RDW

CARTRE
Coordination of Automated Road Transport Deployment for Europe

RDW on safety and security
UNECE taskforce on CS/ OTA

Geert Pater

Hari Sankar Ramakrishnan

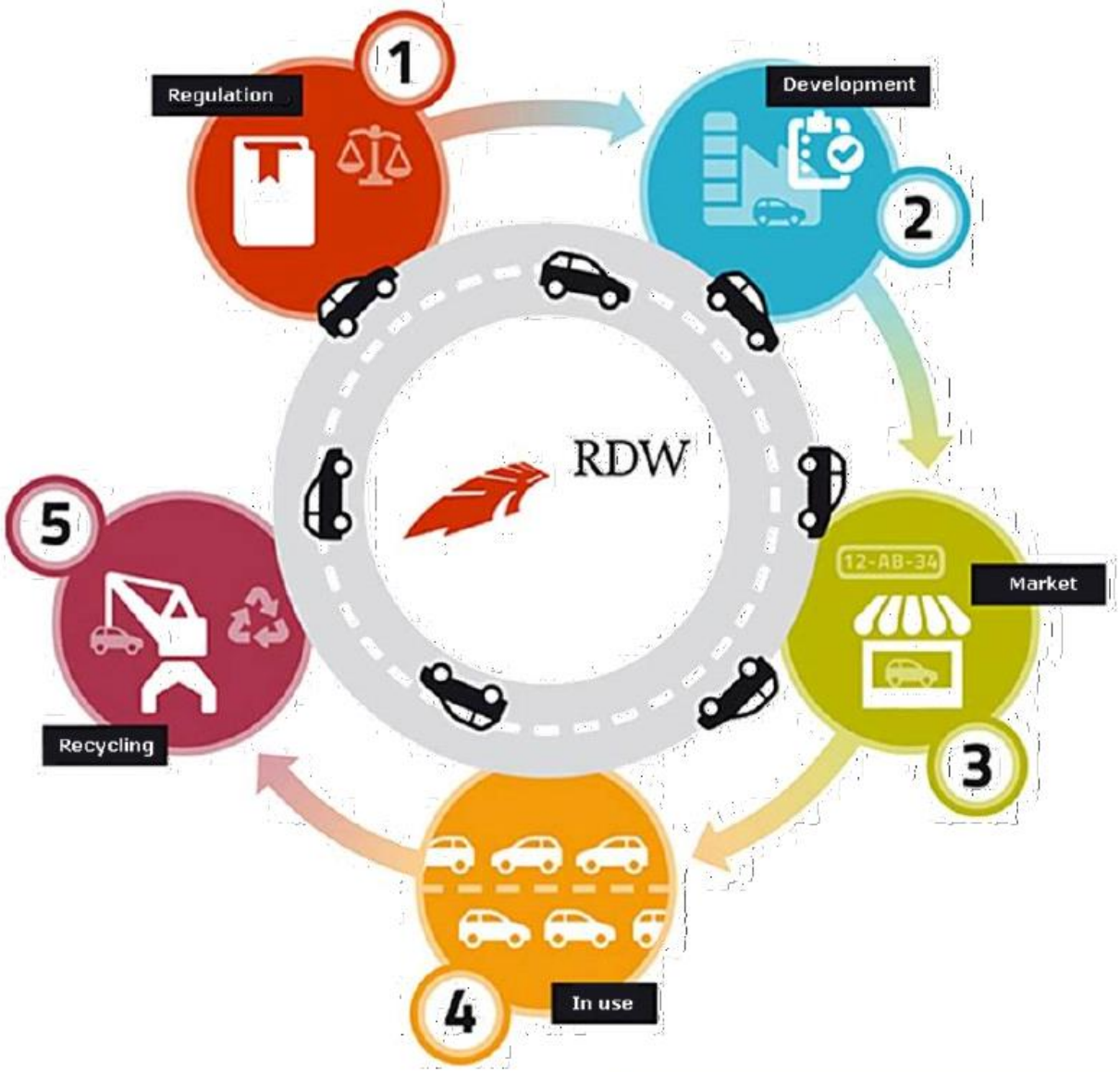
5 December 2017

RDW

About RDW

RDW is the Netherlands Vehicle Authority in the mobility chain. RDW has developed extensive expertise through its years of experience in executing its statutory and assigned tasks. Tasks in the area of the licensing of vehicles and vehicle parts, supervision and enforcement, registration, information provision and issuing documents. Tasks that RDW carries out in close cooperation with various partners in the mobility chain.
This provides RDW with a clear position in this chain, where it operates as a partner that stands for safety, sustainability and legal certainty in mobility.

