White paper [PRELIMINARY- March 2, 2021]

Cyber security on Vehicles: Roadmap to Compliance

New EU transportation regulations give a pragmatic approach to Cyber Security for connected vehicles

Introduction

Transportation regulations give a pragmatic approach to cyber security for connected vehicles. Approving a car or a truck for compliancy in public roads is challenging because the life of persons is taken into account. Cyber attacks are a serious threat in this context and it's important to understand how and to what extent regulations are dictating ways for building security.

In this white paper Bluewind will illustrate the Cyber Security on vehicle status until 2021. Starting by given a background on vehicles regulation, Bluewind will explain the context of cyber security on Vehicle. Connected Vehicles can't ignore the safety consequences of a hack. In the end, there will be an overview to the new regulations and standards (EU Regulation No. 2019/2144). Bluewind will show the new guidelines R155, R156 and the ISO/SAE 21434.

Background on Vehicles Regulations

Vehicles to be awarded the right to circulate in public roads need to comply to several regulations (based on world areas), and appointed national bodies are in charge of approving a newly designed vehicle.

For a large geographical region the United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations (also known as WP.29) is a unique regulatory forum within the institutional framework of the UNECE Inland Transport Committee.

https://unece.org/transport/vehicle-regulations

The role of WP.29 in the context of United Nations is to develop regulatory requirements for safety and environmental performances of vehicles. WP.29 establishes several Working Parties that provide technical oversight and expertise for the development of regulations.

UNITED NATIONS

World Forum

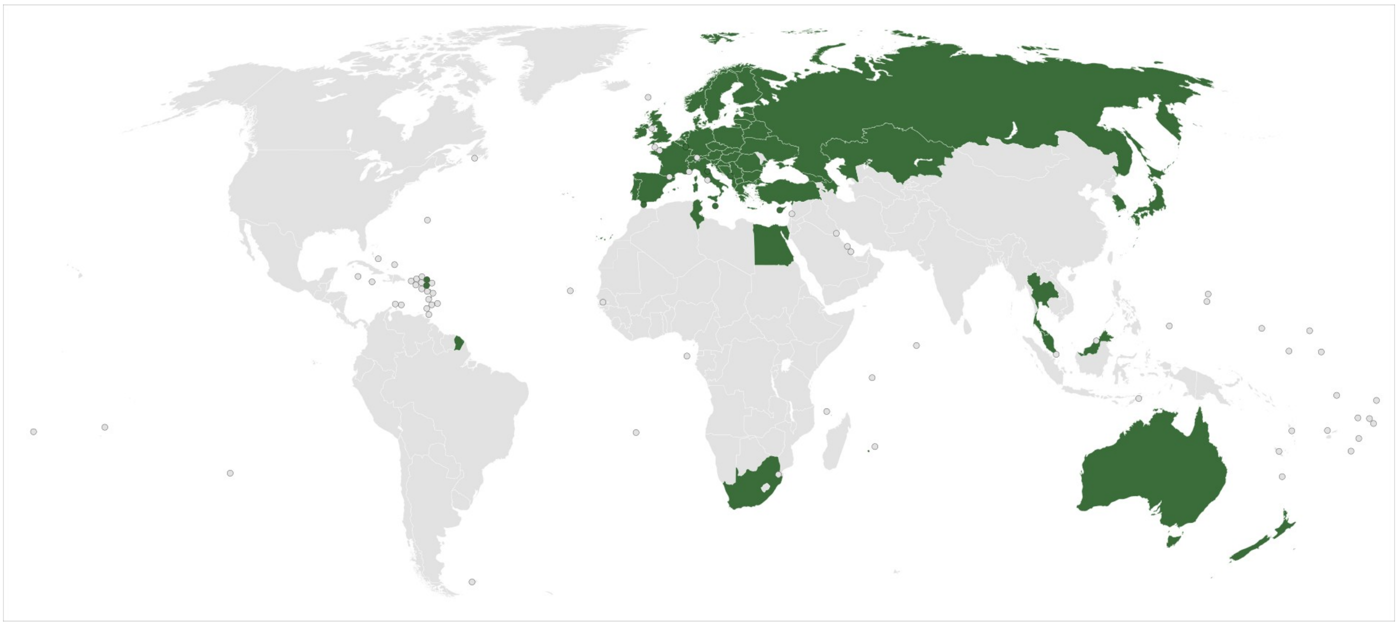
for

Harmonization of Vehicle Regulations (WP.29)

A legal framework to WP.29 actions is provided by three historical agreements, that happened back in 1958, 1997 and 1998. All Member countries attending the WP.29 sessions can establish regulatory instruments concerning vehicles thanks to elaborations while participating to the works of WP.29.

