HTW D
Hochschule für Technik und
Wirtschaft Dresden
University of Applied Sciences

5G as part of secure V2X Communication

Mobile Communication:

14.05.2025

Prof. Dr.-Ing.
Julia M. Engelbrecht
Faculty Electrical Engineering
HTW Dresden
Germany

Control Questions

Differences between IEEE802.11p and C-V2X?

- …

Different Configuration principles of C-V2X?

- …

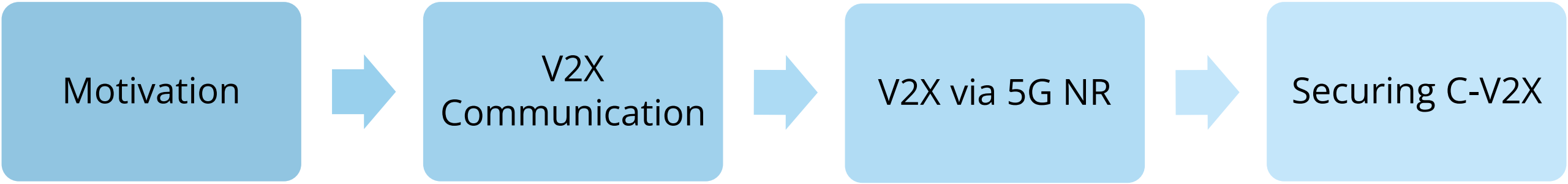
Key security measures of C-V2X?

- …

Unified Standards for C-V2X (why and how)?

- …

Overview of Lecture



Motivation

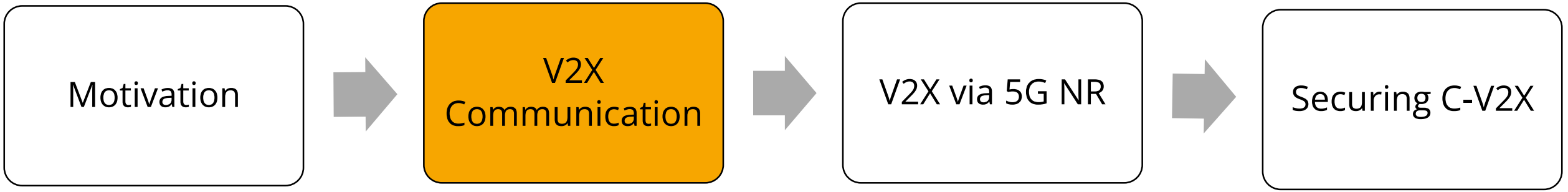
Do you know any fields from the smart city context?

- according to UN statistics of 2023: 57% of the world's population live in cities
  - Problems and Challenges due to dense coexistence of people
  - e.g. traffic is increasing
- Industrialisation and digitalisation continue to advance

→ Automation technology can provide a remedy

- **Smart city**
- Sensor data as a basis

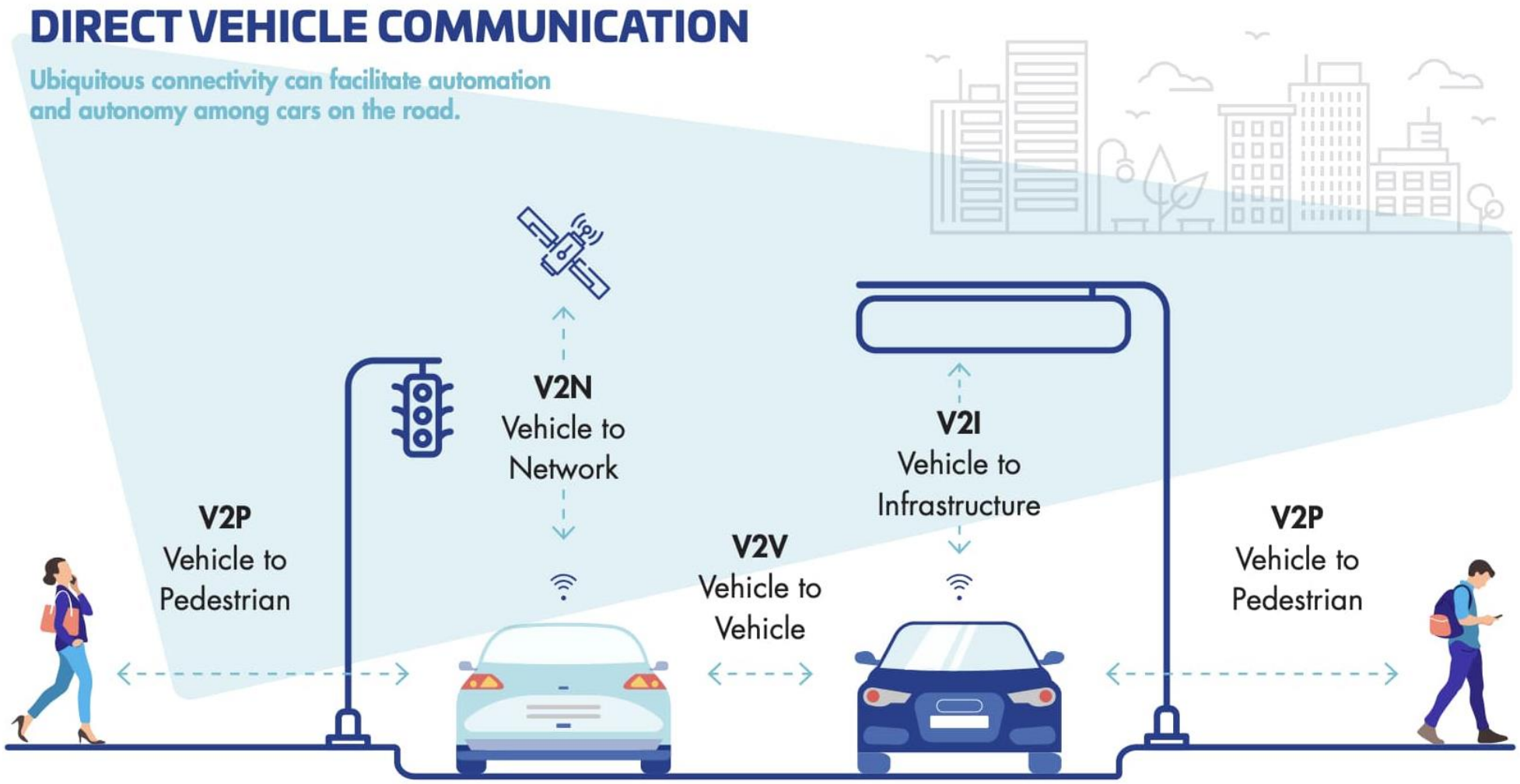
Overview of Lecture



V2X-Communication

Adhoc Network	MANeT	VANet

V2X-Communication



©https://www.thalesgroup.com/sites/default/files/database/assets/images/2020-12/v2X.jpg

V2X-Communication

Aspect	Onboard Unit (OBU)	Roadside Unit (RSU)	Infrastructure
Location			
Function	Sends/receives V2X messages (V2V, V2I, V2P)	Broadcasts messages to/from vehicles and infrastructure	Oversees data processing, traffic coordination, and cloud services
Primary Role	Provides real-time vehicle communication & situational awareness	Serves as intermediary between vehicles and central systems	Enables large-scale traffic management and decision-making
Connectivity	Connects to other OBUs, RSUs, pedestrians	Connects to OBUs and backend systems (via wired or wireless links)	Connects to RSUs and cloud/edge computing infrastructure
Mobility			

V2X-Communication: Use cases

Collision avoidance

- e.g.

Traffic management

- e.g.

Emergency warnings

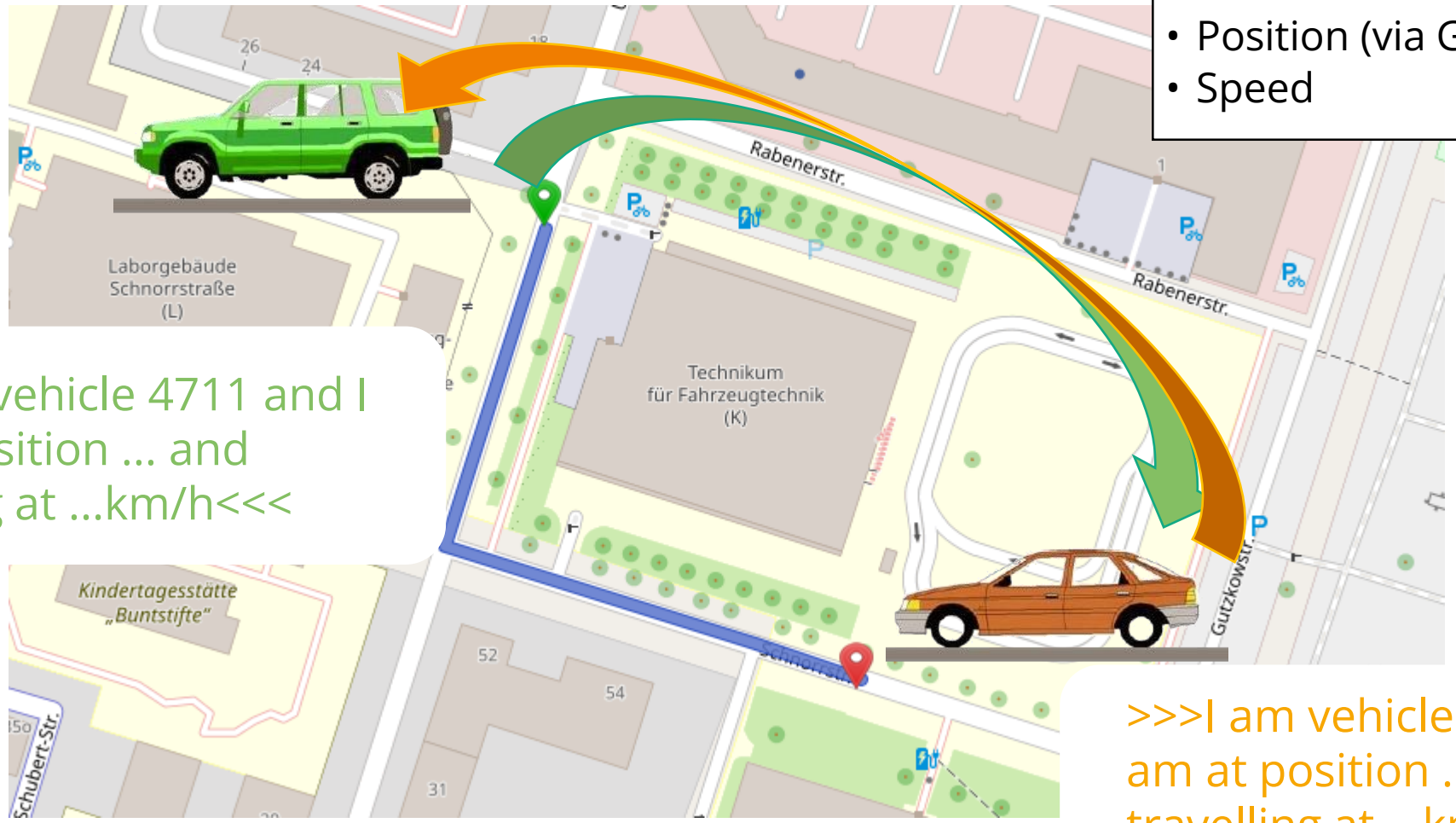
- e.g.

