Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for
Security and Safety

Guido Gluschke

KEYNOTE SESSION 2
Vehicle cybersecurity framework is ready: It's time for deployment

Future Networked Car, 22-25 March 2021

Institute for Security and Safety (ISS)

Scientific institute at the Brandenburg
University of Applied Sciences in Germany

Area of expertise: cyber security in energy and automotive

Involved in international activities on cyber security:

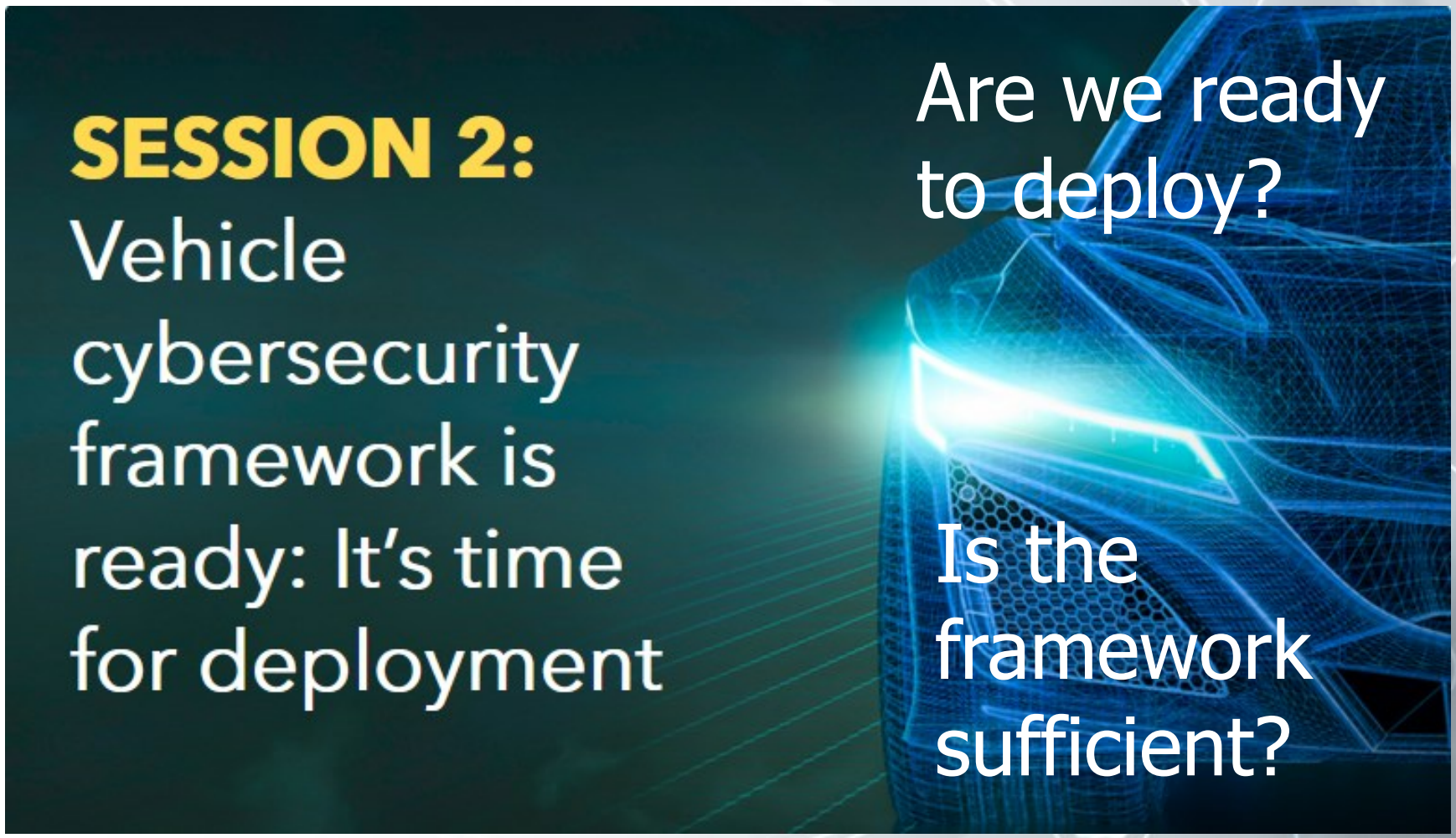
- In consultative status with the UN, e.g. OEWG, UNECE, ITU
- Center of Excellence of the ITU Academy
- Member of the IAEA Nuclear Security Education Network
- Member of the EU CyberNet
- Member of European Energy Cyber Security Platform
- Member of European Energy Information Sharing and Analysis Center
- Member of WG on Cyber Security at the World Economic Forum
- Member of WG on Cyber Security at Chatham House

