UNECE regulatory developments on Cybersecurity and OTA

Dr. Kai Frederik ZASTROW, Chairman of OICA Technical Committee

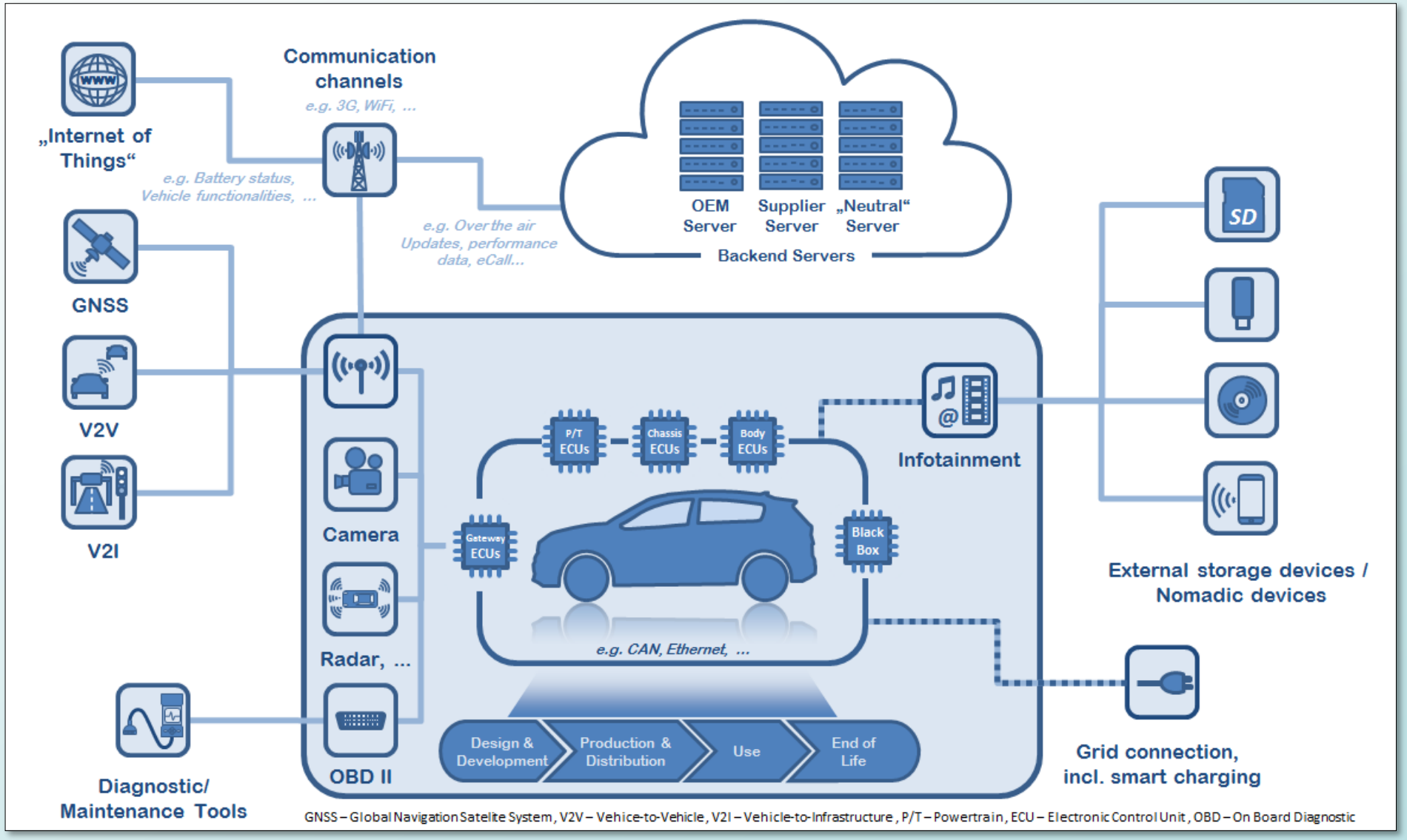
PSA GROUPE

Introduction

- Necessity of Software Updates
  - New functions and services of the **connected vehicle**
  - Necessity to update software on vehicles **during the whole vehicle life**
  - Some vehicle manufacturers (Tesla) make already SW updates OTA Over The Air in order to **add new ADAS functions** on **already registered vehicles**
- Risk of cyberattacks
  - Security impact: Hacker may get access to **private data** or may **manipulate** existing vehicle software
  - Safety impact: Hacker may use vehicle as weapon for **criminal actions** / terrorist attacks
  - Economic impact
    - Worldwide cybersecurity market: 3,1 billion € (2004), 67 billion € (2015) and 152 billion € (2020 forecast Gartner).
    - Automotive cybersecurity market: about 683 M € in 2023 (IHS Markit)
    - Example for economic risk: 1.4 M Jeep Cherokee recalled after successful attacks + cost of the class action which is still ongoing

Cybersecurity concerns the **whole vehicle**

Example for risks of unsecured access :



⇒ **Cybersecurity cannot be covered by certification of only some specific components**

Global Automotive Standards and Regulations to address Cybersecurity and SW updates

UN / WP.29 – World Forum for Harmonization of Vehicle Regulations

› Draft Proposal to introduce Regulations on Cyber Security and Software Updates

ISO TC22/SC32/WG11 - Cybersecurity

› ISO/SAE 21434 Cybersecurity Engineering

ISO TC22/SC32/WG12 – Software update

› ISO 24089 Software Update Engineering

National Discussions

› Germany VDA QMC

› UK BSI PAS 1885:2018

› …

European Union

› Cybersecurity Act