Communication with pedestrians & infrastructure

V2X-Communication: Message Types

Cooperative Awareness Message (CAM)

- Vehicle ID and Type
- Position (via GPS)
- Speed



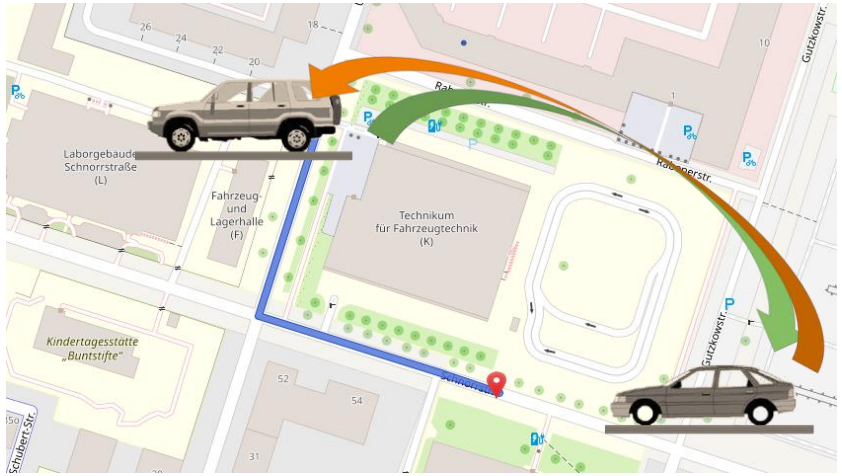
>>>I am vehicle 4711 and I am in position … and travelling at …km/h<<<

>>>I am vehicle 12345 and I am at position … and travelling at …km/h<<<

V2X-Communication: Message Types

Cooperative Awareness Message (CAM)

- Vehicle ID and Type
- Position (via GPS)
- Speed



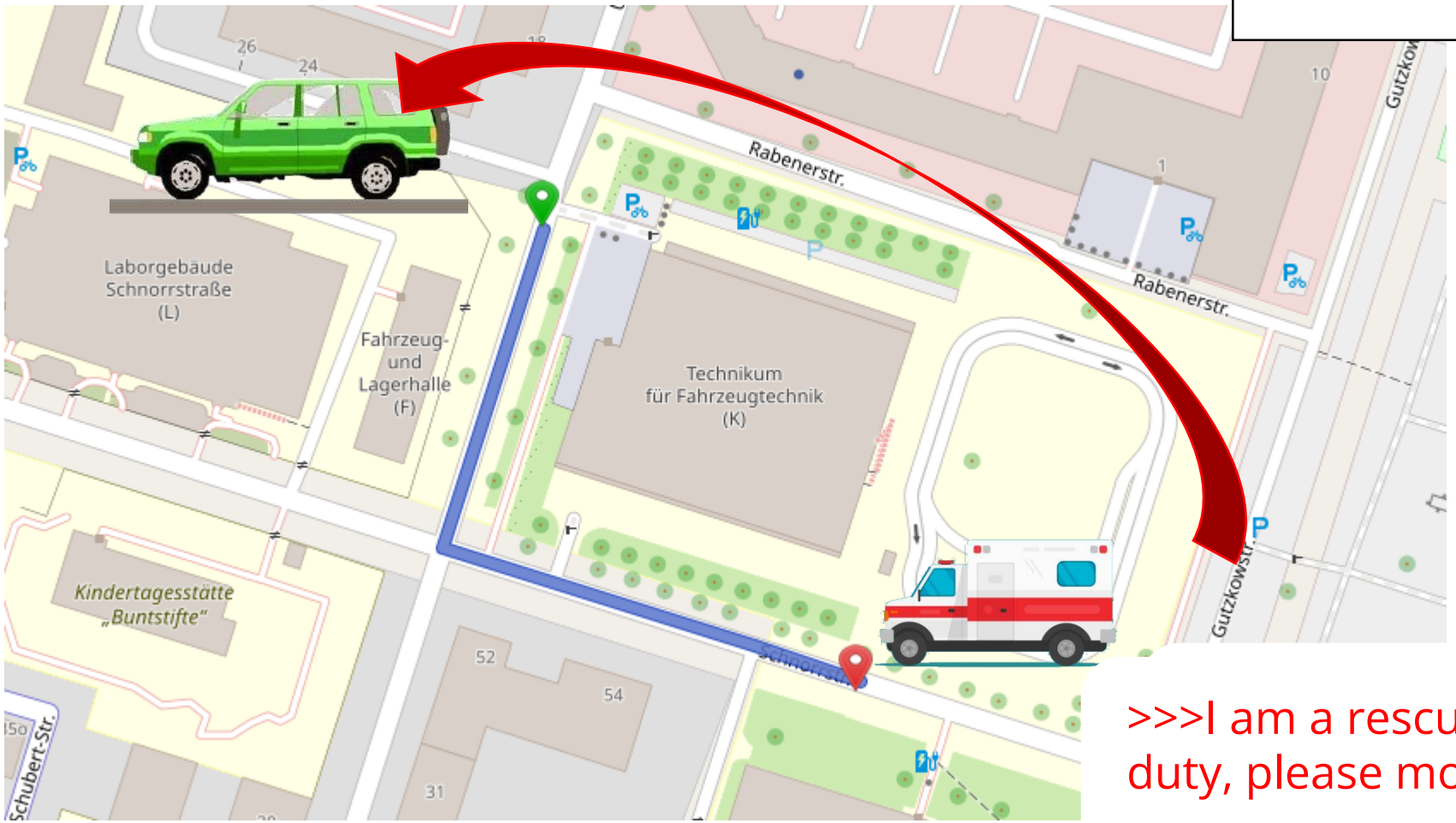
- Transmission: generate and broadcast
- CAMs are sent cyclically via a point-to-multipoint procedure to all subscribers within the direct communication radius.
- The content of a message depends on the ITS station used, vehicle vs. infrastructure unit
- Transmission is dependent on:
  - Position changes,
  - the current speed and
  - channel load

ITS – intelligent transportation systems

V2X-Communication: Message Types

DENM

- Decentralized Environmental Notification Message

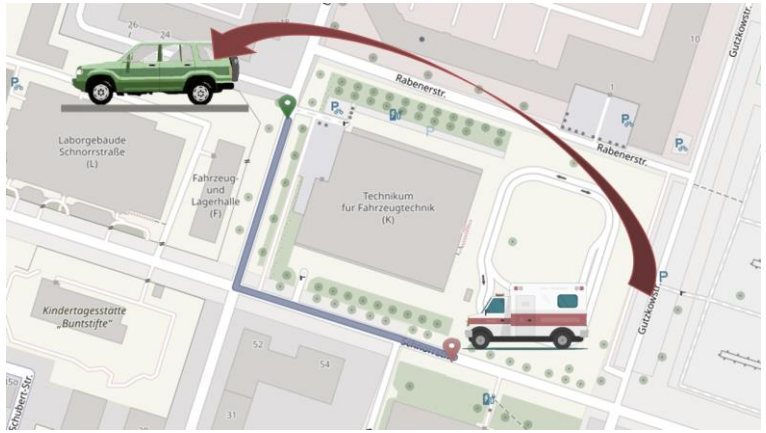


>>>I am a rescue vehicle on duty, please move over<<<

V2X-Communication: Message Types

DENM

- Decentralized Environmental Notification Message

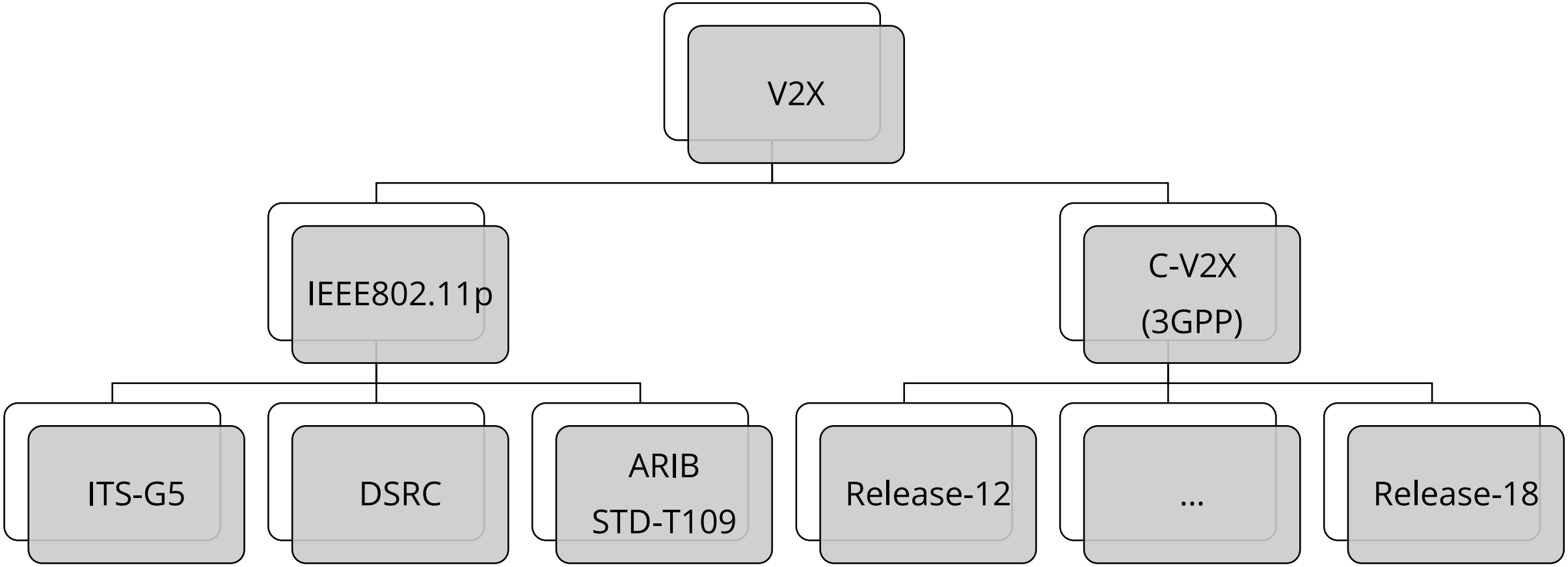


- Event-based, i.e. only sent when required:
  - Hazard warnings from other ITS stations such as
    - emergency braking,
    - roadworks,
    - approaching emergency vehicles,
    - accidents,
    - traffic jams or
    - also special road conditions (slippery roads).

- The event is characterised by
  - type of warning,
  - position,
  - occurrence time and
  - estimated duration of the event.

- between vehicles but also between vehicle and infrastructure

V2X-Communication: Overview



- Europe
- USA

V2X-Communication: IEEE802.11p

- Technical Details of DSRC (Dedicated Short Range Communication)

Low latency (~1ms) : ideal for safety-critical applications.

Range: 300–1000 meters (short range).

Data rate: Around 6–27 Mbps.

No dependency on cellular coverage: operates in ad hoc mode.

Uses **WAVE (Wireless Access in Vehicular Environments)** protocols.

V2X-Communication: IEEE802.11p

- **Security Features of DSRC**

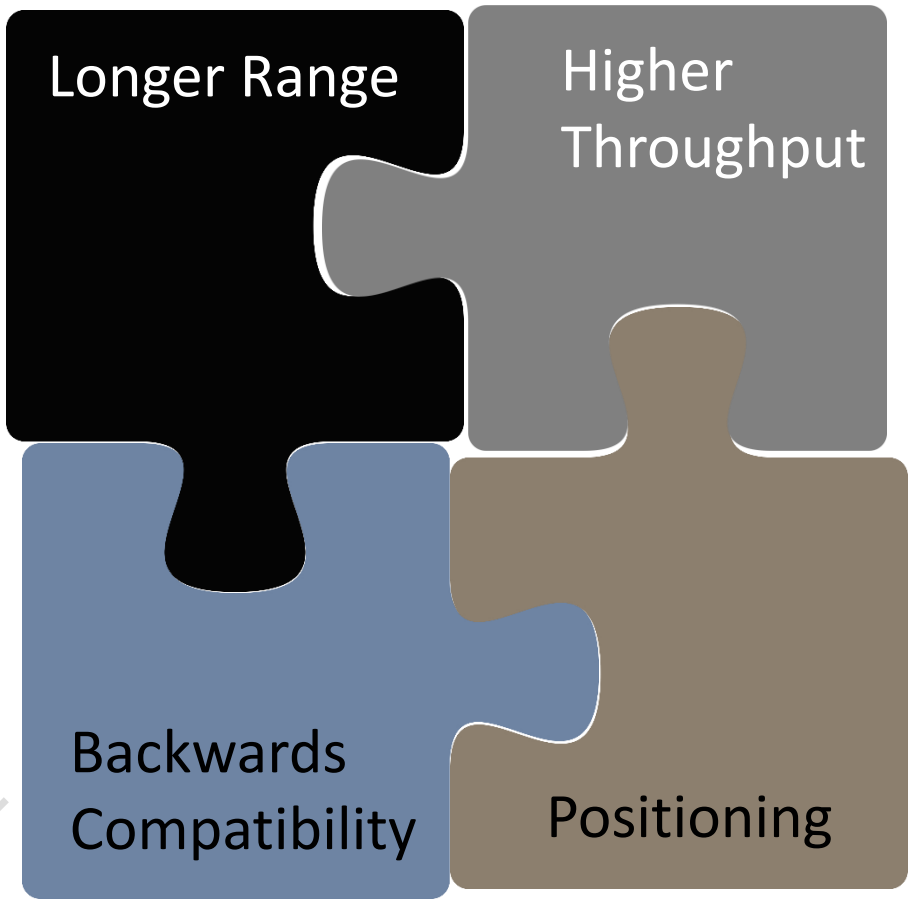
Typically relies on a **Public Key Infrastructure (PKI)** to ensure message authenticity and integrity.	Messages are **digitally signed** to prevent spoofing or tampering.	**Privacy mechanisms**: pseudonym certificates to limit tracking.