RDW's field of work



RDW

RDW

- Type Approval
- Oversight and Control
- Registration and information provisioning
- Issuing documents

RDW erkend
www.rdw.nl

RDW

Examples we bring forward in this Webinar on the things we do to help innovation forward.

There are a lot of activities we are active in or where we are contributing like:

- High secure identity management (National and EU)
- Privacy on high private registration based on the General Data Protection Regulation
- Open Data
- Current and Future Vehicle regulations in UNECE and/or EU
- We contribute to design new standards in cooperation with ISO, ETSI and NEN
- Testing and Experimenting with ITS trials
  (https://www.rdw.nl/information-in-english/intelligent-transport-system)
- ……..

In this Webinar we will highlight 2 actions we contribute on the subject Security:

- We perform “Learning Audits” with OEM’s (on voluntary basis)
- We contribute very intensely in a UNECE Taskforce on Cybersecurity and Over The Air Updates

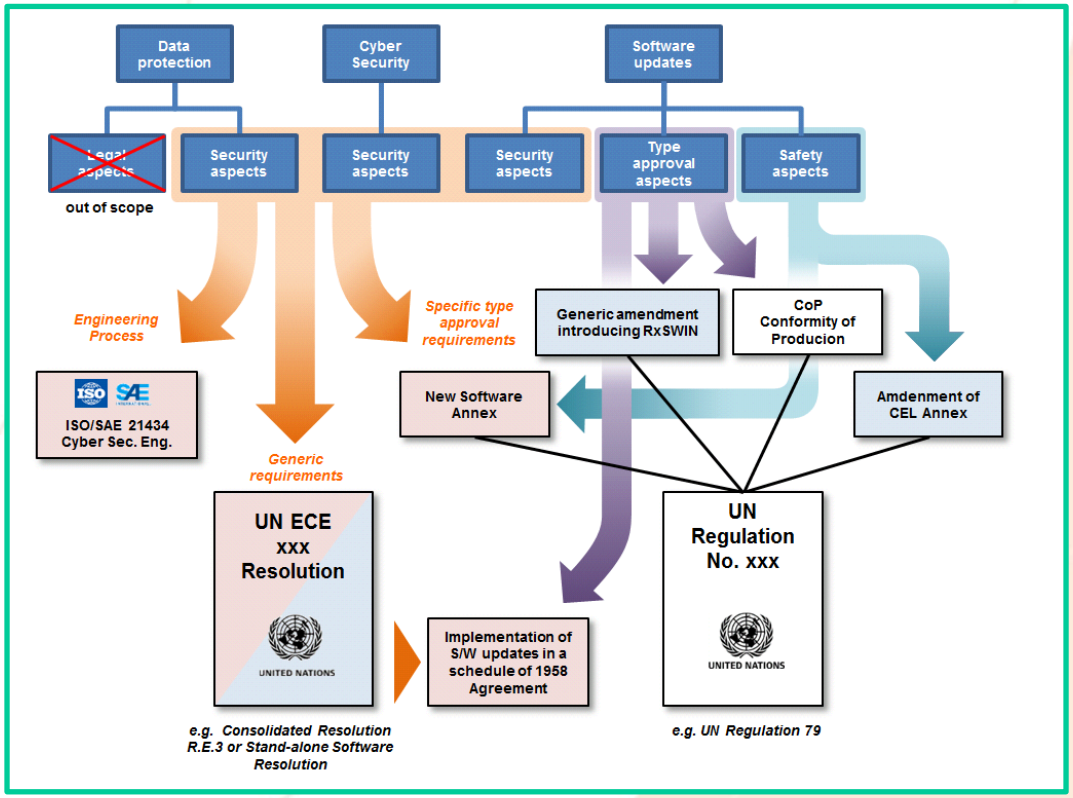
RDW

Overall Structure Learning Audit Basic Framework

RDW

Overview of UNECE TFCS

- Taskforce on Cybersecurity and software updates set up under the ITS/ AD working group under WP 29
- Established since December, 2016
- Physical meeting once every 2 months to evaluate the work process
- Currently drafting working papers on Cybersecurity and software updates

