**
14.	**Page No 34/40** **Add below new clause.** Clause 8. CODE OF PRACTICE for Implementation of Vehicle Location Tracking (VLT) Device, Emergency Button(s) and Command and Control Centres Including Clause 8.1,8.2, 8.3, 8.4 & 8.5 Conformity of Production- Testing Parameters

8.0 CODE OF PRACTICE for Implementation of Vehicle Location Tracking (VLT) Device, Emergency Button(s) and Command and Control Centres

This Code of Practice for AIS-140 has been formulated for facilitating smooth I mplementation of Vehicle Location Tracking (VLT) Device, Emergency Button(s) and Command and Control Centres for the guidance of the stakeholders concerned.

8.1 General

a. The VLT device manufacturers will get their devices tested and certified from the testing agencies referred to in rule 126 of the CMVR for compliance to the rule 125 H of CMVR

b. The Backend System shall mean the backend Command and Control Centre set up/ authorized by State/UT or VLT manufacturers, providing interface to various stakeholders/systems such as State emergency response centre, the transport department or Regional Transport Offices, Ministry of Road Transport and

Highways and its designated agency, Vahan (or any other State/UT system used for registration of vehicles and/or issuance of permits), VLT device manufacturers and their authorised dealers, testing agencies, permit holders, etc. In the absence of State/UT backend system, the registration, activation, health check and alert updates of VLT devices shall be through a common layer.

The details of each VLT device (VLT device manufacturer code, device serial number, IMEI number, IccID number and other details as notified by the Central Government/State Government) shall be uploaded on the Vahan directly or through backend system by the VLT device manufacturer using its secure authenticated access.

The VLT device manufacturers or their authorised dealers shall install the VLT devices in vehicles and register/activate the devices along with details of vehicle and permit holder on the Vahan/corresponding backend systems in real-time.

The backend system/common layer will update the details of device in the Vahan system against the respective vehicle record.

c. The VLT device manufacturers or their authorised dealers, at the time of installation of VLT device in vehicles, shall configure the IP address and SMS gateway details in the device for sending emergency alerts to the emergency response system of the State/UT concerned.

d. The VLT device manufacturers or their authorised dealers, at the time of installation of VLT device in vehicles, shall configure the configuration parameters mentioned in AIS-140 in the device such as IP address and SMS gateway details for sending required data to the backend system.

e. The VLT device manufacturers shall ensure that a control mechanism is established for the secure data transfer from VLT to the backend system and that only the authorized devices transfer data to the backend system. The VLT device manufacturers shall also ensure that the mechanism for authenticating the vehicle owner and devices is followed as per the protocol specified in AIS-140 or such additional requirements as specified by the States/UTs. Authentication of vehicle shall be done through an OTP sent on vehicle owner's mobile number from the corresponding backend system.

f. In case of press of an emergency button, the VLT device will send data directly to the emergency response system of the respective State/UT. In addition, the backend system will send the alert to the respective permit holder, as decided by the State/UT.

g. VLT device manufacturers shall get their devices tested for conformity of production every year from the date of first certification, from the testing agencies referred to in rule 126 of the CMVR.

h. VLT device manufacturers shall get their backend systems certified for the States/UTs from the testing agencies referred to in rule 126 of the CMVR.

i. The VLT device manufacturers or their authorised dealers, at the time of installation of VLT devices in vehicles, shall configure the VLT device to send a secure authenticated activation message directly to the State/UT backend system/common layer as per the details provided in this Annexure.

j. The VLT device manufacturers shall ensure that the Health Check parameters are configured in the VLT device to send Health Check messages, on request from the State/UT backend system/common layer, to the respective backend system through SMS as per reference protocol mentioned in this Annexure.

k. VLT device manufacturers or their authorised dealers shall provide comprehensive warranty/maintenance support for the VLT device and facilitate cellular connectivity in accordance with the guidelines issued by central government vide Motor Vehicles (Vehicle Location Tracking Device and Emergency Button) Order, 2018 as amended from time to time.

l. The testing agencies will verify the conformity of production for the VLT devices as prescribed in section 8.5.