- **Limitations of DSRC**

Limited **scalability** and potential congestion in dense environments.	**Less support** for high-throughput or non-safety use cases.	**Slower innovation** pace compared to 3GPP (Cellular) standards.

802.11bd defines an evolution of 802.11p for Vehicle to Anything (V2X)

- 802.11p is largely based on 802.11a.
- 802.11bd defines MAC/PHY enhancements from 802.11n, ac, ax, to provide a backwards compatible next generation V2X protocol.
- **Higher Throughput**
  - OFDM frame design
  - Higher MCS, LDPC coding
  - Packet aggregation
- **Longer Range**
  - Mid-amble design
  - Repeated transmission mechanism
  - More robust channel coding
- **Support for Positioning**
- **Backward Compatibility**
  - Backward compatible frame format design, Version indication



802.11bd: Next Generation V2X Use Cases

5.9 GHz band mainly, and optionally 60 GHz;
Completion in 2022/2023
http://www.ieee802.org/11/Reports/tgbd_update.htm

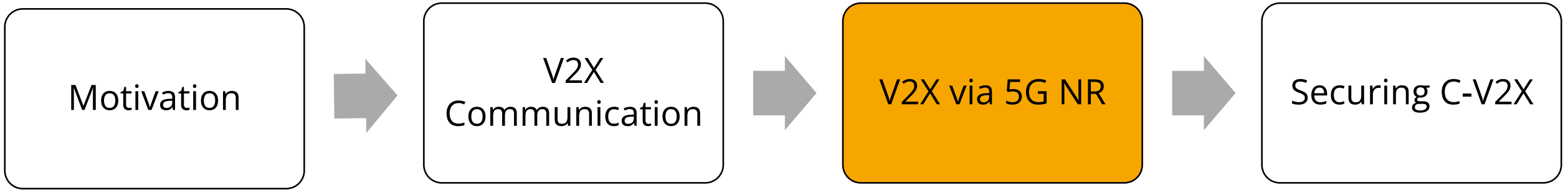
V2X Use Cases:

- Suport all defined DSRC/802.11p use cases, including Basic safety message (safety, range, backward compatibility, fairness)
- Sensor sharing (throughput)
- Multi-channel operation (safety channel + other channels)
- Infrastructure applications (throughput)
- Vehicular positioning & location (LoS and NLoS positioning accuracy)
- Automated driving assistance (safety, throughput)
- Aerial vehicle IT application (video)
- Train to train (high speed)
- Vehicle to train (high speed, long range)

Key additions :

- Higher throughput (2x) than 802.11p
- Longer range (3dB lower sensitivity level)
- Support for positioning
- Backward compatibility with 11p

Overview of Lecture



C-V2X: The Standard

©http://www.hellomaestro.de/der-mensch

- **3GPP Release 14**
  - 2014 Standardisation started
  - 2016 Publication
  - Building on LTE
  - Description of V2V and V2I as well as V2N

    → LTE-V2X

- **3GPP Release 15**
  - Migration to 5G enabled.

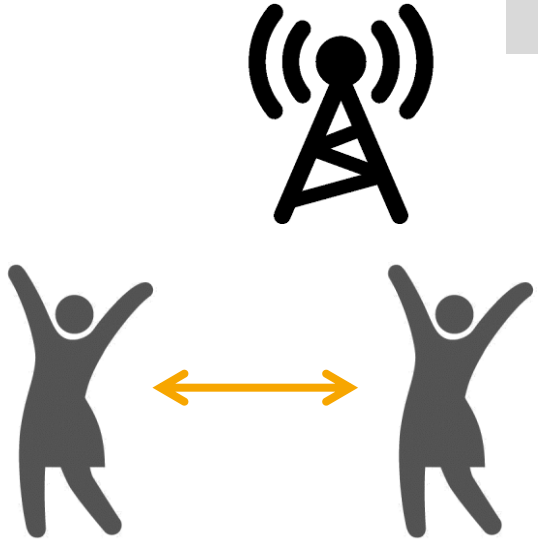
- **3GPP Release 16**
  - Functional scope of C-V2X extended
  - Migration to 5G included

- **3GPP Release 17**
  - Enhanced NR V2X (New Radio V2X)
  - Improved sidelink communication
  - Positioning and sensor sharing

C-V2X: D2D-Communication

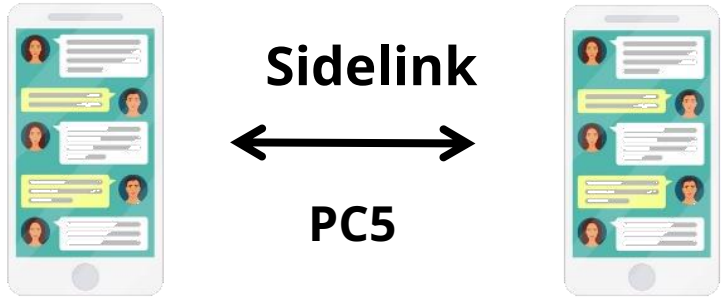
- Device2Device communication (D2D)
- Specification defined in 3GPP Release 12 and Release 13 in the ProSe services (Proximity Service) section