Research & Development

Education & Competence Building

Dialogue & Advice

Vehicle Cybersecurity Framework

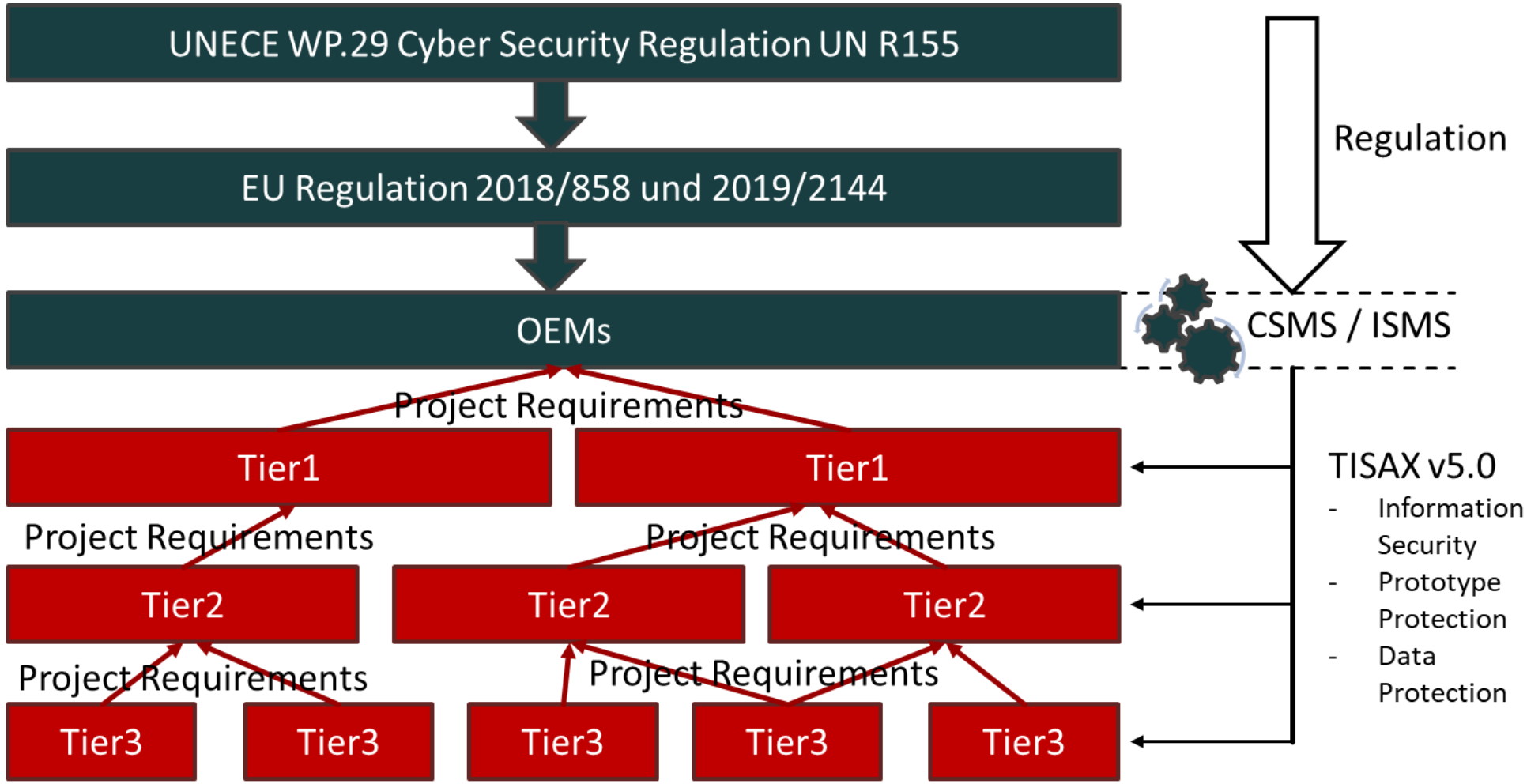


Vehicle Cybersecurity Framework

Security Domains In Light Of UN R155

Business Security	Security & Risk Management Human Factor Secure Engineering & Projects Physical & Prototype Protection Threat & Vulnerability Management Secure Supply Chain	Secure Software Development Secure Hardware Development Secure Diagnostic Systems Secure In-Car Components Secure V2X Communication Secure Backend Systems	Product Cyber Security
Business IT Security	Secure Data Processing/Data Center Secure IT Projects Secure IT Operation Secure IT Systems & Platforms Secure Applications & Cloud Secure Network & Communication	Secure Production Environment Secure Data Processing Secure Data Center Secure Automation Secure OT Operation Secure Network & Communication	Production OT Security

Implementing UN R155



Skills, Competences And Methodologies For UN R155

"Competent personnel with appropriate cyber security skills and specific automotive risk assessments knowledge" (UN R155)