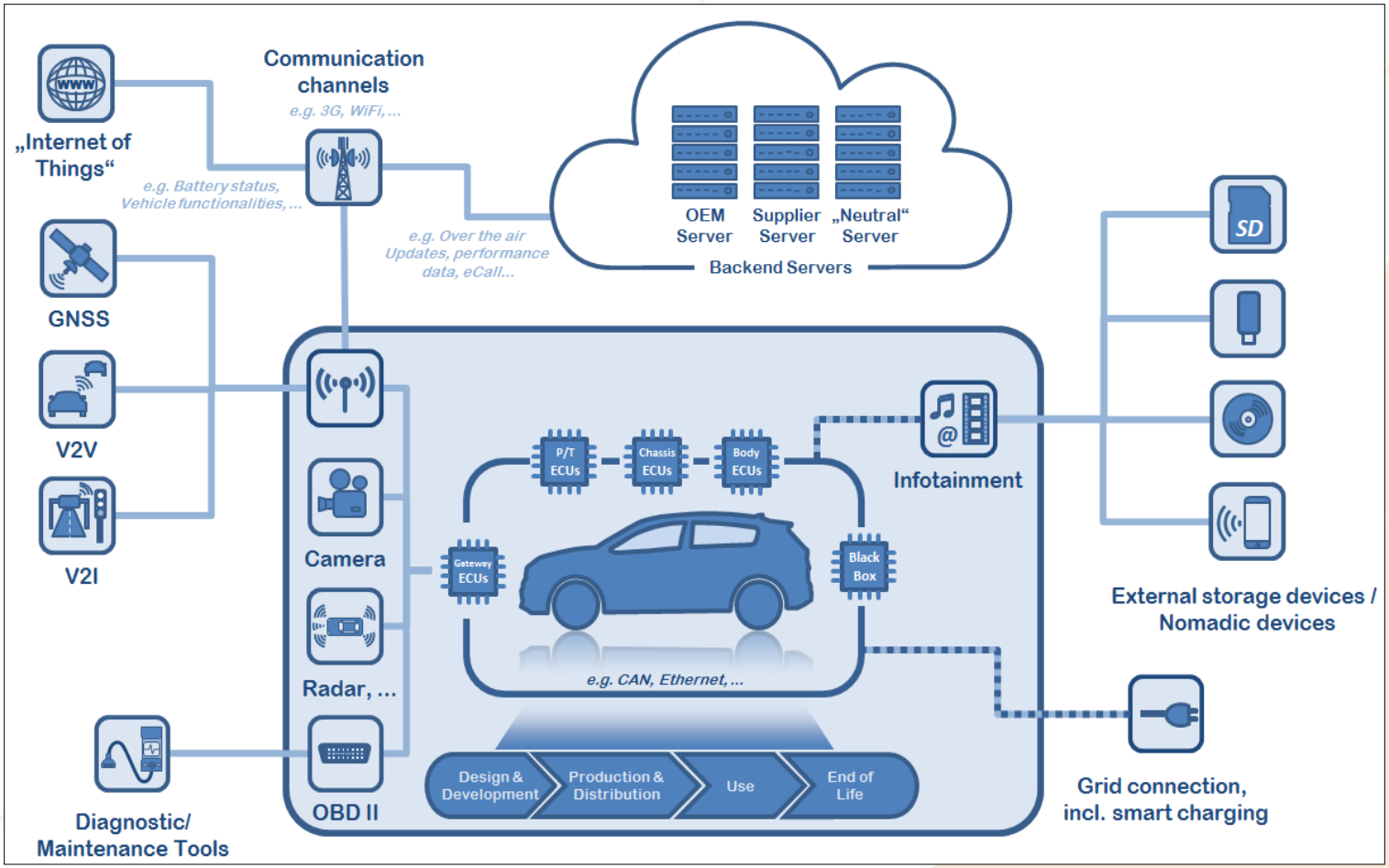


- Upcoming meetings in January and February, 2018 to finalize the contents drafting paper
- Final deliverables expected by mid 2018.