8.2 Installation, Registration, Activation and Service Process for VLT Device

a. VLT device manufacturers or their authorised dealers shall install VLT devices on permit holder's vehicles (only tested and approved model).

b. VLT device manufacturers shall ensure necessary uploading/integration of the installation data to the backend system/Vahan.

c. In case of any problem in updating Vahan, it will be VLT device manufacturer's responsibility to resolve the same.

d. VLT device manufacturers or their authorised dealers will also provide necessary print of installation/activation report to permit holder from the respective backend system.

e. Regional Transport Offices shall be able to verify the registration/activation/functional status of VLT device in the Vahan/corresponding backend system at the time of fitness testing.

f. The permit holder will have option to check the installation and device working status in the Vahan.

g. The VLT device manufacture may offer value added services, in addition to the mandatory performance requirements to the permit holders as per the mutual agreement between them. Mandatory performance requirements shall mean the following:

   i. Uploading device data in Vahan

   ii. Updating registration and activation data of VLT device

   iii. Sending device health status to the backend system

iv. Sending emergency alerts to the corresponding State/UT emergency response system

v. Sending over speeding alerts to the backend system

vi. Other performance requirements as per AIS 140 and as notified by central government vide Motor Vehicles (Vehicle Location Tracking Device and Emergency Button) Order, 2018 as amended from time to time.

h. The VLT device manufacturers may create their own system to monitor their supplied devices, emergency button/s & connectivity working / non-working status for managing warrantee / AMC and Cellular services.

i. The VLT device manufacturers or their dealers will update the SIM numbers and their validity/renewal details in the backend system.

8.3 VLT Device Manufacturers Backend Application/System Requirements

In case VLT device manufacturer offers to provide its backend system for State/UT, the same will need to meet the following requirements, in addition to those specified in Clause 7 of AIS 140:

a) The application will provide the ability to locate a vehicle at a given time.

b) Facility to track defined vs. actual movement of vehicles, capture deviations if any. (For vehicles where scheduled movement can be defined on GIS map).

c) The application should provide ability to track vehicle location on map. The map engine and data should comply with applicable regulations including guidelines as set out by Survey of India from time to time.

d) Facility for users to access and view position / location information on GIS maps near real-time through web interface with historic data displayed on maps.

e) Facility for providing current information location on demand.

f) Facility for playing back the recorded details of the vehicle movement along the authorized route (where applicable).

g) Provide facility of alert generation

   i. Ability to define new alerts on specific events

   ii. From the on-board devices in case of tampering

   iii. Speed exceeds the permissible limit

   iv. Vehicle moves out of its designated route or area

   v. Data feed not received from the on-board device

h) Provide facility to define rules for alerts/ notification and their delivery mode like SMS, email, pop-up etc.

i) Management of notifications to various stakeholders by way of email or SMS e.g. permit holders, RTO about device not working, over-speed etc.

j) Notification to the permit-holder through SMS in case any device stops functioning/sending data to the application.

k) Capability to update the on-board devices' firmware from the backend.

l) Capability to configure on-board device parameters from the backend.

m) The tracking data will be kept live in the system for at least 90 days. Utilities will be provided to support archive and restore functions for older data. Alerts/reporting shall be available for one year in the backend.

n) The backend will store VTS time-related data at the same resolution as received in the live application. The archived data after 90 days can also be restored using utilities provided.

o) From a security perspective, the devices will not communicate to any IP address located outside India whether it be the manufacturer's application or for purposes of configuration or firmware updates.

p) Firmware of the device needs to be available for auditing to notified testing agencies. Firmware binary should be made available with version matching one in the device as well as binary size & modification timestamp and/ or checksum should match for the binary provided and one installed on device. Backend System should be able to remotely read the existing version number of the firmware via an OTA configuration read command. A new version of the firmware should be pushed over the air from the VLT manufacturer's application. This shall be verified by the backend system remotely reading the new version number of the firmware in the device via and OTA configuration read command.

q) The device will communicate only to whitelisted set of IP addresses located in India and will receive communication and commands also from whitelisted set of IP addresses located in India.

r) The application and all key components like device management, firmware control, GIS map shall be hosted at a data centre/ cloud in India and it will be available for auditing by regulatory agencies.

s) The system shall provide > 99% availability and adhere to Infrastructure Security, Vulnerability Assessment and Penetration Testing guidelines as set out by Ministry of Electronics, Information and Technology, GoI.

t) No data should flow out of the country under any circumstances in compliance with applicable laws/regulations/guidelines.

u) The common layer shall be got tested from the testing agencies specified in CMVR Rule 126 for the following minimum functionalities:

   i. Registration and activation of the device(s) fitted on the vehicle, including the details of vehicle registration number, engine number, chassis number, vehicle make and model, device make and model, and connectivity details (telecom service provider's name, ICCid, SIM Nos., IMSI, date of validity, etc.).