Discovery of user devices and/or services

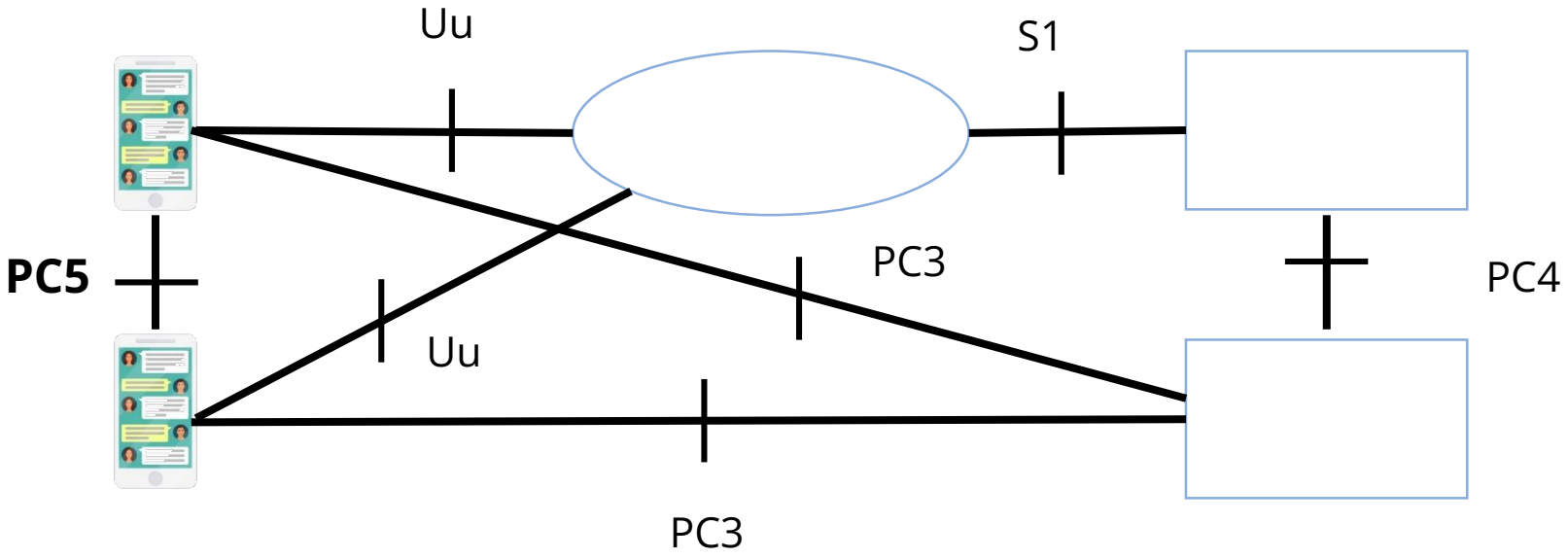


Data and language exchange between neighbouring UEs

C-V2X: Sidelink Interface

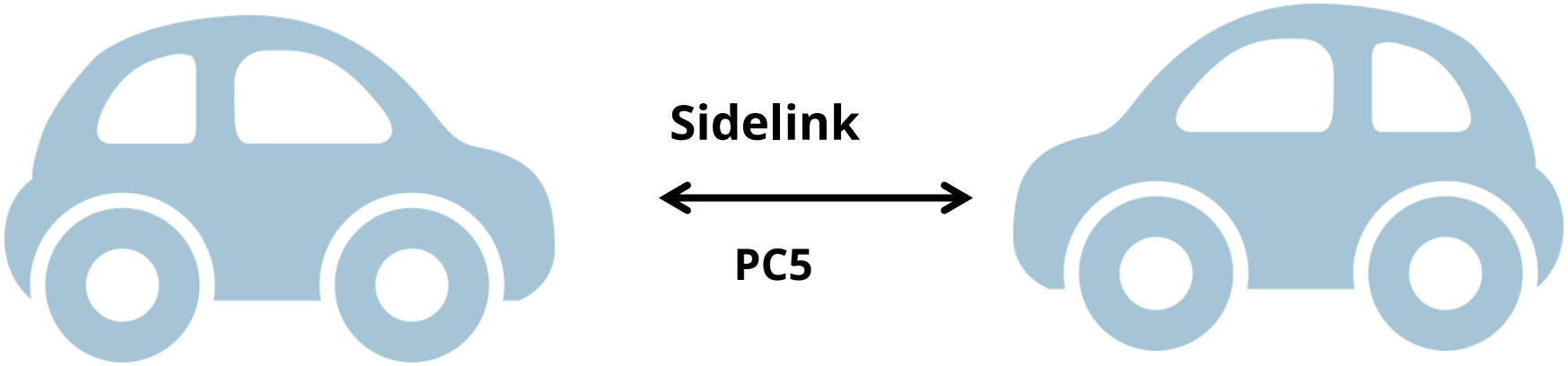


- D2D with LTE: Sidelink
- Sidelink radio interface: PC5



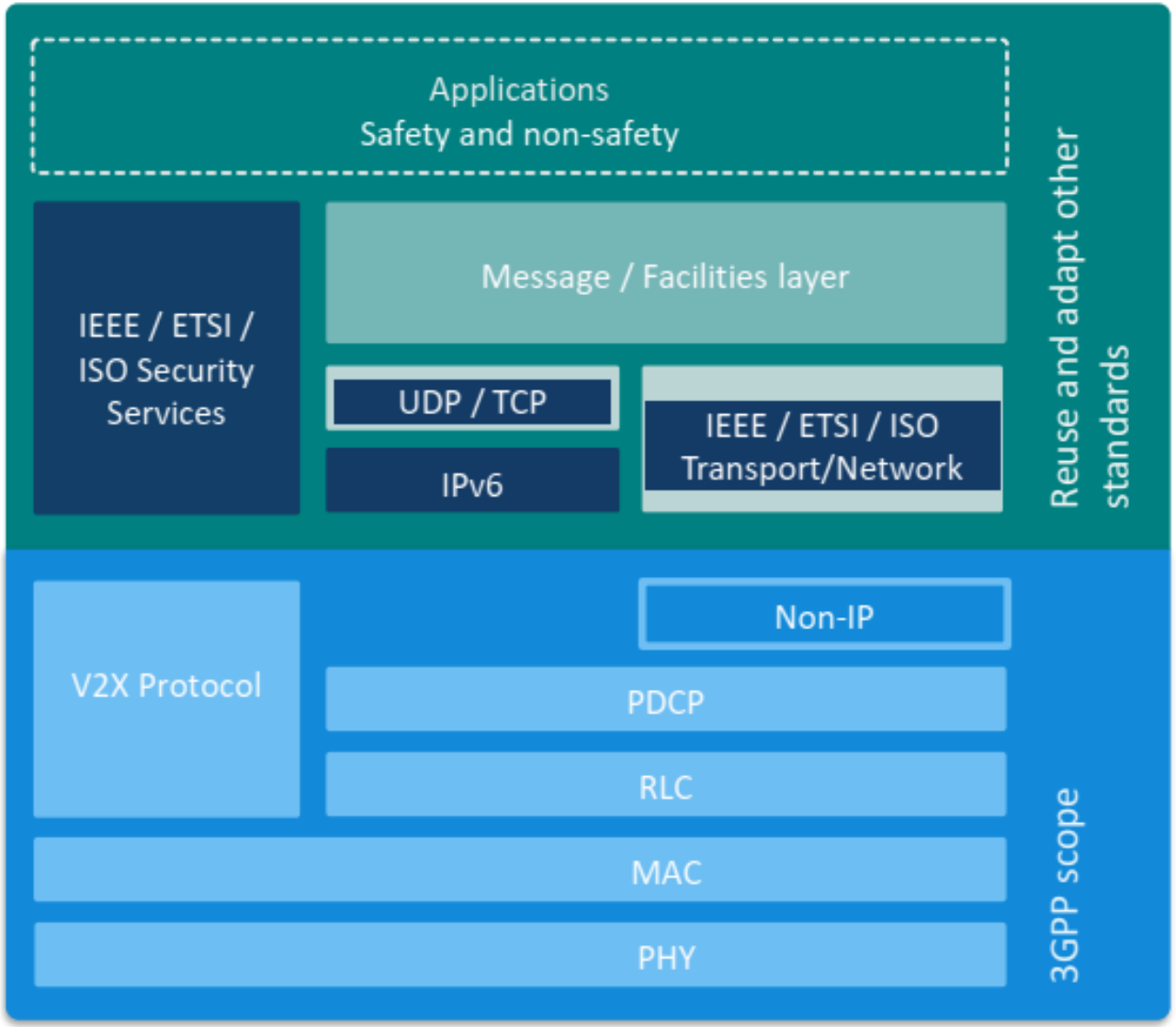
EUTRAN: Radio access network
EPC: Core network
ProSe: Short-range services
Uu: Air interface S1: Interface between EPC & EUTRAN
PC3: Logical interface ProSe & UE
PC4: Logical interface ProSe & EPC

C-V2X: Sidelink and PC5



- PC5 describes direct communication interface for communication for V2V, V2I and V2P
- Responsible for providing low-latency and highly reliable V2V/I/P services
- Independent of mobile network operator and availability of the mobile network
- Designed for: high speeds (up to 250 km/h) and high density (thousands of nodes)

C-V2X: Protocol Layers



©https://www.qualcomm.com/media/documents/files/c-v2x-its-stack.pdf/

- **Packet Data Convergence Protocol Sublayer (PDCP)**
- **Radio link control layer (RLC)**
- **Media-Access-Control Layer (MAC)**
- **Physical layer (PHY)**

C-V2X: Protocol Layer

- **Physical layer (PHY)**
  - transmits data on the sidelink.
  - uses 10 MHz or 20 MHz bandwidths at 5.9 GHz in ITS band 47.

Band	Name	Downlink [MHz]			Bandwidth (UL/DL) [MHz]	Area
		Low	Middle	High		
47	TD V2X	5855GHz: 54540	5890GHz: 54890	5925GHz: 55239	70	Global

©https://www.next-mobility.de/die-einzelheiten-der-v2x-kommunikation-a-871156/

C-V2X: Protocol Layers

- **Media-Access-Control Layer (MAC)**
  - manages the flow control of packets and the allocation of resources.
  - Packet filtering ensures that only protocol data units intended for a specific V2X device are forwarded to the higher layers.
  - hybrid ARQ protocol (HARQ)

- **Radio link control layer (RLC)**
  - Sequential transmission of service data units
  - segmentation and reassembly.

- **Packet Data Convergence Protocol Sublayer (PDCP)**
  - separates 3GPP radio access protocol layers from those of the C-ITS applications.

Processing of non-IP data is essential for C-ITS applications !

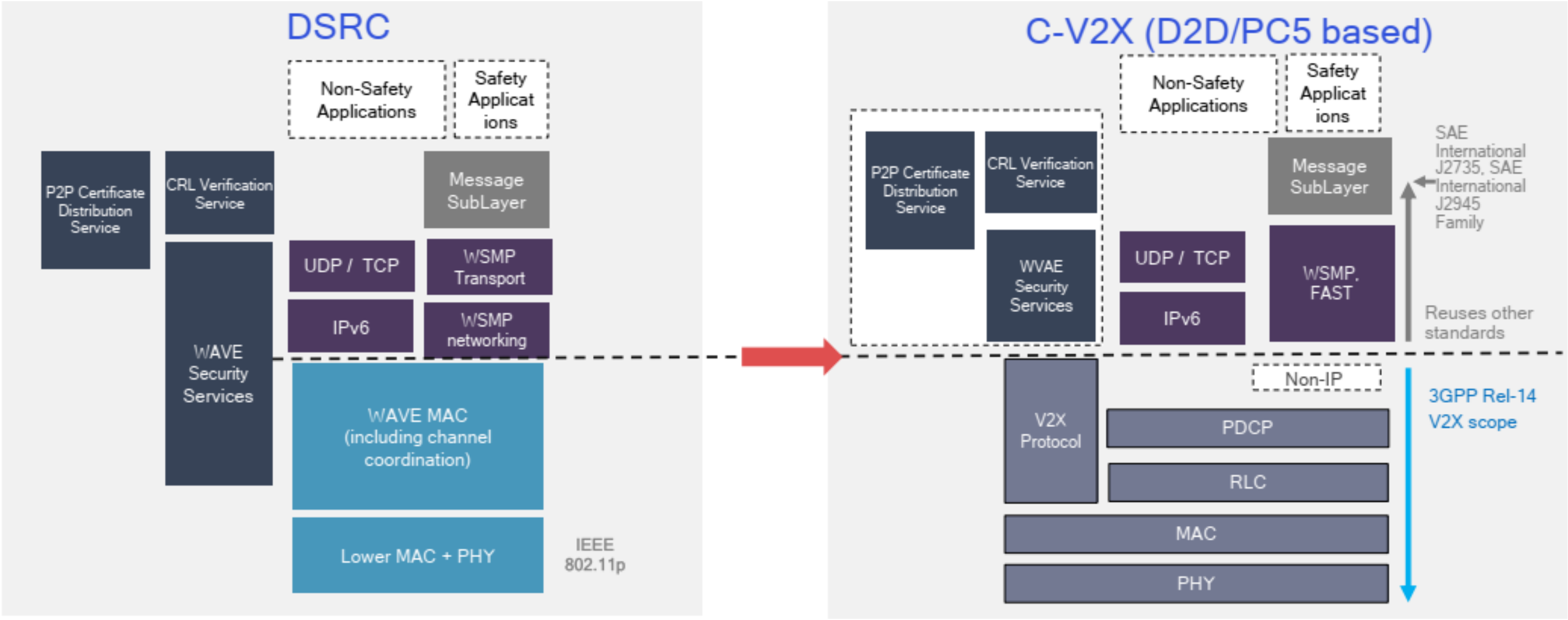
C-V2X: Protocol Layers

- **Radio resource control sub-layer (RRC)**
  - Additional layer in the control layer,
  - covers broadcast communication services,
  - manages communication,
  - configures protocol services and
  - adjusts radio parameters.

Zone Concept

uses the vehicle's latitude and longitude to ensure that the received radio signal is within an acceptable range.

C-V2X: Protocol Layers (DSRC vs. C-V2X)



©https://www.qualcomm.com/media/documents/files/c-v2x-its-stack.pdf/

C-V2X: Communication Channels

MAC sublayer provides the RLC sublayer with two logical communication channels for C-V2X communication.

Sidelink Broadcast Control Channel (SBCCH)	Sidelink Traffic Channel (STCH)
• Processes messages at control level • Sidelink Broadcast Channel (SL-BCH) transports control data from higher layers	• Processes user-level messages • Sidelink Shared Channel (SL-SCH) transports user data

C-V2X: Communication Channels

- Transport layers are mapped to physical channels in the second bit transmission layer:
  - **SL-SCH** to the Physical Sidelink Shared Channel (PSSCH)
  - **SL-BCH** to the Physical Sidelink Broadcast Channel (PSBCH)
  - **PSCCH:**
    - control information regarding processing time and frequency resource allocation
    - Transmission of control information with QPSK (robust)
    - Transmission of user data with QPSK and 16QAM

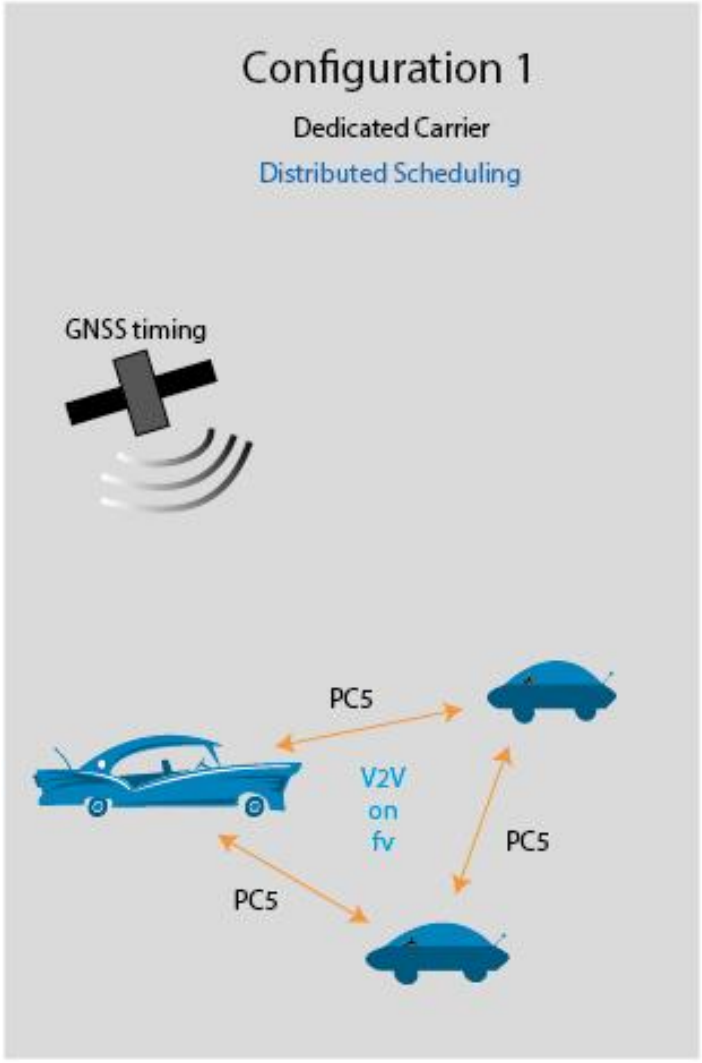
- PC5 communication adopts 1-ms subframe structure of LTE
  - 14 single carrier frequency division multiple access symbols (SC-FDMA) per subframe are transferred four to a demodulation reference symbol (DMRS).