› General Data Protection Regulation

› NIS Directive

› Draft C-ITS Delegated Act

China

› Cybersecurity Law

› Encryption Law

› SAC/TC 114/SC 34/WG Cyber

Regulation American Market

› NHTSA Cybersecurity Guidelines

› Draft SELF DRIVE Act

› Draft AV START Act

=> The UN Regulations will be the first regulations worldwide on automotive Cybersecurity and SW updates

OICA created “Cluster 4” in order to follow the UN activities

Subgroup Cyber Security / OTA

Pilot: Kai Zastrow, PSA

Active members (attend UN + OICA meetings):

Mark Grainger, SMMT
Thomas Weiß, Stephan Ulrich, Carmen Venninger De Marco & Nupur Rakhe, Daimler
Erika Apro, Mazda
Jens Schenkenberger, Hyundai
Federico Guglielmone & Armando Mogavero, GM
René Nulens, Toyota
Tatsuya Ota, JAMA
Joao Pereira Lima, VW
Eva Meier, Audi

Members to be kept in info loop:

Yves van der Straaten & Olivier Fontaine, OICA
Joost Vantomme + Jocelyn DELATRE, ACEA
Paolo Alburno, Erik Vandervreken, CLEPA
Tim Vink, Honeywell
Tan Xu, CAAM
Thomas Goldbach, Opel
Torbjorn Andersson, Autoliv
Harry Lightsey, GM
Marko Gustke, VDA

Tech. Expert Group Cyber Security

Active members (attend UN + OICA meetings):

Shigeyuki Kawana & Hiroshi Honda, Toyota
Christian Urban-Seelmann, Wabco
Markus.Tschersich, Continental
Christophe Jouvray, Valeo
Jacques Kunegel, Actia / PFA
Robert Rohr, Matthias Hense, BMW
Alessandro Farsaci, IVECO
Dominique Roudink, Xin Ye, Catherine Keen, Ford
Jansson, Tania Ottebrink, Volvo Cars
Di Jin & Alan D Wist, GM
Rob Hare & Mitsuhiko Kikuchi, Nissan
Masahiro ODA, Denso
John Ellam & Steve McCabe, JLR
Alex Frost, Bentley
Jianzhong Huang, SAIC Motor
Markus Mitropoulou, Veoneer

Members to be kept in info loop:

Albert Held & Jan Waldmann, Daimler
Bernd Lutz, Sabir Idrees, Werner Mueller, Bosch
Pierre Gachon, Renault