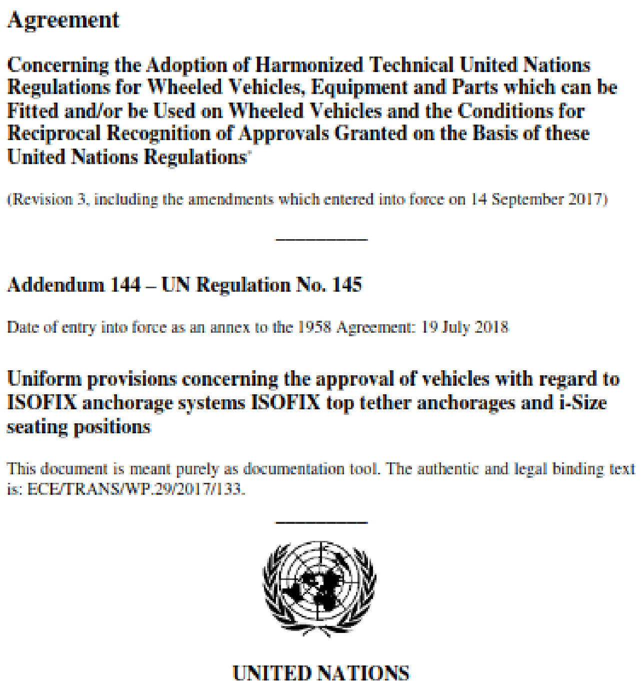
The three agreements refer to different regulatory instruments:

- UN Regulations (1958 Agreement)
- United Nations Global Technical Regulations (1998 Agreement)
- UN Rules (1997 Agreement)



Regulatory proposals are documented per month, year on website.
Each regulation is known as a UN ECE Rxxx document (xxx=number) discussed in one of the WP.29 working parties (subsidiary bodies) or specialized task forces. Active working parties are:

- GRBP: Noise and Tires
- GRPE: Engine, Emissions, Energy
- GRE: Lighting and Light-Signaling
- GRVA: Automated/Autonomous and Connected Vehicles
- GRSP: Passive Safety
- GRSG: General Safety Construction



Agreement

Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*

(Revision 3, including the amendments which entered into force on 14 September 2017)

Addendum 144 – UN Regulation No. 145

Date of entry into force as an annex to the 1958 Agreement: 19 July 2018

Uniform provisions concerning the approval of vehicles with regard to ISOFIX anchorage systems ISOFIX top tether anchorages and i-Size seating positions

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2017/133.

