Submitted by the experts from
SAE International

Informal document **GRVA-13-29**
13th GRVA, 23-27 May 2022
Provisional agenda item 5(a)

Proposal for amendment to UN Regulation No. 155

1 Introduction

This paper notes ambiguous language in Annex B of UN R155 that has been interpreted within the automotive industry as putting a narrow requirement on implementations – specifically, a mandatory requirement that vehicles carry out cryptographic authentication of received GNSS messages. The paper questions whether that narrow requirement is or should be intended and examines consequences if that interpretation is in fact enforced as part of conformance testing. Finally, the paper proposes alternative wording that is suggested to be more appropriate and, in practical terms, will lead to more resilient implementations than the interpretation-of-concern of the current wording would.

2 Problem statement

The language of concern in UN R155 appears in the first row of Table B.1 in Annex 5:

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

The point of concern arises from the fact that the Threat column lists GNSS messages as a type of message that can be spoofed and the Mitigation column mandates that the vehicle verify the authenticity and integrity of messages it receives.

A natural reading of this is to mean **cryptographic** authenticity and integrity, i.e. that the vehicle is required to carry out cryptographic operations on **all** messages it receives. If this is the intention of the text, then this is a concern for GNSS for the following reasons.

In GNSS, there are multiple providers (GPS, Galileo, BeiDou, etc) but only one currently natively supports authentication of messages, the OSNMA authentication that is provided in Galileo. (Other systems are trialing authentication technologies). Even OSNMA is currently not fully deployed; OSNMA is currently in public testing and the service phase of OSNMA, i.e. availability for everyday use, is not anticipated to start until 2023, according to the European GSC which manages the system (https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_Info_Note.pdf). Therefore a requirement for GNSS authentication in vehicles to be sold from 2024 on has two issues:

1. The marketplace of GNSS receivers that can carry out OSNMA authentication may not be mature in 2024, leading to (a) lack of choice of suppliers and increased cost and (b) the security risks that may come from the use of early-stage products.
2. A requirement for authentication effectively means that type-certified vehicles can only use Galileo for positioning. This decreases the ability of receivers to use diversity as a mitigation technique – i.e. to use multiple GNSS providers for more reliable positioning. It also means that

any service interruption to Galileo would cause all devices conformant to this regulation to completely lose positioning. This is a significant risk to the robustness of the system.

Both of these risks might be mitigated over time as authentication in GNSS becomes more widespread, but it is not appropriate to require GNSS authentication in 2024, if this was indeed the intention of the aforementioned text of UN R155.

Therefore we kindly request that the language in UN R155 is clarified, or interpretation provided, to make it clear that the intent is not to require cryptographic authentication of GNSS messages, or at least not required at the start time of the application of the regulation due to the aforementioned issues.

3 Current status of interpretation

3.1 Background

We note that the currently available implementation clarification material does not provide an unambiguous resolution to the question of whether GNSS authentication is required. In this section we review available clarification material and explain why we believe that additional clarification is needed.

First, we note the main text of UN R155, specifically the requirements to vehicles in clause 7:

7. Specifications

...

7.3. Requirements for vehicle types

...

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 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, 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 type approvals prior to 1 July 2024, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, 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.

Regarding the yellow highlighted text, if there are no risks identified for the vehicle relating to its capability to determine its position (i.e. spoofing of GNSS messages will have no effect on the safety of the vehicle), then one could argue that no mitigations are needed.

Regarding the purple highlighted text, the inability to cryptographically verify the authenticity of GNSS messages due to deficiencies of the GNSS being used could be an argument for the stated mitigation in Annex 5 being not relevant. In which case, another mitigation such as verification using multiple GNSSs could be argued as more appropriate.

