Submitted by the experts from
SAE International

Informal document **GRVA-13-28**
13th GRVA, 23 - 27 May 2022
Provisional agenda item 5(a)

# SAE proposals to UNECE WP.29 related to automotive cybersecurity

S. William Gouse (SAE), Nick Russell (BlackBerry), William Whyte (Qualcomm)

2022-05-06

# Summary

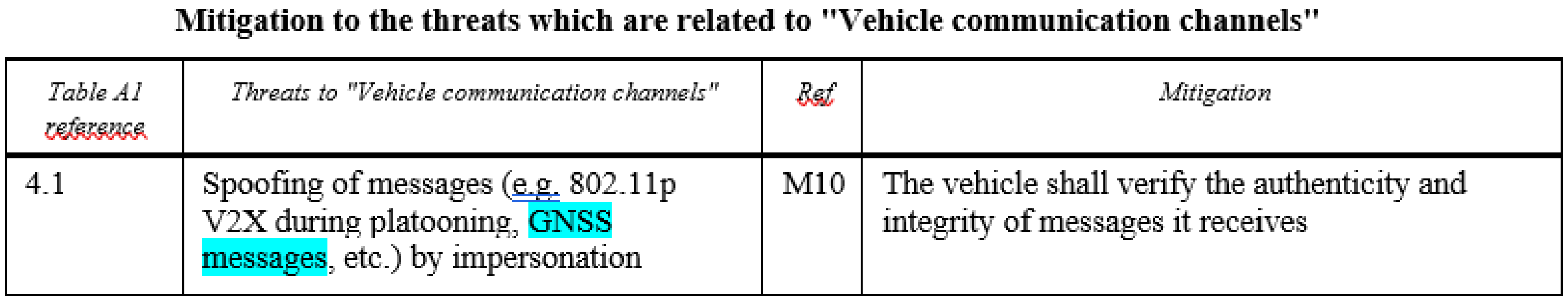
- Issues with the UNECE’s WP.29 regulation on cybersecurity (UN R155) have been noticed by two SAE members
  - UNECE's official interpretation document for UN R155 references an out-of-date version (DIS) of ISO/SAE 21434 and does not correctly cite ISO PAS 5112
  - Annex B of UN R155 contains ambiguous language that has been interpreted within the automotive industry as putting a narrow requirement on vehicle GNSS implementations – specifically, a mandatory requirement that vehicles carry out cryptographic authentication of received GNSS messages
- SAE has Special Consultative Status with the UN Inland Transport Commission, which governs UNECE WP.29 and its working groups
  - This includes the GRVA committee, which oversees the work done on UN R155 and its interpretation document in the now-closed CS/OTA Informal Working Group (IWG)
  - See back-up slides for more info on UNECE and its structure
- Since SAE has presence at GRVA, it is proposed that SAE request GRVA to address these issues
  - First step will likely be to request re-opening of the CS/OTA IWG so that the proposals can be discussed by the necessary experts i.e. those who originally drafted UN R155 and its interpretation document
  - Off-line sharing of the proposals with various government entities (e.g. NHTSA, Transport Canada, etc) and other interested parties will also take place
- TEVEES18A is kindly requested to endorse SAE’s engagement with UNECE WP.29 GRVA (and its CS/OTA IWG subcommittee) and the proposals to address the above issues
  - GRVA’s next meeting is w/b 23rd May
  - It is *hoped* that the CS/OTA IWG can be reopened again sometime in the Fall

# Update UN R155 official interpretation document

- The Official Interpretation Document for UN R155 makes extensive reference to ISO/SAE **DIS** 21434, which at the time of writing that document was the latest version available of this standard.
  - The document also makes some reference to ISO PAS 5112 (CS audit handbook), which at the time of writing the document was very much in its infancy.
- Both ISO/SAE 21434 and ISO PAS 5112 have now been finalised and published, therefore the it is proposed to update all references to the final/published version of ISO/SAE 21434 as well as modify and add references to ISO PAS 5112 in a new version of the interpretation document for UN R155.
  - Some simple updates to the new numbering of clauses, requirements and work products are made, as well as suggest some more extensive updates, including addition of references to ISO PAS 5112.

# Fix ambiguous text on GNSS in UN R155 Annex B (1/2)

- UN R155 contains the following language which can be read as requiring cryptographic authentication of GNSS messages



**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 |

- Currently no GNSS system supports authentication of messages
  - EU's Galileo intends to switch on Navigation Message Authentication (OSNMA) in 2023, no precise date has been published
  - Even in Galileo, other signals are not authenticated
- Concerns about this implied requirement
  - Can't be met until after 2023 at least
  - Would rule out the use of other GNSS systems, reducing robustness
  - In practice, privileges EU's Galileo over other GNSS systems – inappropriate for a UN regulation

# Fix ambiguous text on GNSS in UN R155 Annex B (2/2)

- Although the requirement is not unreasonable as a goal, it is not appropriate to require it for type-certification in the near future
  - Would be suitable once, e.g., [two] GNSS systems have supported authentication for [two] years
  - Note that OEMs still need to provide rationale for accepting non-authenticated signals even if Navigation Messages are authenticated
- Several possible language fixes (to both the regulation itself and the interpretation document) are provided in our doc submitted to this meeting as a starting point for discussion
- Examples of possible fixes include:
  - Change R155 as follows:
    - The vehicle shall verify the authenticity and integrity of messages it receives using appropriate mechanisms. Depending on the message type and capabilities, these may include cryptographic authentication and integrity checking; plausibility checking; use of a diversity of sources; and other appropriate means of providing assurance.
  - Change R155 interpretation doc:
    - Referring to row 1 of table B.1 in Annex 5 Part B: This row should not be read as creating a requirement that received GNSS messages are cryptographically authenticated by receivers. The manufacturer may choose to use cryptographic authentication or may choose to use other means to mitigate risks from incorrect GNSS messages. The manufacturer should be able to justify the strategy implemented.

SAE INTERNATIONAL

# Thank you for listening

Questions?