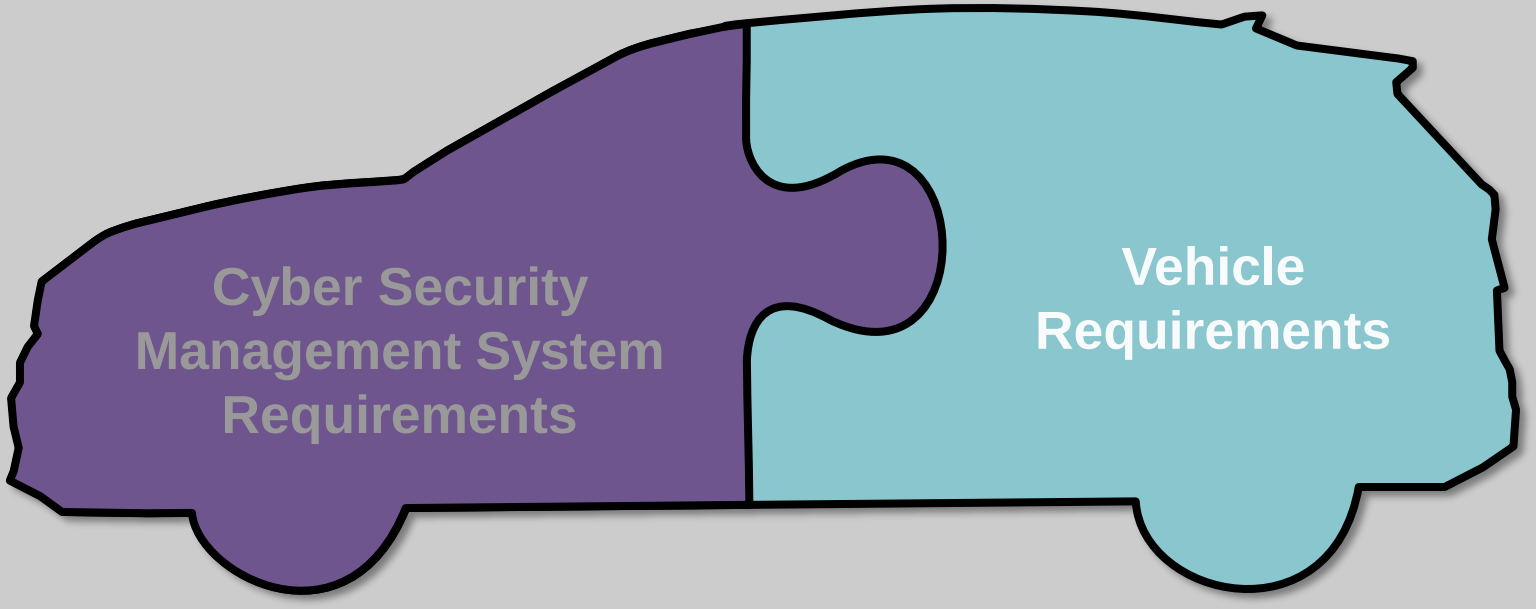
=> Large number of experts from manufacturers and suppliers all over the world.

UN Regulation on Automotive Cybersecurity

Split approach for the cybersecurity assessment:

i) Assessment and certification of vehicle manufacturer **cybersecurity management system**

ii) Assessment and certification of **vehicles**



Organizational structure & processes

Design of the vehicle EE architecture, risk assessment and implementation of mitigations

