Submitted by the expert of
SAE International

Informal document **GRVA-15-46**
15th GRVA, 23-27 January 2023
Agenda item 5(a)

SAE proposal to UNECE WP.29 GRVA related to CS/OTA

Text on GNSS in UN R155 Annex B: Effect of current language

- ISSUE: As currently written, UN R155 is design restrictive by explicitly promoting one technology without appropriate clarifying language or guidance.

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

- Unless the interpretation document states otherwise, “authenticity and integrity” will be read to mean “cryptographic authenticity and integrity”
  - So implementers are expected to either support cryptographic GNSS authentication or document why they don’t
- … but cryptographic GNSS authentication is not widely supported
  - Support announced for Galileo but not yet deployed; Japanese QZSS support planned; no support announced for GPS, GLONASS, BDS
- Listing a single approach when other approaches are available to achieve the stated threat mitigation objectives, implies this approach is preferred and makes the current language design restrictive.
  - Implementers are encouraged to use a technology even if contracting parties have themselves chosen not to deploy that technology
- The language implies there is WP.29 consensus on GNSS authentication when there is not

Text on GNSS in UN R155 Annex B: Background

- SAE believes that cryptographic authentication is useful but that **the example should not be included in a UN regulation until more individual contracting parties operate GNSS constellations that support the technology**
- There are other mechanisms that can be used to mitigate the impact of GNSS spoofing
  - See, e.g., NIST, *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of PNT Services* https://www.nist.gov/pnt
- Until there is global technical consensus among contracting parties that cryptographic authentication is the preferred mechanism to mitigate GNSS spoofing, UNECE regulations should not imply that it is the preferred mechanism

Text on GNSS in UN R155 Annex B: History of discussion

- September 2022, GRVA: Extensive discussion of SAE proposal which included proposed revisions to R155 and to the interpretation document
  - No disagreement was voiced on the substance of the proposal
  - Concerns that the proposed language for R155 was too detailed
  - Some sentiment that R155 should be left unchanged and the only modification should be to the interpretation document
  - SAE was asked to prepare a revised proposal for consideration by CS/OTA
- December 2022, CS/OTA:
  - SAE provided a new proposal with more general language for R155 and revisions to the interpretation document
  - ESA objected, stating that cryptographic authentication should be **required**
  - It was determined that there was **no consensus** to advance the SAE proposal
    - However, the discussion on substance was brief and did not address points raised in the September meeting
  - SAE respectfully suggests that the current wording, if understood to recommend cryptographic authentication of GNSS, **also does not represent the consensus of the group** based on the September discussion

Text on GNSS in UN R155 Annex B: Proposal

- Although the language may be appropriate in the medium to long term, UN regulations should include examples that are appropriate for current technology.
- SAE proposes adding the following language to the interpretation document, section “AB. Paragraph 7.3.4.”

  (d) Referring to row 1 of table B.1 in Annex 5 Part B: The validity of received messages may be carried out by any appropriate means. For example, for V2X, digital signatures might be applied to the message. For example, for GNSS, the technique used might be the Galileo Commercial Authentication Service (CAS) using cryptographic authentication, or technologies such as directionality, dual antennas, signal strength, and consistency of velocity.

- SAE would welcome alternative suggestions to clarify the language and make clear that cryptographic authentication is not being promoted above solutions preferred by other contracting parties to prevent GNSS spoofing

Thank you for listening

Questions?