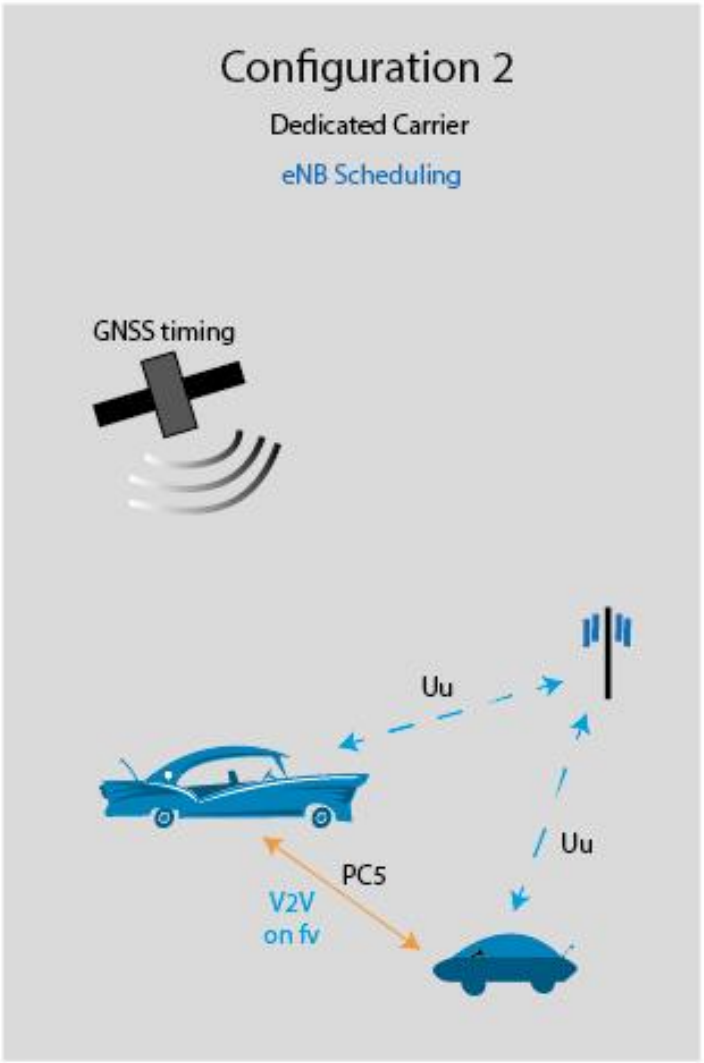
  → Compensation of Doppler shifts in C-V2X communication

C-V2X: Configurations

- 2 different deployment configurations
  - PC5-based V2V communication
  - GNSS for time synchronisation

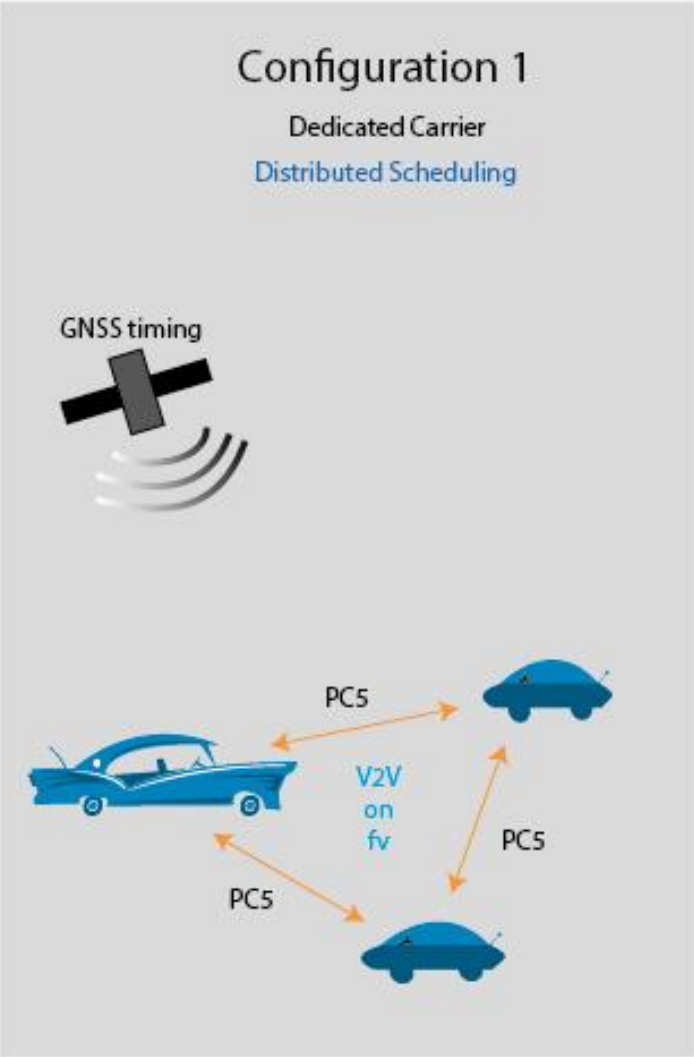
1. …
2. …





©https://www.3gpp.org/news-events/3gpp-news/1798-v2x_r14

C-V2X: Configurations



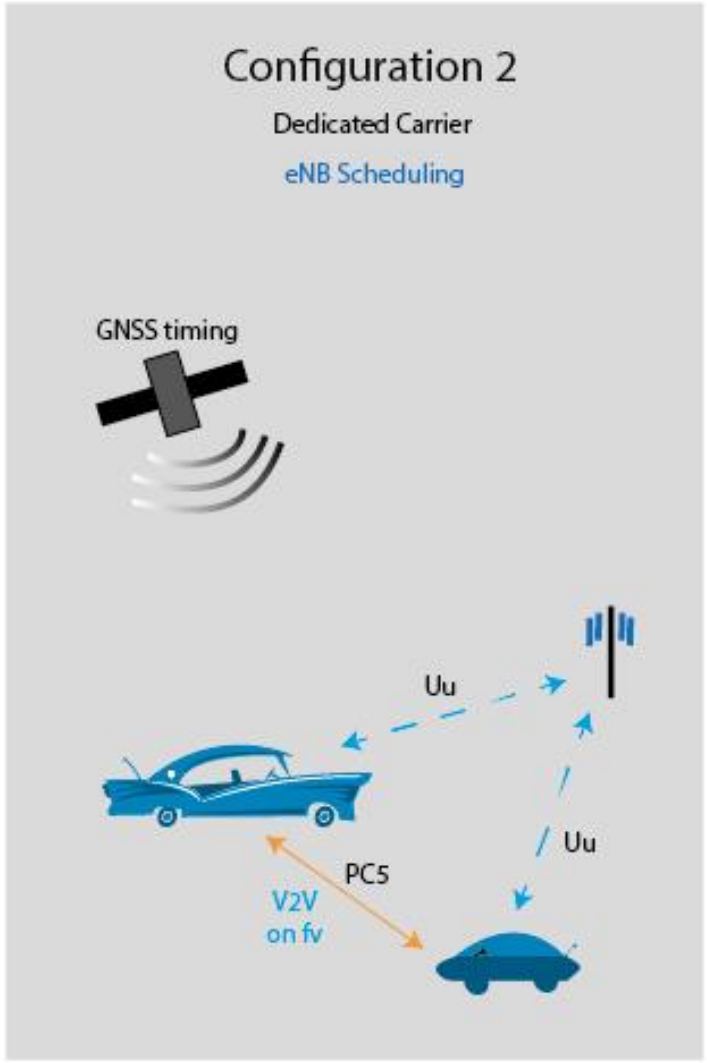
- Scheduling (fair resource allocation) and interference management of V2V traffic
  - Supported by distributed algorithms
  - Implementation between vehicles

- New mechanism where resource allocation is dependent on geographical information or zones

PC5-Interface

©https://www.3gpp.org/news-events/3gpp-news/1798-v2x_r14

C-V2X: Configurations



- Device in network coverage and in RRC connection status
  - UE sends eNB a scheduling request
- Scheduling and interference management is supported by the eNBs through control signalling via Uu interface
- eNodeB dynamically allocates resources for V2V signalling
- Use of licensed spectrum for communication with eNodeB
  - Unlicensed V2X spectrum between vehicles

©https://www.3gpp.org/news-events/3gpp-news/1798-v2x_r14

C-V2X: Differences between 4G and 5G

– **More Functionalities**

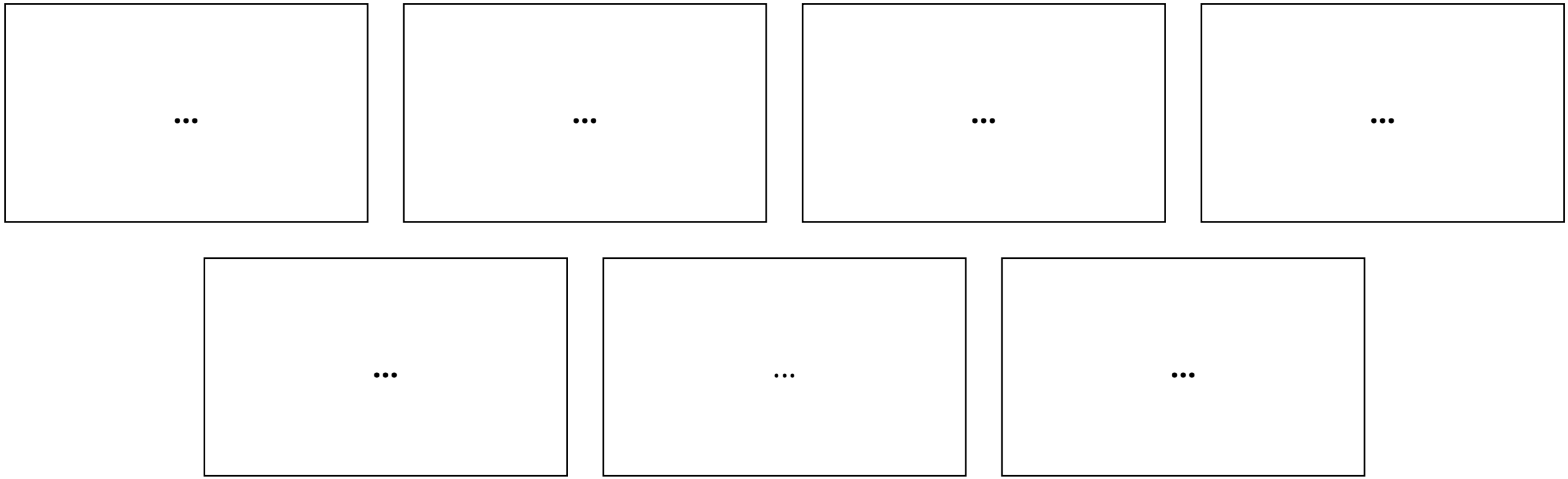
- Efficient design at sidelink link level for optimised performance at all speeds
- Connectionless 'on-the-fly' distance-based groups
- Multicast with distance-based reliability and application relevance