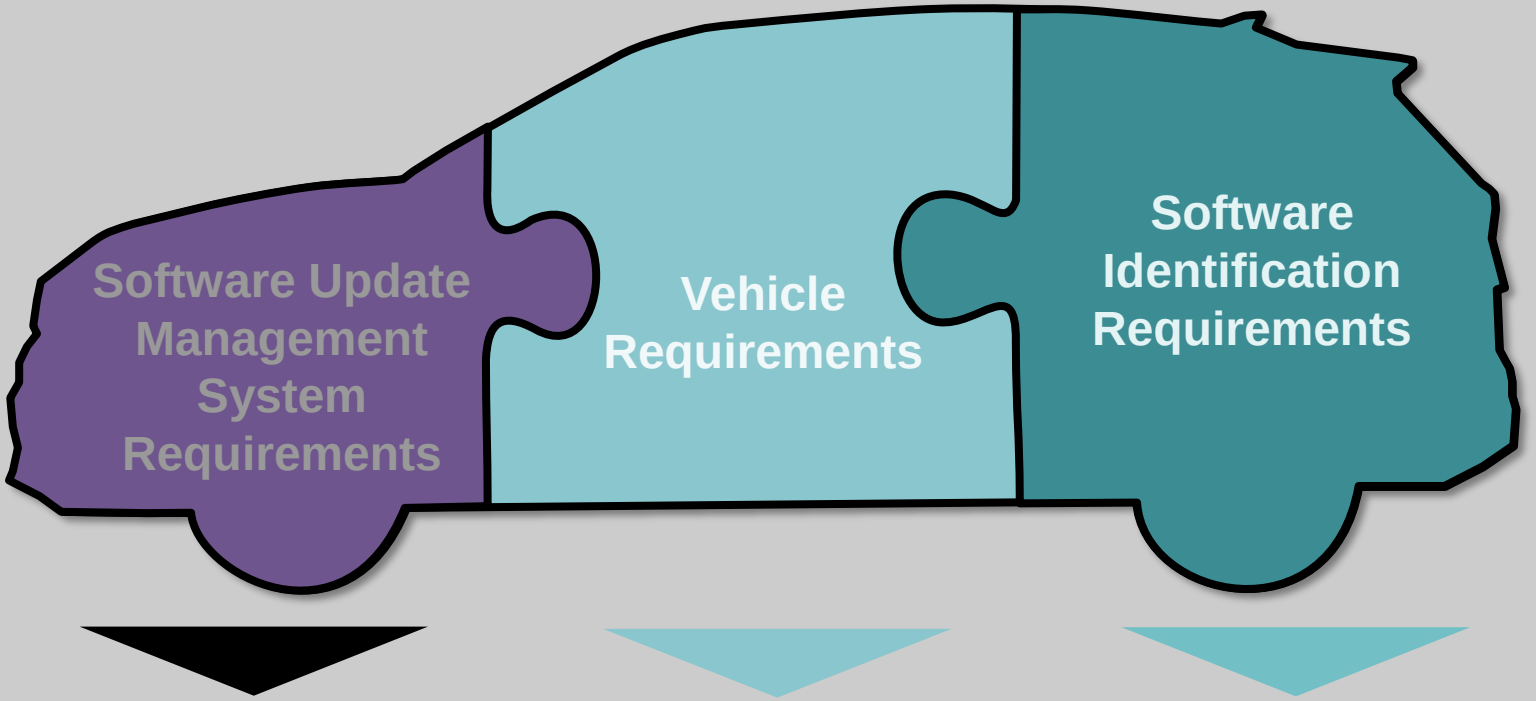
UN Regulation on SW updates

Split approach:

i) Assessment and certification of vehicle manufacturer **SW update management system**

ii) Assessment and certification of **vehicles**

iii) Implementation of **software identification number** for each regulation (RxSWIN)



Test Phase of draft UN Regulations

Scope: 2 draft UN Regulations on Cybersecurity and SW updates

Test phase:

- Participating Authorities / Technical Services:
  - France, Germany, Japan, Korea, Spain, The Netherlands, UK
  - DEKRA, Epoche, Idiada, RDW, Secura, TÜV Nord, TÜV Rheinland, TÜV Süd, UL, UTAC, VCA …
- Over **15 vehicle manufacturers** (of categories M and N)
- From February to August 2019

Aim:

- Verify the **robustness** of the **draft regulations** (not of the tested vehicles)
- Verify that **different approval authorities** / technical services **reach the same conclusions** for the **same vehicle manufacturer**

Results:

- Report on Test Phase (see WP29-179-24)
- Interpretation documents
- Draft amendments to current texts