   ii. Publish VLT device details in the Vahan/ any other State/UT system used for registration of vehicles and/or issuance of permits

   iii. Re-registration/re-activation of the device(s) fitted on the vehicle in case of any change in device or telecom service provider, etc.

   iv. Periodic health check of the device(s) fitted on the vehicle through SMS, as per section 8.5.

   v. Receiving alerts from VLT devices in case of defined deviations by vehicle such as over-speeding, etc. Publish alerts and health check received from VLT device in

the Vahan/ any other State/UT system used for registration of vehicles and/or issuance of permits.

vi. Provide interface to Vahan, respective State/UTs, RTOs, testing agencies, VLT device manufacturer's and their dealers.

8.4. Activation message and Health Check Message Protocol

The protocols for activation message and health check message are given below. Device shall send the activation and health check messages on request as specified below directly to the backend system (i.e. backend Command and Control Centre set up/ authorized by State/UT or a Common Layer system providing interface to VLT device manufacturers' backend applications).

A. Activation SMS Format from Backend System to Device

Activation Message Request Format from the Backend System to the Device (Through SMS): ACTV, Random Code, Reply SMS Gateway no.

Activation Message Reply Format from Device to the Backend System (Through SMS) as per Table 1 below:

Table-1: Activation & Health Check Response SMS Format from Device to Backend System

Field Name	Characters	Activation Example	Health Check Example
Header	5	ACTVR	HCHKR
Separator	1	,	,
Random code	6	343434	474747
Separator	1	,	,
Vendor ID	4		
Separator	1	,	,
Firmware version	6	V1.6.1	V1.6.1
Separator	1	,	,
IMEI	15	012345678912345	012345678912345
Separator	1	,	,
Alert ID	2	1	1
Separator	1	,	,
Latitude	12	14.034533	14.034533
Separator	1	,	,
direction	1	N	N
Separator	1	,	,
Longitude	12	79.32045	79.32045
Separator	1	,	,

Table-1: Activation & Health Check Response SMS Format from Device to Backend System			
Field Name	**Characters**	**Activation Example**	**Health Check Example**
Direction	1	E	E
Separator	1	,	,
GPS fix	1	1	1
Separator	1	,	,
Date and Time	15	16112018 120317	16112018 120317
Separator	1	,	,
Heading	6	263.19	263.19
Separator	1	,	,
Speed	4	25.4	25.4
Separator	1	,	,
GSM Strength	2	23	23
Separator	1	,	,
Country Code (MCC)	3	404	404
Separator	1	,	,
Network Code (MNC)	4	10	10
Separator	1	,	,
LAC	4	d6d6	d6d6
Separator	1	,	,
Main Power	1	1	1
Separator	1	,	,
IGN Status	1	1	1
Separator	1	,	,
Battery Voltage	4	24.6	24.6
Separator	1	,	,
Frame Number	6	100000	100000
Separator	1	,	,
Vehicle mode	2	ID	ID
Total Characters	**139**		

B. Health Check Random Messages from Backend System to Device

Frequency: Twice Daily (Recommended),

Health Check Message Request Format from the Backend System to the Device (Through SMS): HCHK, Random Generated ID, Reply SMS Gateway no.

Health Check Message Reply Format from Device to Backend System (Through SMS): As per Table 1 above.

C. Publish Data to Common Layer by VLT Device Manufacturers' Applications (Sample)

Requirement to be complied with by VLT device manufacturers' applications

Application shall publish the data to common layer in a specified frequency and format as mentioned below

Services to publish data to the common layer

a. pushOffenceDetails

Type : REST web service

Data Type : JSON Array

Frequency : 1 Hour

A single request may contain JSON Array of maximum 500 JSON Objects of the following format.

Sl No	Key	Value Length in bytes	Description
In Parameters			
1.	oftyp	2	Offence Type OS= Overspeed
2.	vno	16	Vehicle number without any delimiter like hyphen (-) or space.
3.	imei	15	IMEI number.
4.	date	8	Date in format DDMMYYYY
5.	time	6	UTC in format hhmmss
6.	lat	12	Latitude,decimal not less than 6 places
7.	latd	1	Latitude Direction. N=North, S= South
8.	lon	12	Longitude,decimal not less than 6 places
9.	lond	1	Longitude Direction. E=East, W= West
10.	spd	6	Speed in km/hrs, Upto One Decimal Value.
11.	loc		Location (Reverse Geo-coded)
12.	rto		RTO Code
13.	state		State Code
Response			
14.	resp		OK/ Error

b. pushAlertDetails

Type : REST web service

Data Type : JSON Array

Frequency : 1 Hour

A single request may contain JSON Array of maximum 500 JSON Objects of the following format.

