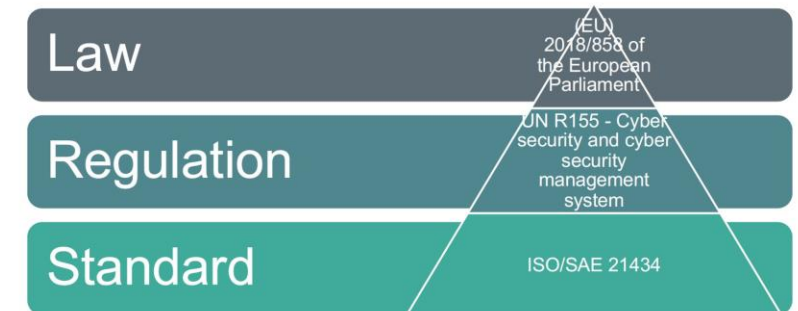## Talk 1: Christoph Schmittner ATI, AT

Automotive Cyber-Security – from standards to regulations

- Vehicular security

- Regulations (mandatory) vs.standards (not mandatory)

- Global view of automotive Cybersecurity (CS) regulations – interesting world map

- UN R155 CS and CS management system (CSMS)

- CSMS from R155 to ISO/SAE 21434 and ISO PAS 5112

- Divide between experts in security, experts in automotive

- Vehicle type cybersecurity

- ISO/SAE 8475

  - Cybersecurity Assurance Levels (CAL) and Target Attack Feasibility (TAF)

- CS of items does not imply CS of architecture

- Several enjoyable Charllie Ciso cartoons

UN R155 CYBER SECURITY AND
CYBER SECURITY MANAGEMENT SYSTEM

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Law	(EU) 2018/858 of the European Parliament
Regulation	UN R155 - Cyber security and cyber security management system
Standard	ISO/SAE 21434

Talk 2: Qi Alfred Chen, UC Irvine, US

Cyber-Attacks Against AI Stack in Autonomous Driving and Intelligent Transportation

- AI stack: Brain for AD

- Cyber attack on AD (automous driving) and V2X

Today: Cyber-attack surface to AD & V2X-based transp. AI

V2V (vehicle-to-vehicle)

GPS

Cooperative Driving Automation (e.g., platoon)

V2I (vehicle-to-infrastructure)

AD vehicle

Intelligent traffic light
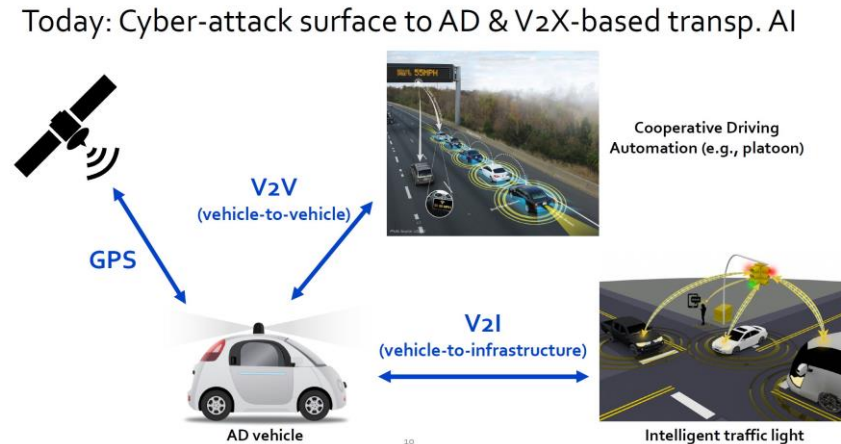
- First automatic vulnerability discovery methodin CV protocols using *model checking*

- Results

2

Discussion

Balanced well between the two talks

- Questions concerning

- Model checking

- Need for analysis by engineers to support statndards

- Cybersecurity and Safety – To what extent dependent?

This was questioned and discussed more than other topics

■

Definition of (Road Vehicle) Cybersecurity per ISO/SAE 21434:2021

3.1.9
cybersecurity
road vehicle cybersecurity
condition in which *assets* (3.1.2) are sufficiently protected against *threat scenarios* (3.1.33) to
items (3.1.25) of road vehicles, their functions and their electrical or electronic *components*
(3.1.7)
Note 1 to entry: In this document, for the sake of brevity, the term cybersecurity is used instead of
road vehicle cybersecurity.

3.1.2
asset
object that has value, or contributes to
value
Note 1 to entry: An asset has one or more
cybersecurity properties (3.1.20) whose
compromise can lead to one or more
damage scenarios (3.1.22).

3.1.33
threat scenario
potential cause of
compromise of *cybersecurity
properties* (3.1.20) of one or
more *assets* (3.1.2) in order to
realize a *damage scenario*
(3.1.22)

3.1.25
item
component or set of
components (3.1.7) that
implements a function at the
vehicle level
Note 1 to entry: A system can
be an item if it implements a
function at the vehicle level,
otherwise it is a component.

3.1.7
component
part that is logically and
technically separable

3.1.20 cybersecurity property
attribute that can be worth
protecting
Note 1 to entry: Attributes include
confidentiality, integrity and/or
availability.

3.1.22
damage scenario
adverse consequence involving
a vehicle or vehicle function
and affecting a *road user*
(3.1.31)

3.1.31
road user
person who uses a road
EXAMPLE Passenger, pedestrian,
cyclist, motorist, or vehicle owner.