=> The regulations work and will provide value

Milestones for implementation of UN Regulation

- Test phase with some authorities and some vehicle manufacturers to test and fine-tune the draft text — February – August 2019
- GRVA decision on content of the final text for UN Regulation — February 2020
- Formal adoption by UN WP.29 of the UN Regulation — June 2020
- Entry into force: legal act is available for application in UN Member States — December 2020
- Contracting Parties require those legal acts for whole vehicle type approval / whole vehicle certification
  - Japan - 2020 for automated vehicles SAE level 3 or higher
    - 2022 for all vehicles with Over The Air update capability
  - European Union - June 2022 for new EU Whole Vehicle Types
    - June 2024 for new registrations in EU
    - SW update regulation probably 1 year later (2023 / 2025)
  - Other countries (Korea (guidelines), Australia, Russia, etc.)

dates are estimations

=> Main challenge: Finalize the UN Regulation on time

OICA

Cybersecurity situation in China

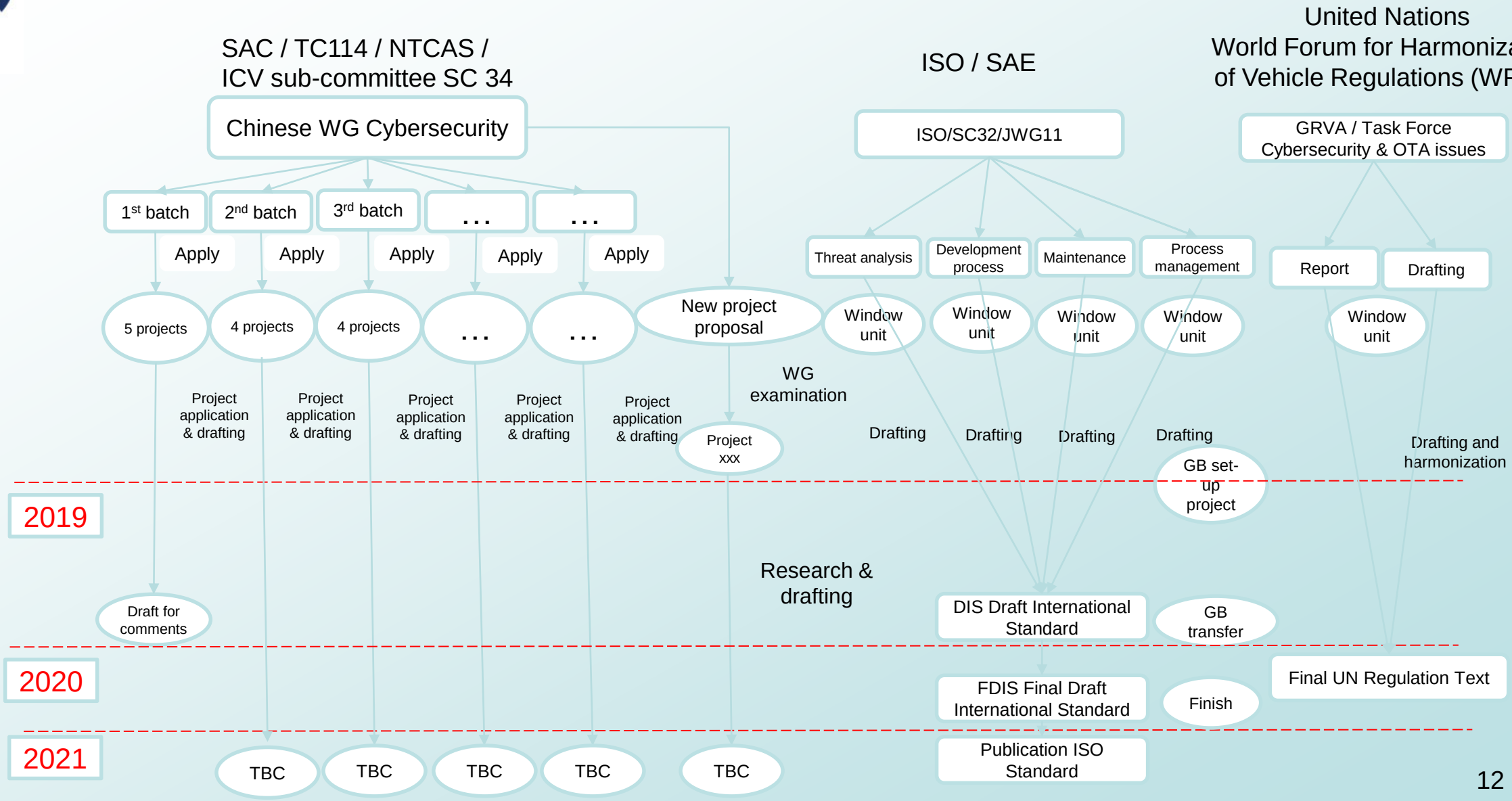
Exchange between Cluster 4 and Liaison persons of Chinese WG on Cybersecurity

