Regulating cyber and software
Dr Darren Handley

Content

▸ Addressing the cyber challenges

▸ The need for international action

▸ Developing regulation under the UNECE

▸ Future challenges

The cyber challenge

V

UNECE task force on cyber security and software updates

▶ The UK believes that regulatory action should be taken at the UN to harmonise the approach globally.

▶ The UK co-chair a task force with JPN and USA. Its aims are to:

   ▶ Define requirements and legislation for addressing cyber threats

   ▶ Define requirements and legislation for managing software updates, particularly with respect to maintaining safety type approvals

▶ Regulations R155 (cyber security) and R156 (software update processes)

   ▶ Will ensure vehicle manufacturers can design secure vehicles and maintain them when in service

   ▶ Came into force in Jan 2021

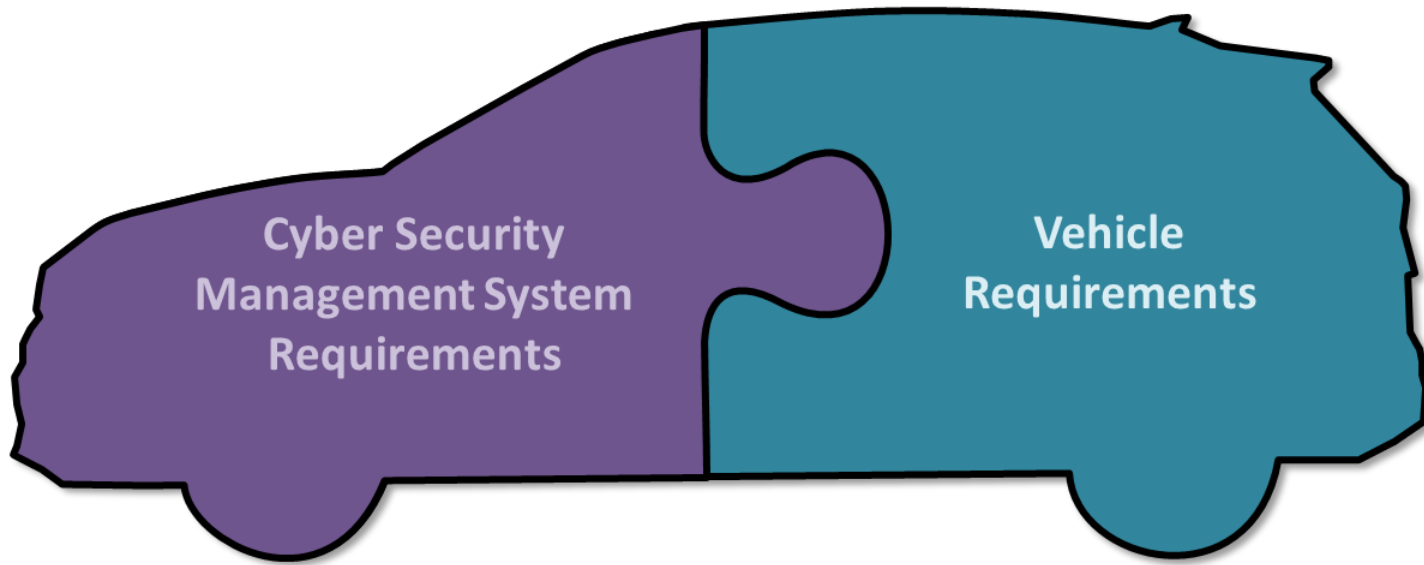   ▶ Has supplementary interpretation documents to further aid harmonisation

The vehicle ecosystem
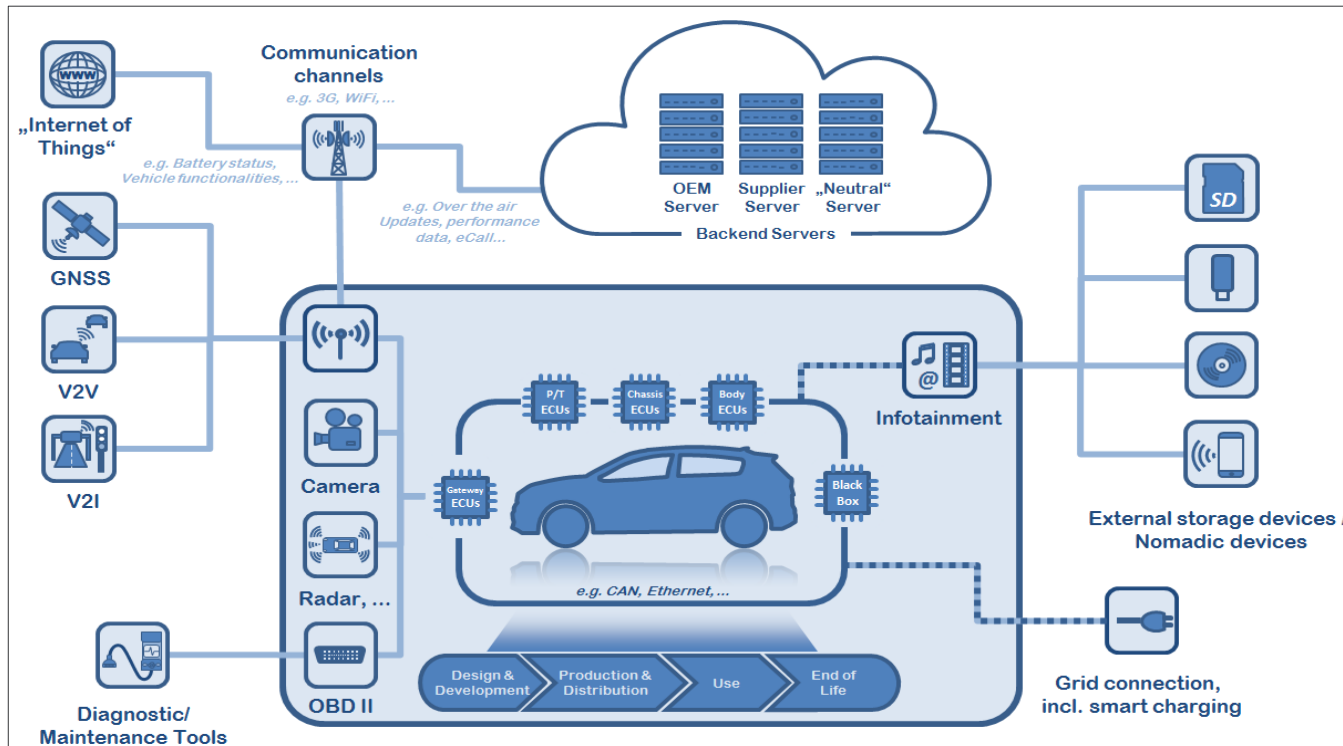
R155, the cyber security regulation