– uses the flexible NR framework

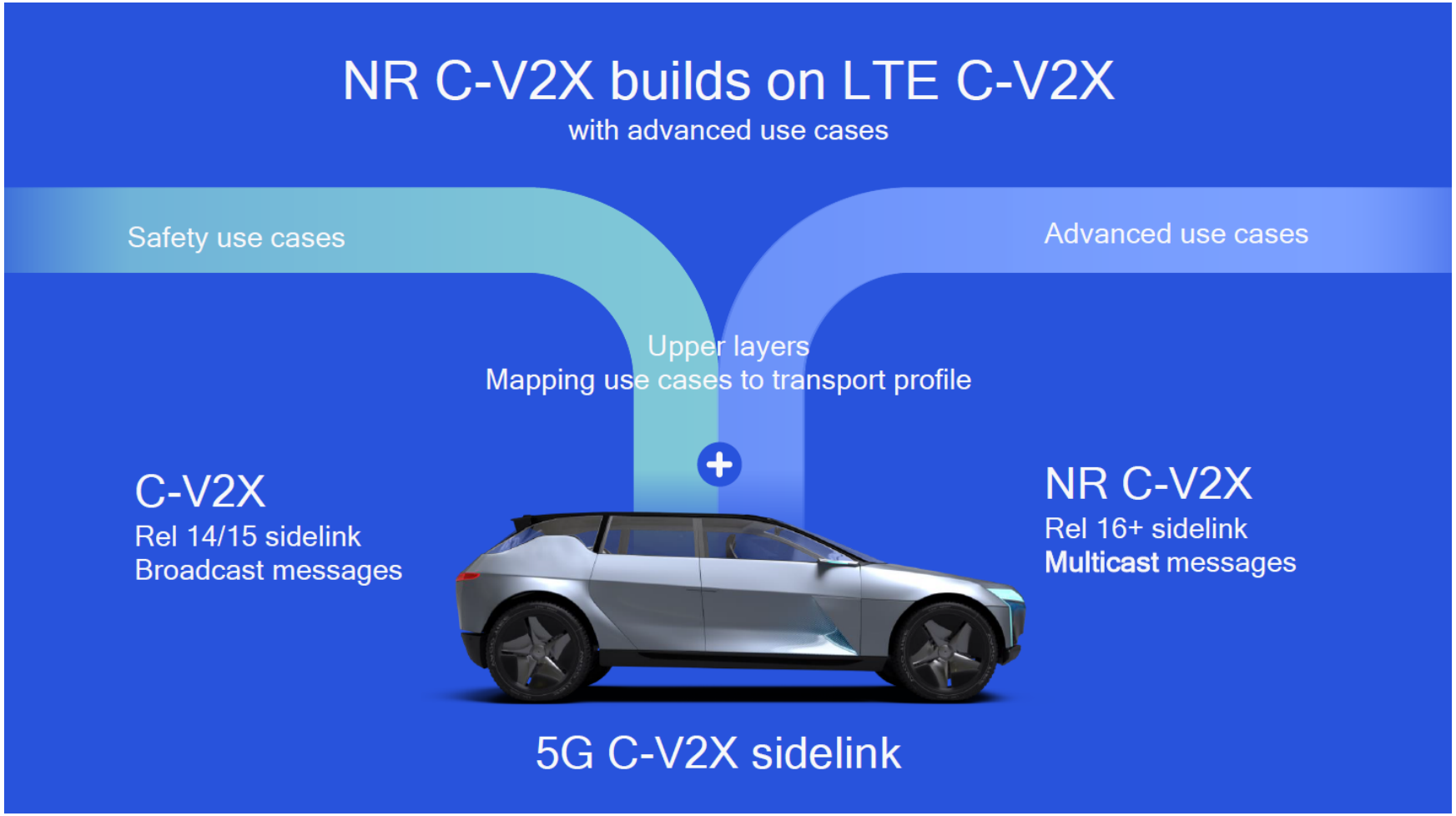
– **Increased performance**

- Lower latency
- Higher spectral efficiency
- Higher capacity

C-V2X: with 5G NR properties ☺



C-V2X: Enhancement to NR C-V2x



©https://www.qualcomm.com/research/5g/cellular-v2x

- NR: New Radio

  → **NR C-V2X**

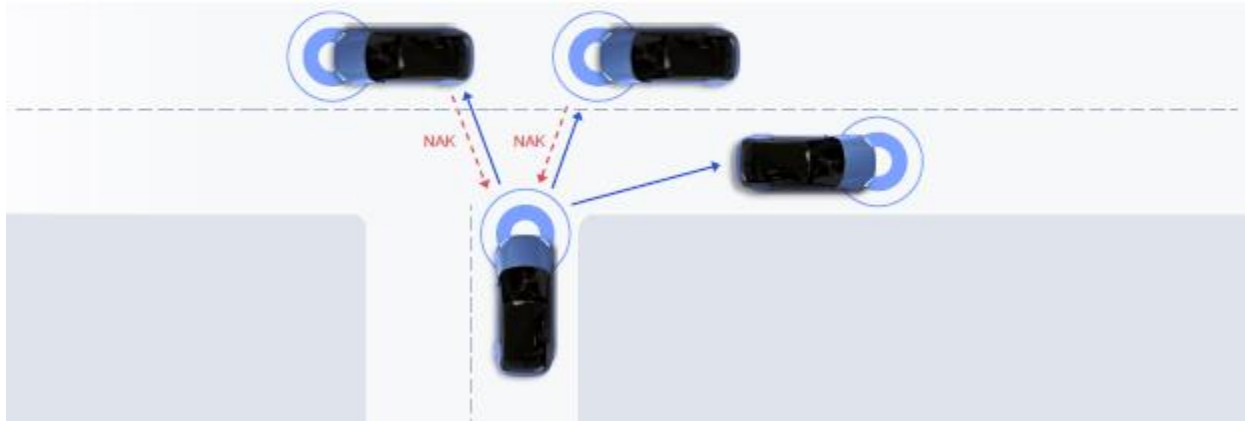
- Additional services
- Multicast messages

NR C-V2X: what‘s new?

- **Based on 5G NR** technology developed by 3GPP (from Release 16 onwards)
- Enables ultra-reliable, low-latency communication between vehicles, infrastructure, pedestrians, and networks
- Supports both Uu (cellular) and PC5 (direct) communication interfaces
- Designed for high-speed, high-density vehicular environments
- Facilitates advanced safety applications, e.g. collision avoidance, cooperative driving
- Scalable for future use cases like autonomous driving and AI-based traffic management
- Offers enhanced security and privacy mechanisms over legacy V2X systems

NR C-V2X: Multicast

- Reliable multicast is based on:
  - NAK (negative acknowledgement)
- Transmission repetition based on:
  - HARQ (hybrid automatic repeat request)
- Multiple receivers send NAK feedback using the same resource (time and frequency, SFN - single frequency network)
- SFN of NAK keeps the feedback overhead constant, regardless of the number of receivers.

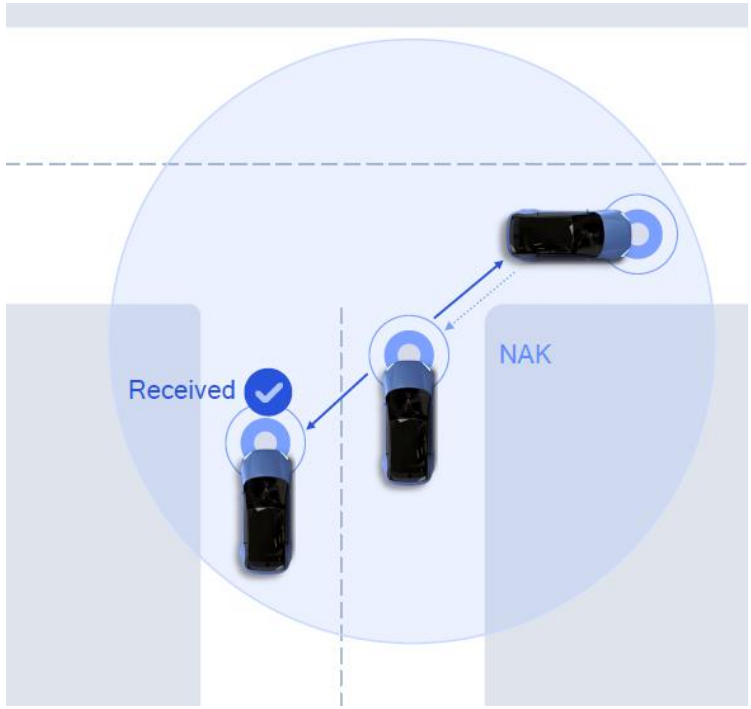


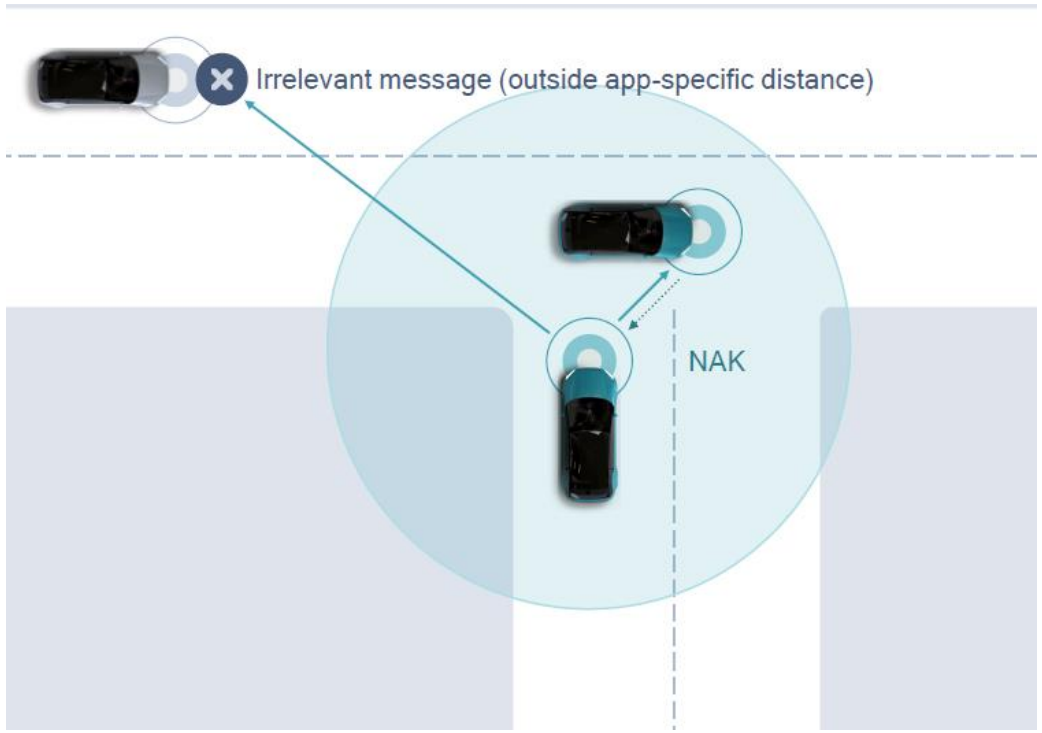
©https://www.qualcomm.com/research/5g/cellular-v2x

NAK: negative acknowledgement

HARQ: hybrid automatic repeat request

NR C-V2X: Multicast

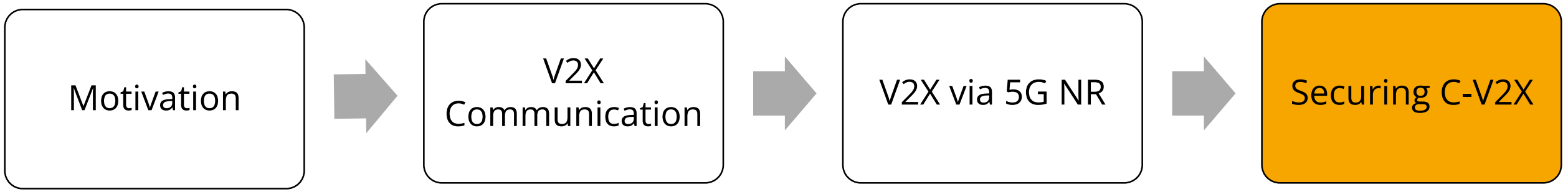




©https://www.qualcomm.com/research/5g/cellular-v2x

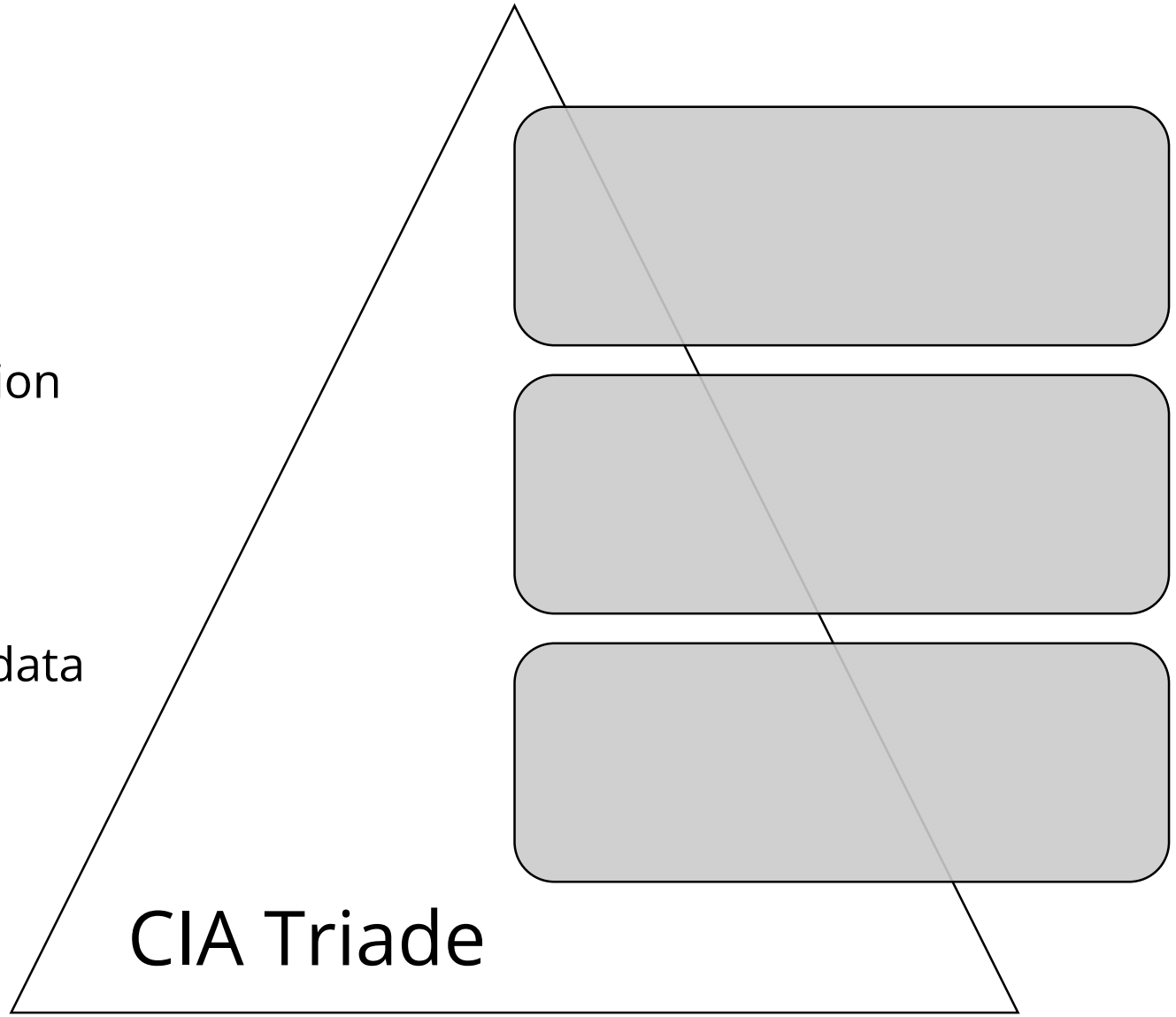
- Application-specific distance is determined on the basis of relevance
- Transmitting vehicles adapt transmission to relevant vehicles within range
- Receiving vehicles only acknowledge (NAK) relevant messages