Automotive Cybersecurity in Chinese ICV Standard System
(SAC / TC114 / NTCAS / ICV sub-committee SC 34 / WG Cybersecurity)

No.	Batch	Project	Status	Cluster 4 liaison participation						
				BMW	Continental	Daimler	PSA	SAIC	Valeo	VW
1	1st batch	General technical requirements for Cyber security of vehicle	Draft available	Y	Y	Y	Y	Y		Y
2		CyberSecurity Technical specifications of remote service and management system for electrical vehicle	Draft available			Y				Y
3		Information security technology requirements of on-board information interactive system	Draft available							Y
4		Information security of automobile gateway	Draft available					Y		Y
5		Technical requirements for information security of electric vehicle charging system	Draft available			Y				Y
6	2nd batch	Information security technology requirement of OBD				Y		Y		
7		Technical requirement of	Pre-research		Y	Y		Y		
8		Guid… management of automobile	Pre-research	Y						Y
9		Specification for risk assessment of vehicle information security	Pre-research					Y		Y
10	3rd batch	Test method of vehicle information safety	Pre-research	Y		Y				Y
11		Road vehicles – Cybersecurity engineering (adoption of ISO 21434)	Pre-research			Y	Y		Y	Y
12		Requirements for standardization of onboard computing platforms research	Pre-research		Y		Y			Y
13		Technical requirements for information safety of on-board ECU	Pre-research		Y					Y
Etc.						Y				

New Cybersecurity list with 28 standards under preparation by CATARC

Cybersecurity Working Groups



OICA

Opportunities for global harmonization

What will happen after adoption of the two UN Regulations in 2020?

- Make sure that 54 signatory countries of 1958 Agreement apply the UN Regulations (and do not invent national requirements)
- USA requested UN TF to extract a list of requirements that may be used for countries outside 1958 Agreement
- China has started the drafting of 13 national cybersecurity standards, in total 28 standards foreseen …

THANK YOU FOR YOUR ATTENTION!

Link to the latest draft versions

Draft versions after Tokyo meeting of UN TF (12-14 November 2019)

UN Regulation on Cybersecurity: TFCS 16-31rev1

UN Regulation on Soft Updates: TFCS 16-34rev1

Access to vehicle data and Cybersecurity

- CITA International Motor Vehicle Inspection Committee
- EGEA European Garage Equipment Association
- ETRMA European Tyre & Rubber Manufacturers
- FIA Fédération Internationale de l'Automobile
- FIGIEFA Federation of Independent Automotive Parts Distributors

- Those stakeholders use the UN Task Force on Cybersecurity in order to introduce new requirements that the vehicle manufacturer shall give access to the data on vehicles for authorized persons.

- The UN Task Force has clarified in the scope of the Regulation that it is without prejudice to other regulations governing access to data or data protection.

Summary: Cybersecurity defines requirements for the lock system but not who gets the key!

Liaison persons
Cluster 4 – Chinese WG on Cybersecurity

Company	Member of Cluster 4	Member of Chinese WG
BMW Group	Maja Luick	Wang Zhe Zhe.WA.Wang@bmw.com
Continental	Markus Tschersich	Estelle WANG estelle.wang@continental-corporation.com
Daimler	Carmen Venninger de Marco	Lv MING Ming.lv@daimler.com
PSA Group	Kai Frederik Zastrow	Zhimin FENG zhimin.feng1@mpsa.com
SAIC	Jianzhong Huang	Li QiuShi liqiushi@saicmotor.com
Valeo	Christophe Jouvray	Hequan Yang hequan.yang@valeo.com
Volkswagen Group	João Pereira Lima	Wen ZHAO Wen.Zhao@volkswagen.com.cn