Cyber Security Management System Requirements
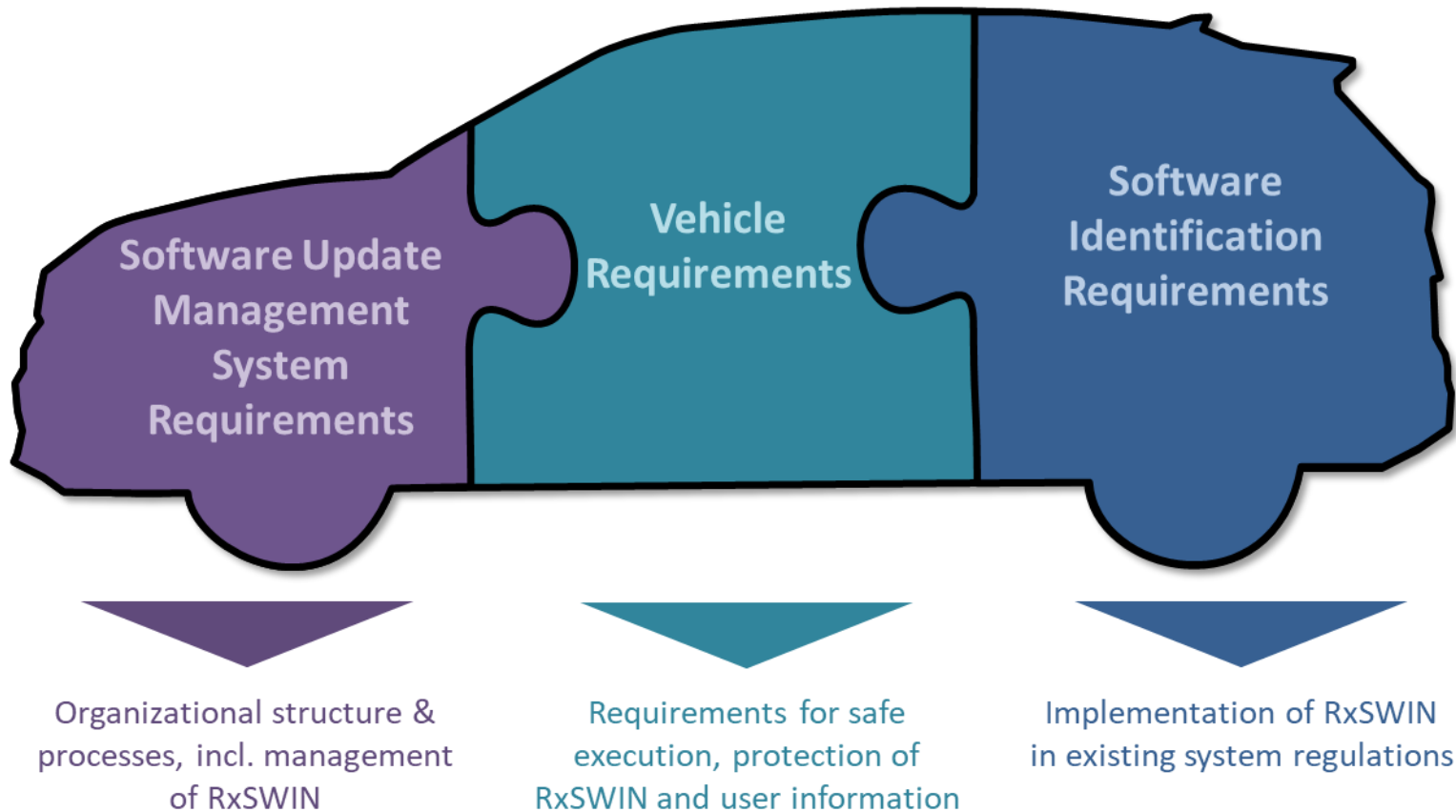
Vehicle Requirements

Organizational structure & processes

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

R156, the software update process regulation

Conclusions

▸ The regulations are based on the principle of risk-reduction not risk-elimination.

▸ They cover all levels of automation and all types of software updates

▸ Focus is on the vehicle but requires external risks to be considered and, where appropriate, mitigated in the vehicle design

▸ Software updates are here and having secure and verifiable processes for delivering them is key to their continued utilisation.

Questions…