UNITED NATIONS

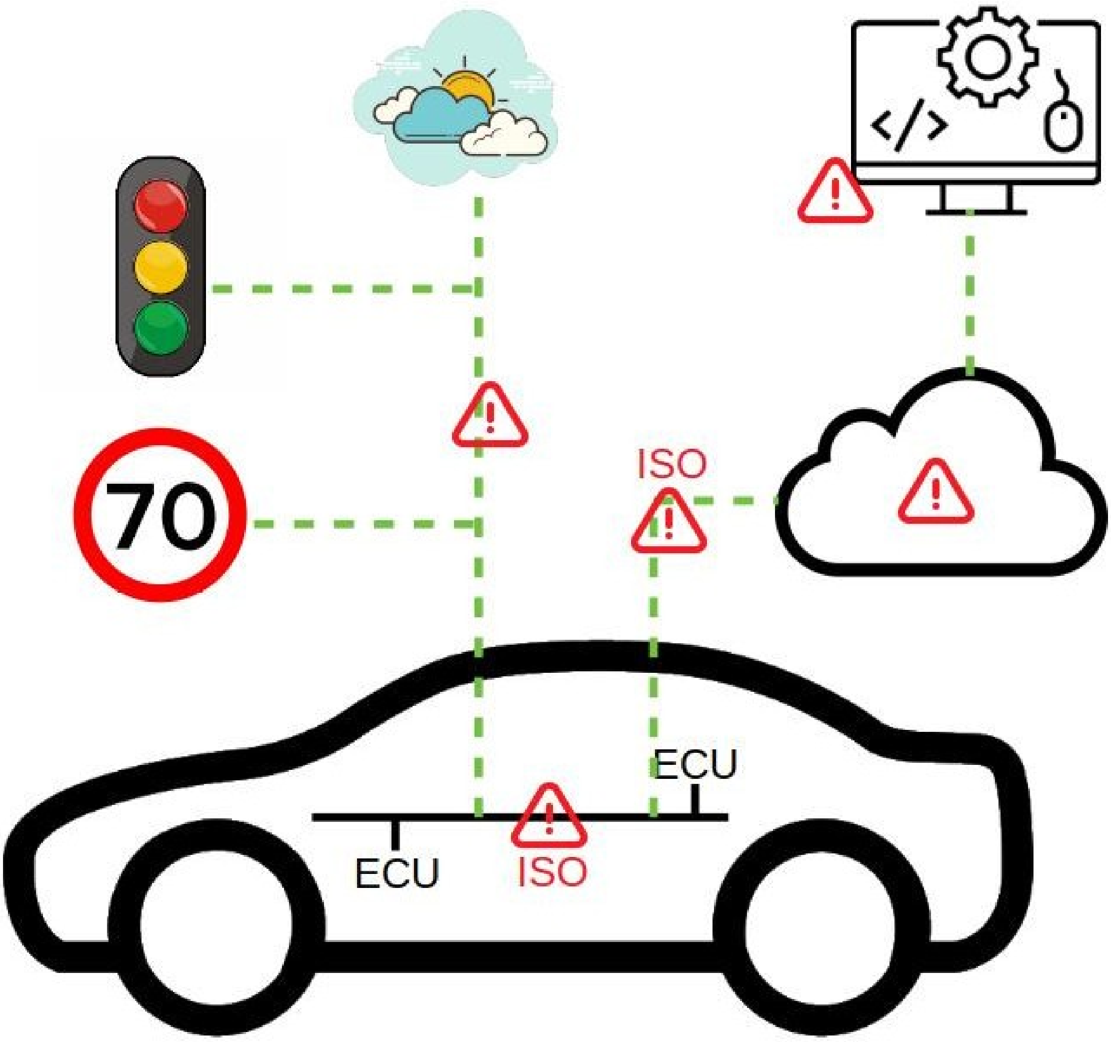
The documents elaborated and published by the working parties contain precise and clearly stated measures for safety, environment protection and road compliance of vehicles with a balance between completeness and generalization, not an easy task.
Recently cyber security has been investigated with very good results despite the complex scenario of transportation connectivity.

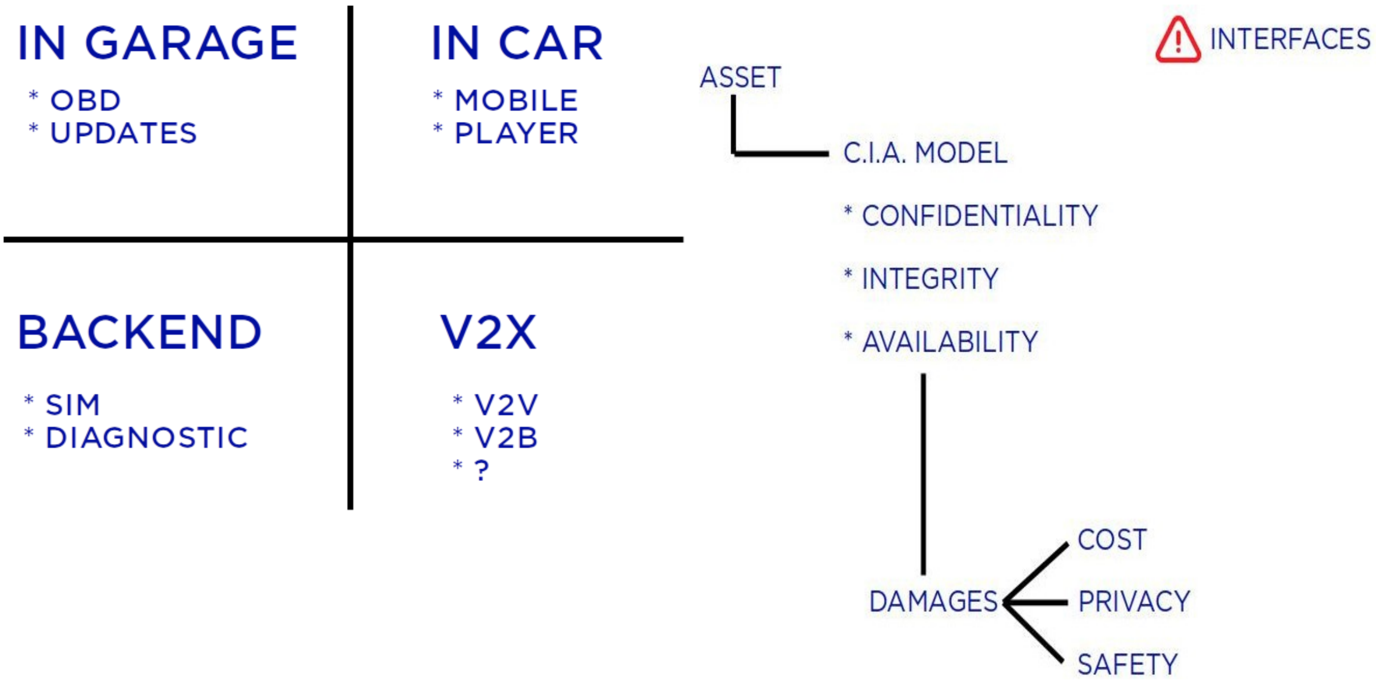
Cyber Security on Vehicles

The context of cyber security is different based on vehicles generations, components and threats.