Overview of Lecture



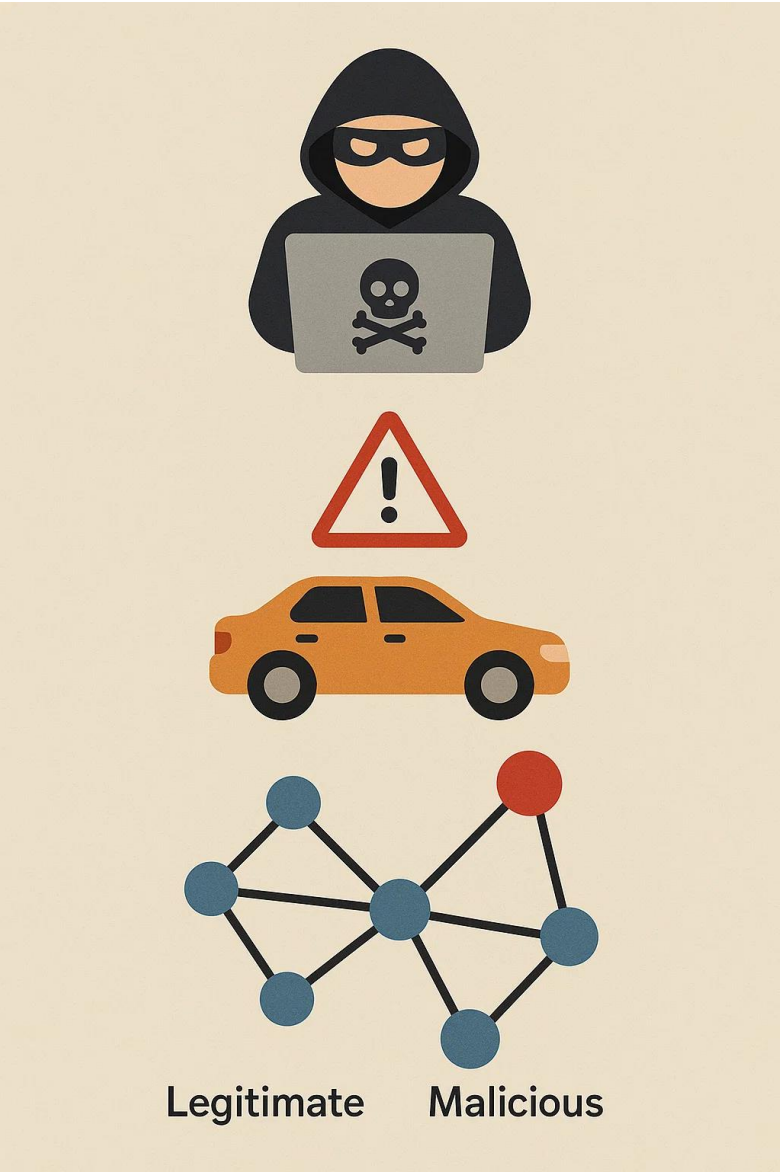
V2X-Communication: Security requirements

- Authenticity of the messages
- Confidentiality and data protection
- Availability of services
  (e.g. in the event of DoS attacks)
- Integrity of the communication data



NR C-V2X: Potential Attackers

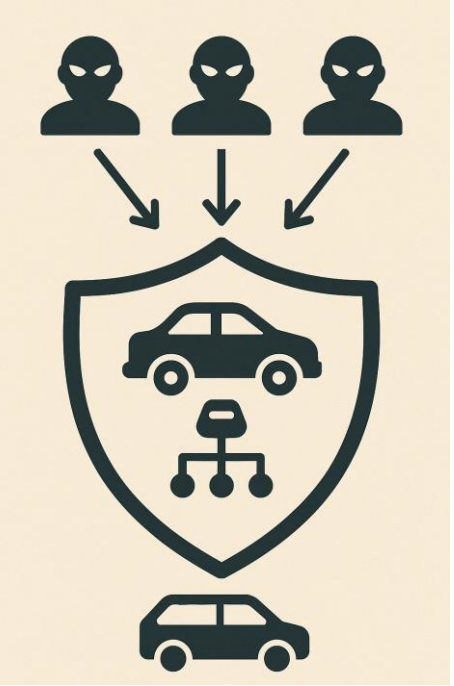
- **External Hackers:** Attempt to disrupt or eavesdrop on V2X communications via wireless interfaces.
- **Insider Threats:** Authorized users (e.g. fleet operators) misusing access to inject false information or compromise systems.
- **Compromised Vehicles:** Vehicles with tampered software/hardware transmitting malicious data into the network.
- **Rogue RSUs or OBUs**: Malicious roadside units or onboard units impersonating legitimate devices.
- **Man-in-the-Middle (MitM)** attackers exploiting weak authentication between nodes.



©generated by sora.chatgpt.com

NR C-V2X: Key Cyberattack Scenarios

Attack Type	Description
	Fake identities broadcast incorrect data (e.g. false GPS location)
	Old legitimate messages resent to mislead systems (e.g. fake traffic info)
	Radio interference disrupts V2X communication (especially on PC5 interface)
	Tampering with sensor data or messages (e.g. forged accident alerts)



©generated by sora.chatgpt.com

- These attacks target availability, integrity, and trust in V2X communication.
- Defense mechanisms include PKI-based authentication, timestamping, spectrum monitoring, and message consistency checks.

NR C-V2X: Key Security Measures

- **Authentication & Authorization**
  - Ensure only legitimate nodes (vehicles, RSUs, infrastructure) can communicate.
- **Integrity Protection**
  - Messages are signed to detect tampering or falsification.
- **Confidentiality** (when required)
  - Sensitive data (e.g., diagnostics, private vehicle info) can be encrypted.
- **Anomaly Detection**
  - AI-based systems to detect abnormal traffic behaviour or malicious nodes (IDS).
- **Secure Boot and Firmware Updates**
  - Ensures trusted software is running on OBUs/RSUs.
- **Separation** of Safety-Critical and Infotainment Systems
  - Limits attack surface within the vehicle.

NR C-V2X: Role of PKI

- **PKI = Public Key Infrastructure**
  - Provides cryptographic foundation for secure message exchange.
- **Digital Certificates**
  - Issued to each vehicle and infrastructure node.
  - Enable identity verification and message signing.
- **Pseudonym Certificates**
  - Protect privacy by changing identifiers periodically.
  - Limit tracking while maintaining trust.
- **Certificate Authority (CA) Hierarchy:** Root CA → Enrollment CA → Authorization CA**.**
- **Message Signing & Verification**
  - Ensures authenticity and integrity of V2X messages (e.g., CAM, DENM).

©https://www.pandasecurity.com/en/mediacenter/cybersecurity-measures/

NR C-V2X: Cybersecurity Challenges

High Node Mobility

- Frequent handovers and dynamic topologies complicate secure session management.

Scalability of Authentication

- Managing thousands of certificates for OBUs and RSUs in real time requires a robust PKI infrastructure.

Resource Constraints in OBUs

- Limited computational capacity impacts the implementation of strong encryption and anomaly detection.

Exposure to Physical Tampering

- OBUs and RSUs may be exposed to tampering in public environments.

Attack Surface via PC5 and Uu Interfaces

- Dual communication paths (sidelink and cellular) increase potential entry points for attackers.

NR C-V2X: Cybersecurity Challenges

Infrastructure Gaps
• Inconsistent deployment of RSUs and edge computing across urban and rural regions hinders secure coverage.

Lack of Standardized National PKI
• most countries are still in the process of defining V2X-specific PKI frameworks.

Limited Regulatory Frameworks
• Data privacy, message authentication, and liability standards are still evolving.

Cost Constraints
• Widespread adoption of secure OBUs may be hindered by affordability in mass-market vehicles.

Cyber Awareness and Skill Gaps
• Need for trained cybersecurity professionals and policy support tailored to vehicular communication systems.

NR C-V2X: Establishing Unified Security Standards

Category	Measure / Approach	Examples / Organizations
International Standardization	Develop global technical specifications	3GPP, ETSI, IEEE 1609.2
PKI Infrastructure	Establish interoperable Public Key Infrastructures	Root CAs, Pseudonym Certificates, Certificate Revocation Lists (CRLs)
Industry & Government Collaboration	Foster joint development across sectors	**5GAA**, CAR2CAR Communication Consortium, SAE International
Legal & Regulatory Alignment	Harmonize national regulations with global security policies	EU Cybersecurity Act, India's CERT-In Guidelines
Certification & Compliance	Introduce standardized security audits and certifications	TÜV, NIST, ISO/SAE 21434, UNECE WP.29
Open-Source & Research	Promote transparent and standards-compliant security frameworks	**OMNeT++**, OpenC2X, **Veins**, Simulation-based Security Evaluation

NR C-V2X: 5G Automotive Association

– **5G Automotive Association (5GAA)**
– Established in 2016 with original members:
AUDI AG, BMW Group, Daimler AG, Ericsson, Huawei, Intel, Nokia, und Qualcomm Incorporated.

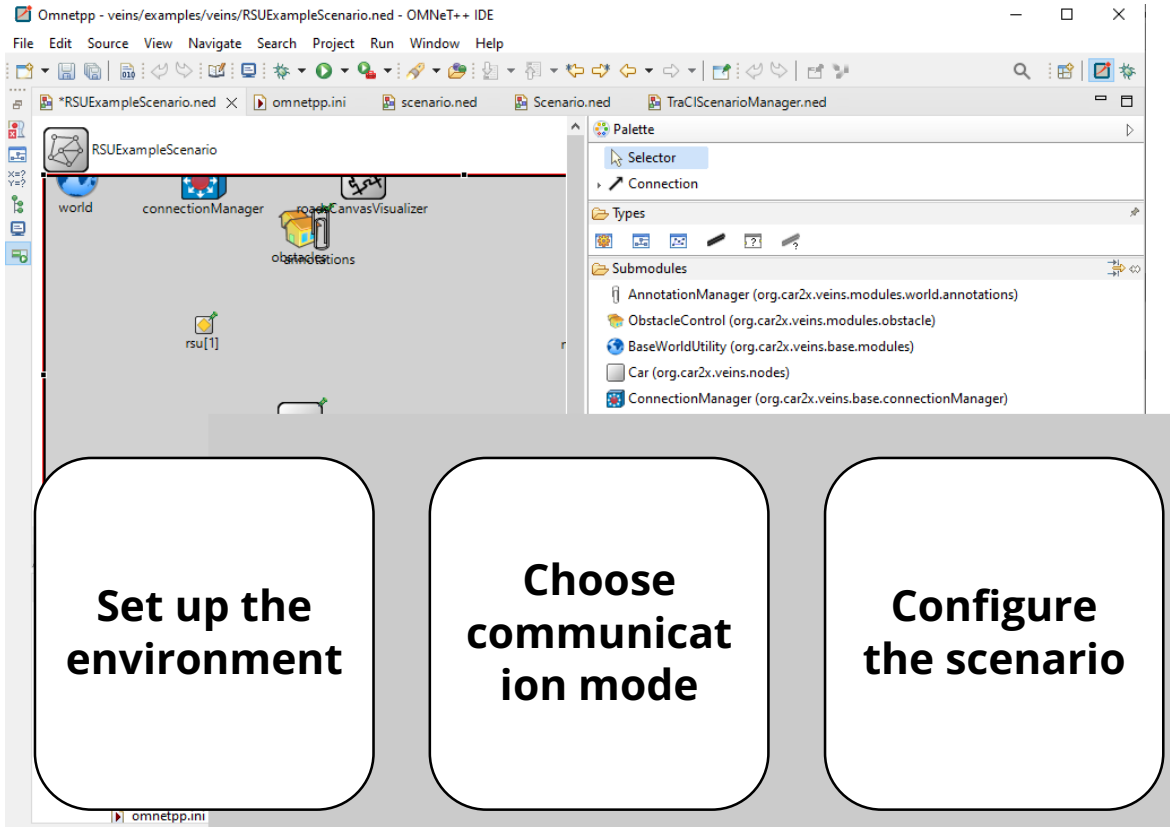
- Fast expansion to include:
  - leading automotive manufacturers,
  - Top Tier 1 suppliers,
  - Telecommunications companies,
  - Smartphone manufacturers,
  - Semiconductor companies,
  - Wireless infrastructure companies,
  - Test and measurement companies and
  - Certification companies.