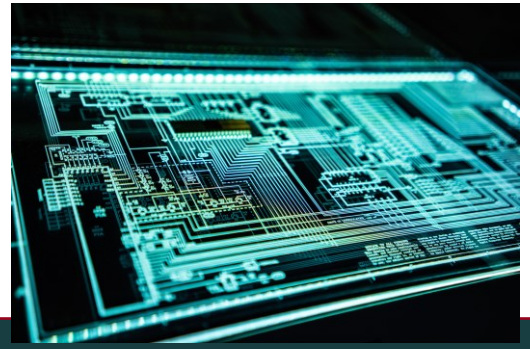
B1	Mitigation to the threats which are related to "Vehicle communication channels"	
M6	Security by design	Systems shall implement security by design to minimize risks.
M7	Protection of system data/code	Access control techniques and designs shall be applied to protect system dat
M8	System design and access control	Through system design and access control it should not be possible for unaut
M9	Prevention and Detection of unauthorized access	Measures to prevent and detect unauthorized access shall be employed.
M10	Authenticity and integrity of messages	The vehicle shall verify the authenticity and integrity of messages it receives.
M11	Storage of cryptographic keys	Security controls shall be implemented for storing cryptographic keys
M12	Confidential data	Confidential data transmitted to or from the vehicle shall be protected.
M13	Detection and Recovery denial of service attack	Measures to detect and recover from a denial of service attack shall be empl
M14	Embedded viruses/malware	Measures to protect systems against embedded viruses/malware should be
M15	Detection of malicious internal messages or activity	Measures to detect malicious internal messages or activity should be conside

Highly sophisticated cyber security requirements should result in competence analysis and in development of appropriate methodologies

Vehicle Cybersecurity Framework

Scoping Of Cyber Security Regulation

Hardware



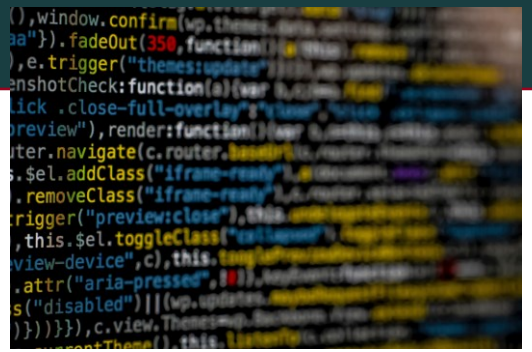
Supply Chain

Development

Production

Smart City

V2X-Communication



Software

Post-Production

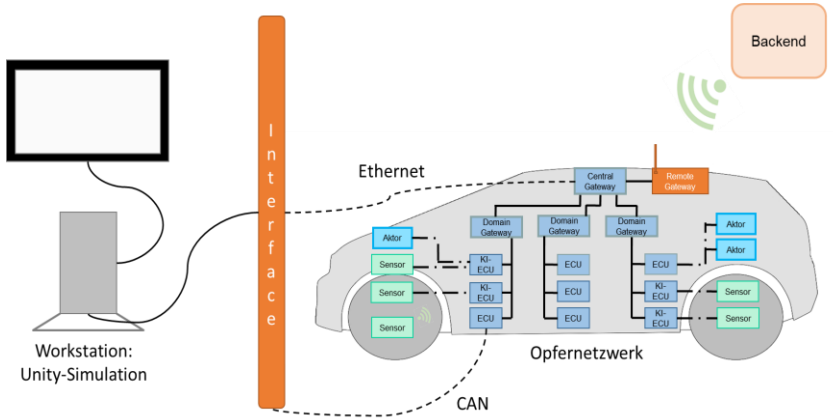
Charging Infrastructure

Ensuring Security And Safety By Holistic And Strategic View

State‘s Responsibilty	Cyber Norms and Protection against cyber terrorism/war
Manufacturer‘s Responsibilty	Secure product, vulnerability monitoring and incident handling
Operator‘s Responsibilty	Secure operation and data protection
Driver‘s Responsibilty	Correct user behaviour

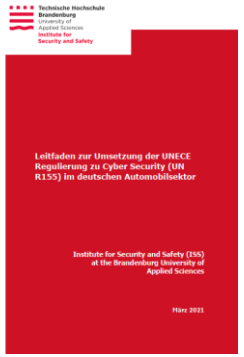
Actions Needed For Cyber Security Readyness And Sufficiency

- Research on generic digitalized Vehicle E/E Architecture for development, testing, training and monitoring along UN R155 (Digital Twin on Automotive Cyber Range)



- Capacity Building in Automotive Security and Curriculum Design along UN R155

- Guidance for implementing UN R155, in particular for the supplier
- Multistakeholder dialog on cyber in the vehicle ecosystem
- International initiatives on security and sustainability in cyber



Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for
Security and Safety

Feel free to contact us:

Guido Gluschke
g.gluschke@uniss.org
www.uniss.org