RDW

Cybersecurity

Reference model to identify threats and mitigation measures



RDW

Cybersecurity

- **Cybersecurity principles**
  - Applicable to Vehicle manufacturers, suppliers, sub contractors and suppliers
  - Expected to adhere to these principles and provide evidence for demonstrating the same to the approval authorities
  - The identified principles include:
    - Organization Principles
    - Design principles
    - Data Protection principles
    - Response principles
    - Verification principles

- **Threat Landscape**
  - TF group identified a list of 81 threats and corresponding mitigation measures
  - Mitigation measures prescribed as high level technology agnostic solutions
  - Security controls detailing how the mitigation measures can be implemented- Included as Annex in the working paper
  - Product design to use the threats and mitigation measures as a basis for ensuring security risks are adequately mitigated.
  - To be use complementary to industry standards to demonstrate product resilience from cybersecurity risks.

Software Updates

Software updates w.r.t. current approval process

Moment of update	No impact on type approval	Limited impact on type approval	Severe impact on type approval
Initial type approval (TA)	Not applicable	Not applicable	Not applicable
Existing TA, before Certificate of Conformity (CoC)	No action	Extension TA	New TA
Existing TA, after CoC, before registration	No action	Extension TA and new CoC	New TA and new CoC
Existing TA, after registration, by OEM	No action	Extension TA or individual approval or approval with limited scope. Registration according to national rules	New TA or individual approval or approval with limited scope. Registration according to national rules
Existing TA, after registration, not by OEM	New National approval. Registration according to national rules	New National approval. Registration according to national rules	New National approval. Registration according to national rules

RDW

Software Updates

- Process for managing software updates to use the existing procedures under UN legal framework
- Software update changes to be assessed based on its impact on the existing type approval requirements.
- For third party updates that are outside the control of the manufactures(and its supplier), the 3rd party is responsible for initiating the approval according to national laws.
- National bodies can use methods like electronic CoC/ DoC for sharing type approval requirements regarding updates across borders.
- For urgent updates, manufactures needs to make an informed and risk based decision regarding issuing an update before a complete verification of the update is done.

RDW

Software Updates

- Software updates to be administrated based on:
  - Configuration control requirements
  - Quality control requirements

- Manufacturers are required to demonstrate that they have a process for:
  - Documenting H/W and S/W components of a system and its interdependencies
  - Identifying the effect of S/W updates on existing type approval
  - Identify target vehicles impacted by the update
  - Compatibility of update w.r.t. to components/ systems in target vehicles
  - Traceability of software updates using an identifier(Rx SWIN)

- Additional requirements were also identified for update delivery and execution :
  - Safely requirements for updates
  - Securely requirements for update
  - Role of driver during software update

- Requirements were also drafted for identification of software updates:
  - Rx SWIN- Regulation X software identifier number
  - Unique Identifier for each regulation(type definition) impacted by a software update
  - Reference made in every regulation which can be impacted by software update
  - Rx SWIN to be read from vehicle during PTI and market surveillance to verify whether type approved update is present in the vehicle.

RDW

Future work

- The taskforce group aims to identify topics within the context of software regulations in vehicle that may require more detailed requirements to be drafted .This includes topics like software validation , software quality, machine learning etc.

- The current developments within the taskforce needs to be considered as a “work in progress” item with further developments to be expected in the coming months.

- The latest versions of the draft paper on cybersecurity and software updates can be accessed from the below links:
    - Cybersecurity- https://wiki.unece.org/download/attachments/51971917/TFCS-09-14%20%28Sec%29%20Draft%20paper%20on%20Recommendations%20for%20Cyber%20Security%20-%20status%20after%20TFCS-09%20incl.%20new%20format%20and%20numbering.docx?api=v2
    - Software Updates- https://wiki.unece.org/download/attachments/51971917/TFCS-09-15%20%28Sec%29%20Draft%20paper%20on%20Recommendations%20for%20Software%20Updates%20-%20status%20after%20TFCS-09%20incl.%20new%20format%20and%20numbering.docx?api=v2
- The taskforce documents are publicly available for reference and can be accessed from the link:
  https://wiki.unece.org/pages/viewpage.action?pageId=40829521

RDW