With funding from the:

Federal Ministry of Research, Technology and Space

ConnRAD – Connectivity and Resilience for Automated Driving

ConnRAD
Connectivity & Resilience for automated Driving Functions in Germany

Final Presentation **23.10.2025**

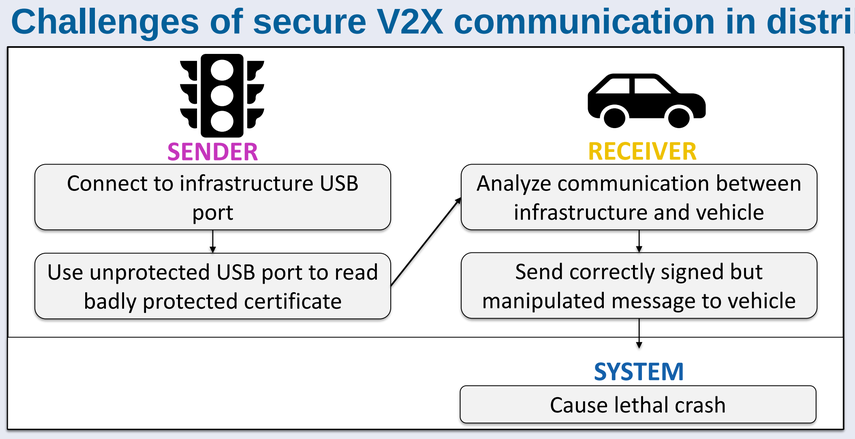
Security

Leonie Pech, Robert Bosch GmbH, XC/ESS1

Driving into the future: Securing V2X communication in distributed systems

Challenges

Challenges of secure V2X communication in distributed systems



Example of a distributed attack path

- **Risks** in distributed systems **relevant to all stakeholders** → root of one attack exists in one subsystem (e.g. sender); but **effect visible in the other subsystem** (e.g. recipient)
- Risk treatment can only be done in originating subsystem
- **Attack paths distributed** between sender and recipient → can not be analyzed without further information from the other subsystem
- **No clear regulations** for development of distributed systems
- **No responsible** for overall system in the sense of ISO/SAE 21434
- Subsystem partners **do not know if** received **information is trustworthy and sufficiently secured**
- Subsystem **partners** will **meet for the first time during runtime**

Results / Concept

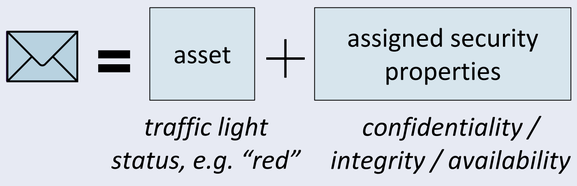
Solution: The Minimum Resilience Factor (MRF) - Terms

MRF *Minimum Resilience Factor*
- universal representation of the likelihood for an attack
- used to assess whether the provided data is sufficiently secured
- can be universally understood and used

Mapping
- mapping of individual results to the defined MRF values
- makes results understandable by mapping them to the MRF

PMRF *Provided MRF*
- defined during the TARA creation of the sender
- MRF a sender can at least guarantee for an object (asset + property)

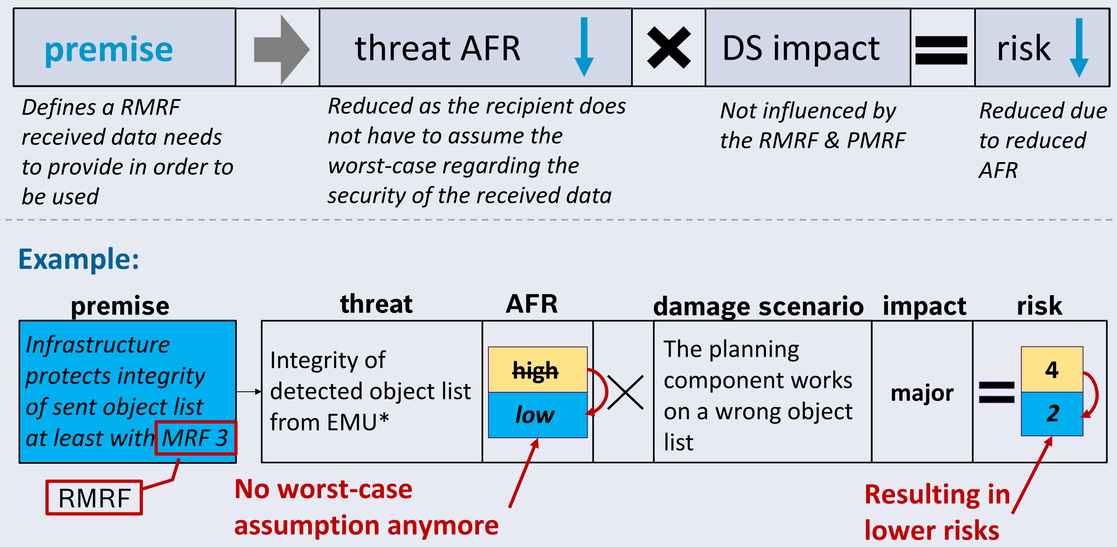
RMRF *Required MRF*
- defined during the TARA creation of the recipient
- MRF an object (asset + property) at least needs to have
- If PMRF < RMRF: receiver unable to use this data