Aim:
Definition and development of the next generation of connected mobility and automated vehicle solutions

News:
In Jan 2025, 5GAA signed an MoU with ITS India to accelerate C-V2X and 5G mobility solutions.

NR C-V2X: Simulations in OmNet++

NR C-V2X: Simulations in OmNet++



Set up the environment

Choose communication mode

Configure the scenario

Model V2X applications

Run the simulation

Optional extensions

→ Exercise

NR C-V2X: Conclusion

- 5G NR C-V2X enables ultra-reliable, low-latency and high-speed communication between vehicles, infrastructure and other road users.

- **Security Enhancements:**
  - Public Key Infrastructure (PKI) for authentication and message integrity
  - Support for pseudonym certificates to ensure privacy
  - Defense against spoofing, replay, jamming and data manipulation

- **Technical Advantages on Physical Layer:**
  - Advanced modulation (256-QAM), LDPC coding and beamforming
  - Flexible subcarrier spacing and ultra-low latency support (<1 ms)

- **Interoperability & Standardization:**
  - Aligned with 3GPP, ETSI, and IEEE 1609.2 standards
  - Supported by global industry alliances like 5GAA

- **Relevance for Emerging Markets** (e.g., India):
  - Key role in addressing traffic safety and urban mobility
  - Supported by initiatives like 5GAA–ITS India collaboration

5G is the foundation for secure, scalable, and future-ready V2X ecosystems.

Control Questions

Differences between IEEE802.11p and C-V2X?

- …

Different Configuration principles of C-V2X?

- …

Key security measures of C-V2X?

- …

Unified Standards for C-V2X (why and how)?

- …

NR C-V2X: Outlook – Cross-Domain Synergy

- **FRMCS (Future Railway Mobile Communication System)**
  is the next-generation mobile communication standard for railways, set to replace GSM-R.
- Based on **3GPP 5G NR**, it offers high reliability, low latency and massive connectivity.
- Key features:

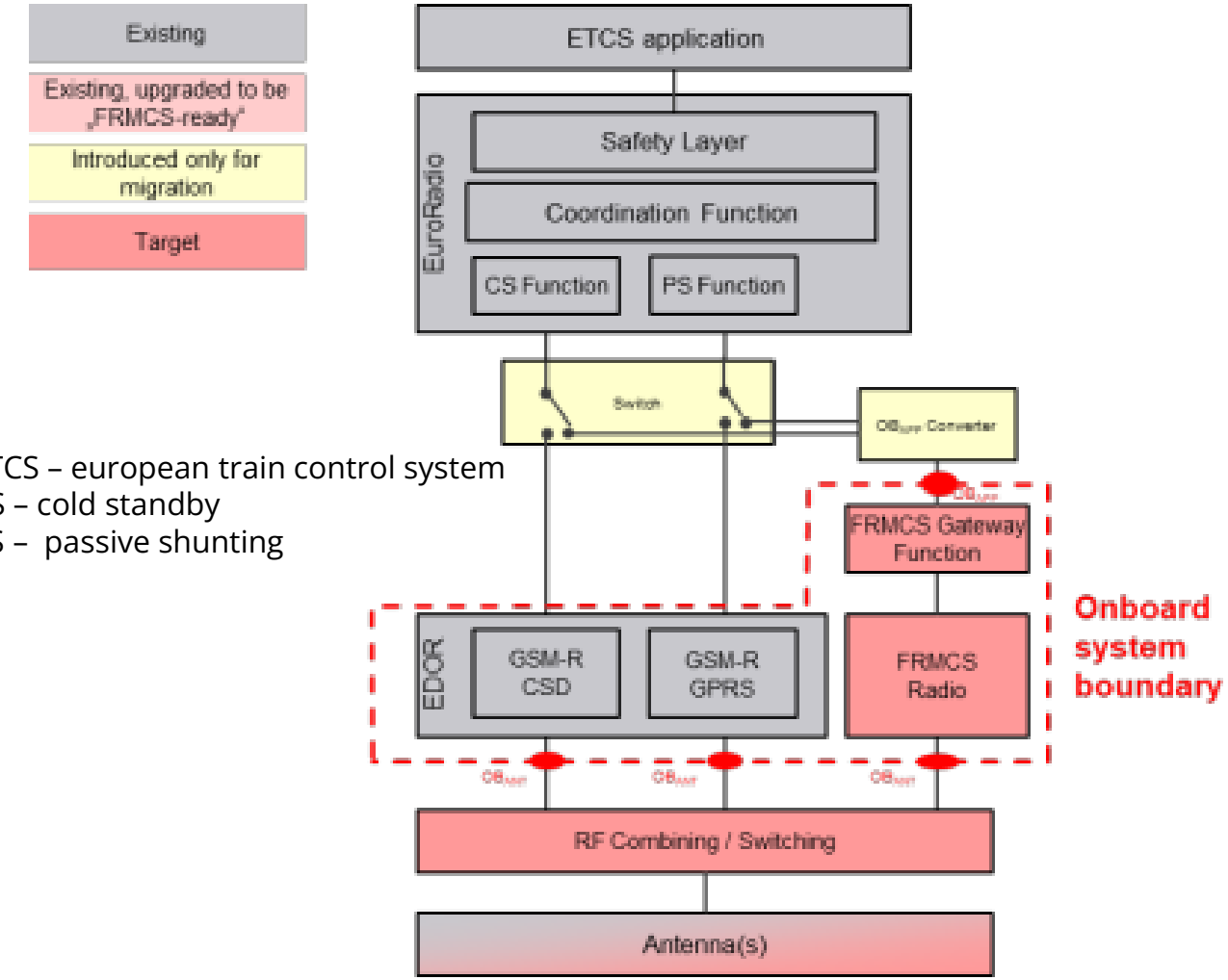
Supports **mission-critical voice**, data and signaling	Designed for **ETCS Level 3**, automatic train control and predictive maintenance	Ensures **seamless communication** between trains, infrastructure and control centers

- Link to NR C-V2X:

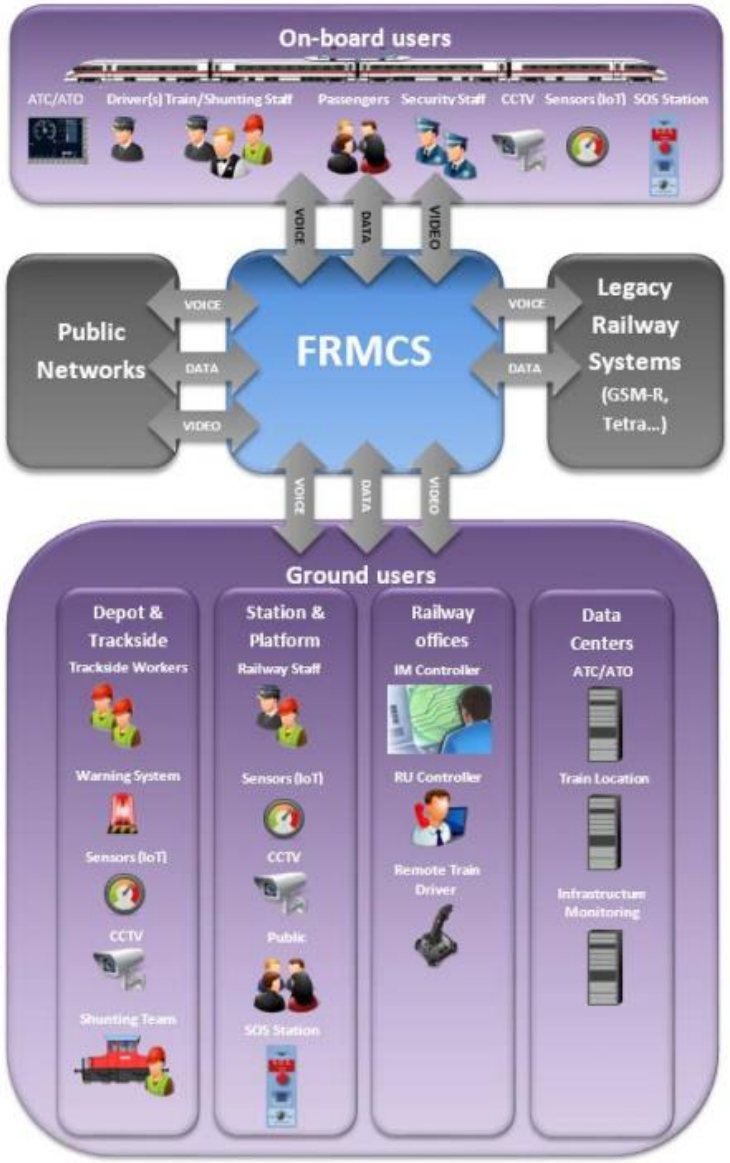
Shares common 5G NR foundation, enabling cross-domain V2X communication (e.g., rail-to-road interoperability)	Beneficial for urban mobility integration, especially in smart cities and **multimodal transport** systems	Uses similar sidelink **(PC5) and network (Uu)** interfaces for direct and cellular communication

Goal: Establish a unified, future-proof communication ecosystem across road and rail transport.

NR C-V2X: Outlook – Cross-Domain Synergy



ETCS – european train control system
CS – cold standby
PS – passive shunting



©UIC Rail System Department: FRMCS and 5G for rail: challenges, achievments and opportunities, Dev. 2020.

Literature

[1] Chen, S. et al. (2023) Cellular Vehicle-to-Everything (C-V2X). 1st ed. 2023. [Online]. Singapore: Springer Nature Singapore. https://link.springer.com/book/10.1007/978-981-19-5130-5

[2] 3GPP, “TS 38.300 NR and NG-RAN Overall Description, v16.5.0,” 3GPP, Tech. Spec., Mar. 2021. (3GPP)

[3] L. Gallo and J. Haerri, „Unsupervised Long- Term Evolution Device-to-Device: A Case Study for Safety-Critical V2X Communications,” in IEEE Vehicular Technology Magazine, vol. 12, no. 2, pp. 69-77, June 2017

[4] M. Castaneda Garcia et. al, “A Tutorial on 5G NR V2X Communications”, IEEE Communication Surveys and Tutorials 2021

[5] Z. Ali, S. Lagén, L. Giupponi and R. Rouil, „3GPP NR V2X Mode 2: Overview, Models and System-Level Evaluation,” in IEEE Access, vol. 9, pp. 89554-89579, 2021

[6] Qiu, H., Qiu, M., & Lu, R. (2020). Secure V2X Communication Network based on Intelligent PKI and Edge Computing. IEEE Network, 34, 172-178.

HTWD Hochschule für Technik und Wirtschaft Dresden University of Applied Sciences

Contact

Prof. Dr.-Ing.
Julia Maria Engelbrecht

julia.engelbrecht@htw-dresden.de