Regarding the green highlighted text, it could be argued that another appropriate mitigation for protection of GNSS message spoofing than that mentioned in Annex 5 is sufficient for all GNSS components manufactured before 1 July 2024. We note the amendment, proposed by GRVA, to the green highlighted text above:

> *In particular, for type approvals ~~prior to~~* ***first issued before*** *1 July 2024* ***and for each extension thereof****, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, 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.*

Finally, there is some clarification given in the official interpretation document to UN R155 to the above mentioned requirement (7.3.4). Specifically, it is stated:

> *The intention of this requirement is to ensure that vehicle manufacturers implement appropriate mitigation measures in accordance with the results of their risk assessment.*
>
> *The manufacturer should provide reasoned arguments and evidence for the mitigations they have implemented in the design of the vehicle type and why they are sufficient. This may include any assumptions made, for example about external systems that interact with the vehicle.*
>
> *The technical mitigations from Annex 5, Parts B and C shall be considered wherever applicable to the risks to be mitigated. The Manufacturer may present a rationale not only for a listed mitigation from Annex 5 being "not relevant or not sufficient", but also may present a rationale, that another mitigation other than the ones listed in Annex 5 is appropriate to the respective risk. That rationale may be substantiated by a risk assessment and risk rating showing the appropriateness of the alternative mitigation. This is to allow the adoption of new or improved defensive technologies.*

3.2 Conclusion on current status of interpretation

We acknowledge that the current text can be interpreted as not requiring GNSS authentication. However, we note that as things stand, every OEM that is attempting to claim conformance to R155 will have to individually make the case that GNSS authentication is not necessary, and that this may then end up being the subject of potentially prolonged negotiation or discussion between the OEM and the certification organization. We believe that it would be simpler and would reduce burden on all parties if instead the language in R155 was clarified to explicitly address the GNSS authentication issue.

4 Proposed resolution

4.1 Overview and rationale

We believe that the stated text of the regulation should not be interpreted to require cryptographic authentication of GNSS messages, or at least not require this until at least two GNSS systems accepted by the regulation support cryptographic authentication for civilian use, and until this has been the case for at least two years. Alternatively, allow other technical solutions for mitigating the spoofing of GNSS messages e.g. validation based on consistency and context of messages, and on comparison of input from multiple GNSS systems, where this is appropriate. This would address the maturity and robustness concerns put forward above.

We believe that the best way to accomplish this, rather than put conditional language such as the above in the regulation itself and raise possible concerns about ambiguities in interpreting the conditions, would be to remove the implied requirement for GNSS authentication from the regulation (or make clear by interpretative language that the requirement is not meant to be implied). When the conditions in the previous paragraph are met, or when it becomes apparent that there is a date on which they will be met, the regulation or interpretation can be revised to make the requirement explicit and state the date from which it applies.

We propose that for now it is made clear that the regulation is to be interpreted as follows:

> The vehicle shall use mechanisms to provide assurance of the trustworthiness and correctness of received messages. 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.

This may be done by replacing the text in the mitigations box of the indicated row of Table B1 directly, or by making it clear in an interpretations document that this is the intended interpretation.

4.2 Specific proposals

4.2.1 Proposal to UN R155

In Annex 5, Part B, modify the text in the first row of Table B1 as follows:

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 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.

4.2.2 Proposal to official Interpretation document

Add the following language to Part A, section AB (“Paragraph 7.3.4”), in the interpretation document (source: https://unece.org/sites/default/files/2021-02/ECE-TRANS-WP29-2021-059e_0.pdf):

> *The following clarifications should be noted:*
>
> (a) The design decisions of the manufacturer should be linked to the risk assessment and risk management strategy. The manufacturer should be able to justify the strategy implemented;
>
> (b) The term "proportionate" should be considered when choosing whether to implement a mitigation and what mitigation should be implemented. If the risk is negligible then it may be argued that a mitigation would not be necessary;
>
> (c) Protection from identified risks means to mitigate the risk
>
> [ALTERNATIVE PROPOSAL 1] (d) 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.

[ALTERNATIVE PROPOSAL 2] (d) Different mitigations to those listed in Annex 5 for their associated risks are allowed if a rationale is provided explaining how the risk identified is sufficiently mitigated e.g. use of a diversity of location determination sources due to a lack of authenticity and integrity protection capability in GNSS messages.

[ALTERNATIVE PROPOSAL 3] (d) The phrase "not relevant or not sufficient" should be considered to include those mitigations that are technically not possible e.g. lack of authenticity and integrity protection capability in a messaging system.
