ADS IWG Working Document
Change Proposal Form
One major comment per form
(Shaded blocks for use by the IWG Secretariat)

Document Reference	ADS-14-38	Date	16 October 2025
Agenda item			

Proposed by (affiliation only—no personal information)

United Kingdom

Summary of Change (25 words or less)

To address open item 'Other provisions' item 2 on cybersecurity and software updating.

To introduce requirements for resilience to electromagnetic interference.
This document supersedes ADS-13-04, ADS-13-05, ADS-13-06

Reason for Change (Justification)

To address the open item on cybersecurity and software updating following discussions on ADS 13-04 on the first day of the 14th ADS IWG, this proposal removes the reference to annexes based on the CS-OTA guidance document leaving it to national law in the GTR countries. This leaves a high level requirement for both cybersecurity and software updating.

This amendment also introduces requirements for the ADS to be resilient to electromagnetic interference.

Location	(e.g., paragraph, chapter, annex, appendix)

Original text

(Reference document ADS-14-03r1)

4.3/6.3. Other Requirements

4.3.2./6.3.2 [Requirements specific to cyber security of ADS installed on vehicles]

4.3.3./6.2.3 The manufacturer shall include a robust process in the SMS to ensure that post-deployment software updates are properly validated and distributed and downloading is confirmed.

5.3.2.5./7.3.2.5. The manufacturer shall describe measures taken to assure the cybersecurity of the ADS and the analysis performed to identify and disposition likely security threats. Where UN R 155 applies, the manufacturer shall describe how the ADS meets the requirements of that regulation.

5.3.2.6/7.3.2.6. [Software updates & Safety Case updates as per 5.1.4.3/7.1.4.3]

Revised text

Replace the existing text of 4.3.2/6.3.2 and 4.3.3/6.3.3 with the following:

UNR text
6.3.2 The ADS shall be protected from cyber threats.
This requirement shall be demonstrated by compliance with the requirements of UN Regulation No. 155 according to its original version or later series of amendments.

GTR text
4.3.2 The ADS shall be protected from cyber threats
4.3.2.1 The manufacturer shall document and implement processes for managing cyber security across the development, production and post-production phases.
4.3.2.2 The manufacturer shall describe its processes for cyber security including:
a) identification, assessment and treatment of cyber security risks
b) monitoring, detecting and responding to cyber-attacks
c) mitigating relevant cyber threats and vulnerabilities in a reasonable timeframe

UNR text
4.3.3. If the ADS software can be updated, the ADS shall support safe and secure software updates.
This requirement shall be demonstrated by compliance with the requirements of UN Regulation No. 156 according to its 01 or later series of amendments.

GTR text
6.3.3. If the ADS software can be updated, the ADS shall support safe and secure software updates.
6.3.3.1 The manufacturer shall document and implement processes for safely and securely managing ADS software updates including:
a) software identification and version control
b) description and notification (e.g. release notes for each software version)
c) verification and validation prior to deployment
d) target vehicle identification and compatibility checks
e) safe and secure delivery and implementation

Delete the existing text of 5.3.2.5./7.3.2.5 and 5.3.2.6/7.3.2.6 (safety case text on cyber security and software updating)

Insert standard text for UN regulations on software identification (RxSWIN) in line with Consolidated Resolution on the Construction of Vehicles (R.E.3) (from WP.29/2025/147 as amended by WP.29-197-06):

UNR text In the "Definitions" chapter, insert a new paragraph to read:
"2.x. For the definitions with regard to Software Identification Number, refer to the Consolidated Resolution on the Construction of Vehicles (R.E.3), Annex 7, paragraph 2."

UNR text Insert a new paragraph, to read:

"8.3.3.5. For all vehicles, equipment and parts with which the approval tests are performed, the manufacturer shall provide the necessary information (e.g. software versions and system parameters) allowing the Technical Service to uniquely identify the configuration of all hardware and software that have an influence on performance with regard to this Regulation; this information shall be appended to the test report."

Insert new provision in 4.3/6.3:

UNR Text
6.3.X The effectiveness of the ADS shall not be adversely affected by magnetic or electrical fields. This requirement shall be demonstrated by compliance with the 07 or later series of amendments to UN Regulation No. 10

GTR Text
4.3.X The effectiveness of the ADS shall not be adversely affected by magnetic or electrical fields.

(new) Possible guidance document text:

Global Technical Regulation requirements regarding cyber-security and software updating

When complying with the requirements for cyber-security and software updating, manufacturers may wish to consider existing regulations and guidelines related to cyber security such as the GRVA Recommendations on uniform provisions concerning cyber security and software updates.

Additional model provisions from WP.29/2025/147 as amended by WP.29-197-06, for inclusion in workshop UNR administrative provisions document

Insert a new paragraph, to read:

"9.4. The vehicle manufacturer may apply for a new vehicle approval for the purpose of differentiating software versions intended to be used on vehicles already registered in the market from the software versions intended to be used on new vehicles. This may cover the situations where type approval regulations are updated, or hardware changes are made to vehicles in series production. In agreement with the Type Approval Authority or its Technical Service, duplication of tests for these approvals shall be avoided where possible."