Sl No	Key	Value Length in bytes	Description
In Parameters			
1.	alrtid	2	Alert ID as per AIS-140
2.	vno	16	Vehicle number without any delimiter like hyphen (-) or space.
3.	imei	15	IMEI number.
4.	date	8	Date in format DDMMYYYY
5.	time	6	UTC in format hhmmss
6.	lat	12	Latitude,decimal not less than 6 places
7.	latd	1	Latitude Direction. N=North, S= South
8.	lon	12	Longitude,decimal not less than 6 places
9.	lond	1	Longitude Direction. E=East, W= West
10.	spd	6	Speed in km/hrs, Upto One Decimal Value.
11.	loc		Location (Reverse Geo-coded)
12.	rto		RTO Code
13.	state		State Code
Response			
14.	resp		OK/ Error

8.5 Conformity of Production - Testing Parameters

a. The VLT device manufacturers will get their devices tested and certified for conformity of production from the testing agencies referred to in rule 126 of the CMVR for compliance to the rule 125 H of CMVR every year from the date of first certification. The parameters for testing shall be as specified in Table 1 of this section.

b. The VLT device manufacturers shall get their backend applications audited from the testing agencies referred to in rule 126 of the CMVR or by the agencies specified by States/UTs every year from the date of first certification. The parameters for auditing shall be as specified in Table 2 of this annexure.

c. The testing agencies shall provide the details of the VLT devices and backend applications certified by them to the States/UTs by uploading the same on the respective backend systems or any other means.

Table 1: Test for COP of VLT Device and Emergency Buttons

Sl. No.	Test Details (As per AIS-140)
1.	Emergency button functionality (Clause No. 3.1.2.4)
2.	SMS fall back (Clause 3.1.5)
3.	Table 4A (Clause 4.1)
4.	Table 4B and 4C (Clause (4.2)
5.	Table 6A: Functional Testing (Sr. No. 1-9, Clause 6.3.1)
6.	Performance Parametric Test of Table 6B (Clause 6.3.2, Sr. No.10)
7.	Protocol & alerts verification as per Table no 4A, 4B, 4C & 3B & OTA Commands verification
8.	Ingress Protection (IP) Test as per Sr. No. 3 of Table 6B

Table 2: Test Parameters for Auditing of VLT Device Manufacturer's Backend Application/System

Sl. No.	Test Details
1.	Firmware over the air update. Backend application should be able to remotely read the existing version number of the firmware via an OTA configuration read command. A new version of the firmware should be pushed over the air. This should be verified by reading the new version number of the new firmware in the device via and OTA configuration read command.
2.	Application availability test to be conducted over a 7 days' period by periodic check of availability randomly or at specified intervals in an automated or manual manner.

Sl. No.	Test Details
3.	Test functionality of application to allow user to map & un-map a device to a vehicle.
4.	Test functionality to track a vehicle on a map over a period of 8 hours given either a device ID or vehicle registration number. The device ID and vehicle should be mapped beforehand.
5.	Test replay of a vehicles location by specifying a start and end date and time and device ID or vehicle registration number. The start and end date and time should be from within the last 3 months at date of test. In case 3 months of historical data is not available, the VLT manufacturer can pre-populate test data for the duration.
6.	Firmware binary should be made available with version matching one in the device as well as binary size & modification timestamp and/ or checksum should match for the binary provided and one installed on device.
7.	Test to confirm geographical location of IP addresses, the device communicates with by IP Geolocation for all IPs configured into the device to confirm they are in India. The IPs configured should be read from the firmware configuration via configuration read command and also separately confirmed against a list of IPs provided by the VLT manufacturer.
8.	VLT manufacturer to provide a certificate, statement or affidavit certifying the location of data centre/ cloud hosting region in India for user, device and vehicle data.
9.	VLT manufacturer to provide a Vulnerability Analysis and Penetration Testing report from a 3rd party test agency authorised by CERT-In/STQC.