The generation of vehicles range from locally connected models to totally meshed ones.
Components relevant to cyber security are ECUs (electronic parts with software), on-board communication buses, remote communication channels and external entities like cloud services and road signals.

Threats to such components are categorized by asset, potential damage and severity. Overall, listing all possibilities is a process that resembles the safety risks and mitigating measures analysis well known to whom functional safety is a familiar engineering practice.





IN GARAGE
* OBD
* UPDATES

IN CAR
* MOBILE
* PLAYER

BACKEND
* SIM
* DIAGNOSTIC

V2X
* V2V
* V2B
* ?

⚠ INTERFACES

ASSET

C.I.A. MODEL

* CONFIDENTIALITY

* INTEGRITY

* AVAILABILITY

DAMAGES

COST

PRIVACY

SAFETY

Cars in the past used to have only a 12V charging plug and later a USB port with the same purpose plus audio broadcasting from a memory stick. Some of those models were subject to penetration and reverse engineering by going through internal communication channels connected to onboard multimedia systems.

More often, talking to the diagnostic port (On Board Diagnostic, OBD) already available even before USB was a very common and dangerous hack. Security measures at that time were rarely in place and limited to some weak obfuscation of exchanged information.

Software upgrade is an issue since before the 90s', but protection against forgery of binary images was not considered a big problem until recently. Today cars software upgrade go through Internet and Wireless, and it's far too easy to intercept and read or modify the code.

Repair shops and garages are places where stealing software code is still possible and often the case given the available computational power and secrets leaks, while modifying and uploading an unofficial binary image to a car should be prevented by integrity checks.

With the advent of connected vehicles that talk each other and with road signs it's now impossible to ignore the safety consequences of a hack.

New Regulations and Standards

Safety prescriptions for vehicles started being listed in an organic document with the first General Safety Regulation published on 2009. The European Commission drafted a completely new version of the General Safety Regulation (GSR) and published the final revision on 2019, as EU Regulation No. 2019/2144.
Among the consequences of the new GSR are:

1. New UN ECE Regulations on Components Introduced
2. New UN ECE Regulations on Occupant Protection Introduced
3. Scope of Existing UN ECE Regulations Expanded
4. New Features Requiring New Regulatory Requirements to be Developed

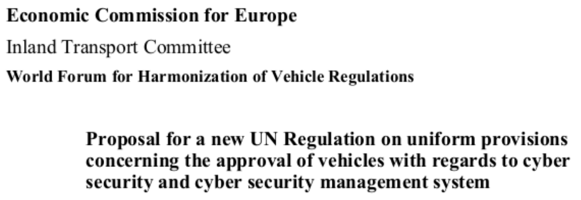
Given the deadlines included with the GSR, a lot of additional safety components need to be installed on newly developed vehicles starting 2022. Examples are:

- Advanced emergency braking systems (AEBS) capable of detecting vehicles, stationary obstacles, pedestrians and cyclists
- Revering cameras
- Emergency lane keeping systems
- Alcohol interlock
- Driver drowsiness and attention detection systems
- Driver availability monitoring systems
- Systems to replace the driver’s control
- Systems to monitor the area surrounding the vehicle
- Systems to provide safety information to other road users
- Communication systems and protocols for platooning
- Protection against cyber-attacks

The last requirement is very interesting: very detailed Cyber Security enforcing guidelines. These guidelines are better expanded in two subsequent regulations, published in final form as R155 and R156 during 2021.