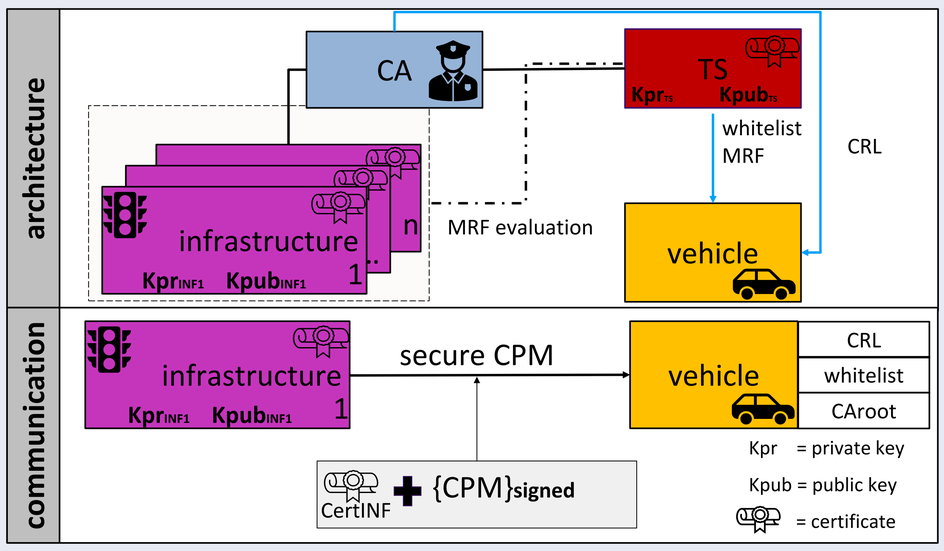
Solution: The MRF – Secure V2X messages

- **extends known V2X messages**, e.g. CPM (ETSI TS 103 324)
- can be transferred to all types of V2X messages
- MRF is assigned to an asset + a security property
- asset linked with up to 3 properties
- signed with private key of sender
- **Secure CPM = assets + security properties + MRF values + signature**

Example: Secure CPM*



Solution: The MRF – Schematic layout



Communication:
- SecureCPM sent to vehicle
- Check certificate revocation list, check whitelist, verify signature
- Check not fulfilled → reject message → start fallback process

Solution: The MRF – Effects on a TARA

- RMRF = the recipient poses a premise to the security level of the received data
- External data will only be used, if PMRF >= RMRF
- Has an effect on the attack feasibility rating and the resulting risk value.

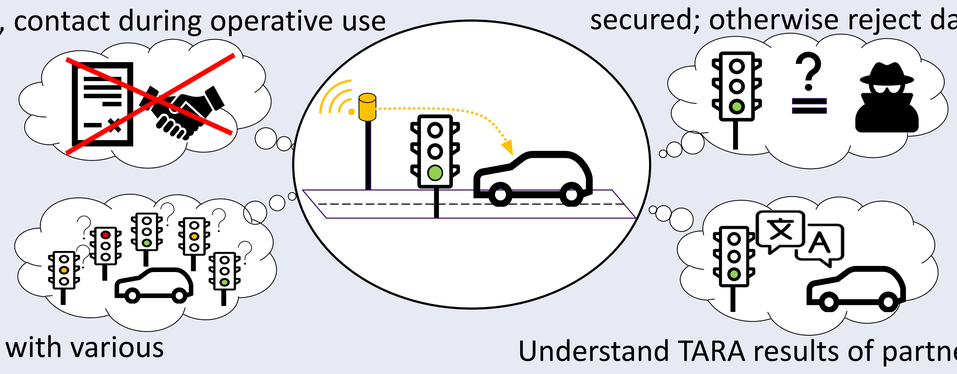
premise	→	threat AFR ↓	×	DS impact	=	risk ↓
Defines a RMRF received data needs to provide in order to be used		*Reduced as the recipient does not have to assume the worst-case regarding the security of the received data*		*Not influenced by the RMRF & PMRF*		*Reduced due to reduced AFR*

Example:

Summary: Approach to secure communication in RDS

No agreement during development needed, contact during operative use

Decide if received data is sufficiently secured; otherwise reject data



Interact with various unknown partners

Understand TARA results of partners using their individual methodology

Outlook: Further challenges

- Extend MRF & TARA with data from further project phases, e.g. design, implementation, test, operation, etc.
- Reduce message size
- Investigate consequences of message size to generation and verification of messages
- Increase maturity: implement concept into real-world applications
- Verify applicability of other Bosch concepts, e.g. Vehicle Trust Anchor

BOSCH · [ˌdiːsɪ arˈtiː] Daimler Center for Automotive IT Innovations · Fraunhofer FOKUS · Fraunhofer IEM · htw saar Forschungsgruppe Verkehrstelematik · infineon · Technische Universität München · TÜV SÜD · universität ulm