R155:

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system



Economic Commission for Europe

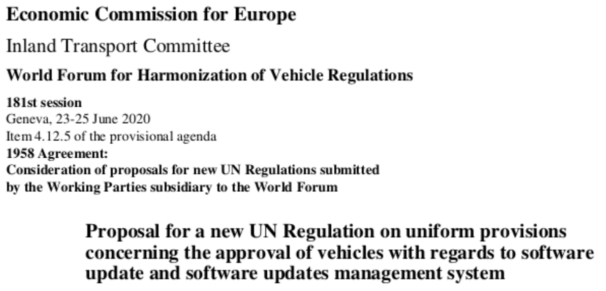
Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

R156:

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system



Economic Commission for Europe

Inland Transport Committee

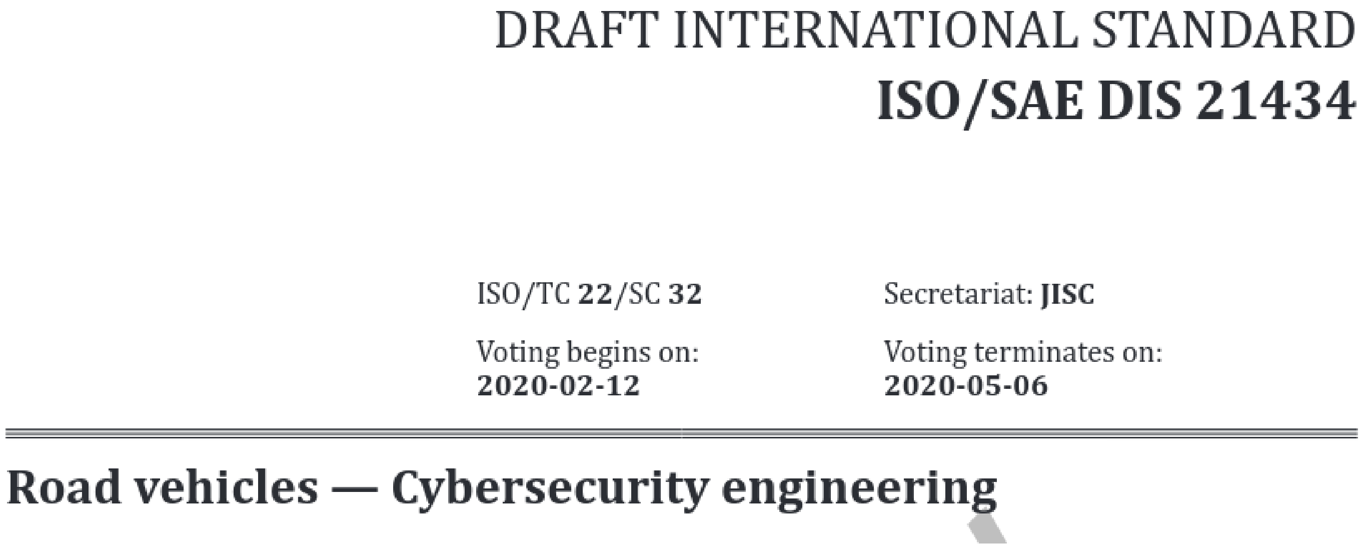
World Forum for Harmonization of Vehicle Regulations

181st session
Geneva, 23-25 June 2020
Item 4.12.5 of the provisional agenda
1958 Agreement:
Consideration of proposals for new UN Regulations submitted by the Working Parties subsidiary to the World Forum

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system

R155 and R156 consider the full lifecycle of a vehicle from the cyber security point of view. The *process* and not the *algorithms* or *implementations* is taken into account, similar to Functional Safety approach. The Engineering Standards ISO 26262-2018 (functional safety), ISO/PAS 21448 (safety of the intended functionality) and ISO/SAE 21434 (cybersecurity engineering) are explicitly recalled and suggested for adoption.

Special mention goes to ISO/SAE 21434: this is the brand new approach to cybersecurity engineering for vehicles, closely resembling ISO 26262-2018 and yet to be published in its final form, but already usable.



DRAFT INTERNATIONAL STANDARD
ISO/SAE DIS 21434

ISO/TC **22**/SC **32** Secretariat: **JISC**

Voting begins on: **2020-02-12** Voting terminates on: **2020-05-06**

Road vehicles — Cybersecurity engineering

Conclusions

Bluewind helps identifying gaps between the development process already in place and requirements of the regulations and standards. A plan for improvement can be elaborated on top of a gap analysis.

Bluewind is able to develop and adapt architectures and algorithms for cyber security, with a deep knowledge of the dedicated hardware today available on several automotive grade microprocessors and components.

About Bluewind

Bluewind, an independent engineering company, provides world-class products, engineering and software solutions in the domains of electronics, safety critical applications, and connected devices.
As a qualified researcher for Artificial Intelligence technologies, Bluewind is actively involved in designing next generation products in the Automotive, Industrial and Medical industries.

Bluewind Srl

Via della Borsa, 16/A - 31033
Castelfranco Veneto (TV) - Italy
+39 0423 723431 - info@bluewind.it