Analysis of Safety-critical Communication Protocols for On-premise SIL4 Cloud in Railways

University of Rostock: Benjamin Rother, Frank Golatowski,
Sysgo: Zeeshan Ansar, Don Kuzhiyelil,
Thales: Stefan Resch, Reinhard Hametner, and
Deutsche Bahn: Prashant Pathak

Presenter:

Dr. Frank Golatowski

frank.golatowski@uni-rostock.de

Institute of Applied Microelectronics and Computer Engineering

Agenda

- Introduction
- SIL4 Communication Requirements
- Railway-specific safety-critical Communication Protocols
- Potential SIL4 Communication Protocols
- Safe Communication Architecture for Railway Systems
- Comparision
- Conclusion

Introduction

Motivation

- Which communication protocols are suitable for on-premise cloud environments?
- Safety communication suitable for Safety Integrity Level up to SIL4.
- SIL4-Coud to support safety-critical applications.
- How SIL4-Applications can communicate safely with internal & external systems?

EN 50159 Compliant Protocols

Peer-to-Peer (e.g. RaSTA)

Publish-Subscribe (e.g. ?)

?

Traditional Railway architecture

Future on-premise SIL4 cloud

1. Requirements
2. Potential protocols
3. Integration in proposed system architecture

Universität Rostock Traditio et Innovatio

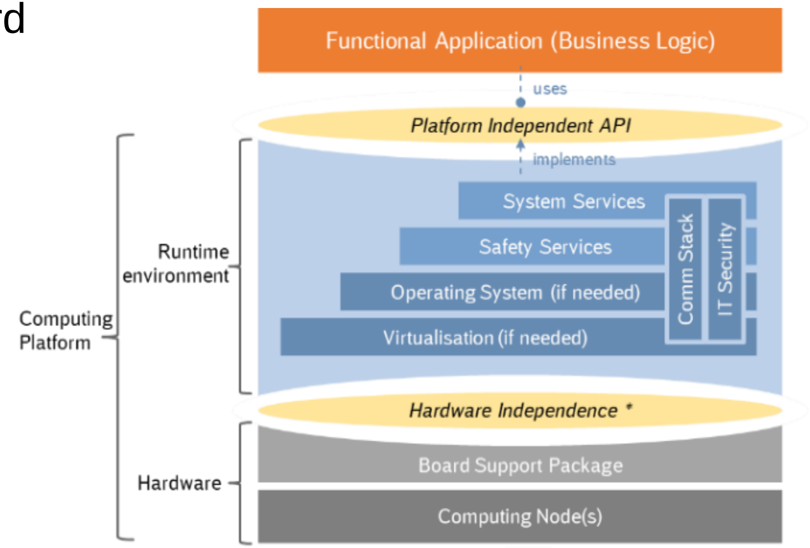
Institute of Applied Microelectronics and Computer Engineering

SIL4 Communication Requirements

Safe Computing Platform

- RCA and OCORA have initiated the work toward a functional Safe Computing Platform (SCP) architecture for a future rail system
  - for onboard and trackside functions
- Functional applications are decoupled from the underlying SCP and isolated from each other.
- PI API approach allows safety-critical railway applications to run unchanged on different SCP implementations

  → Maintaining application portability

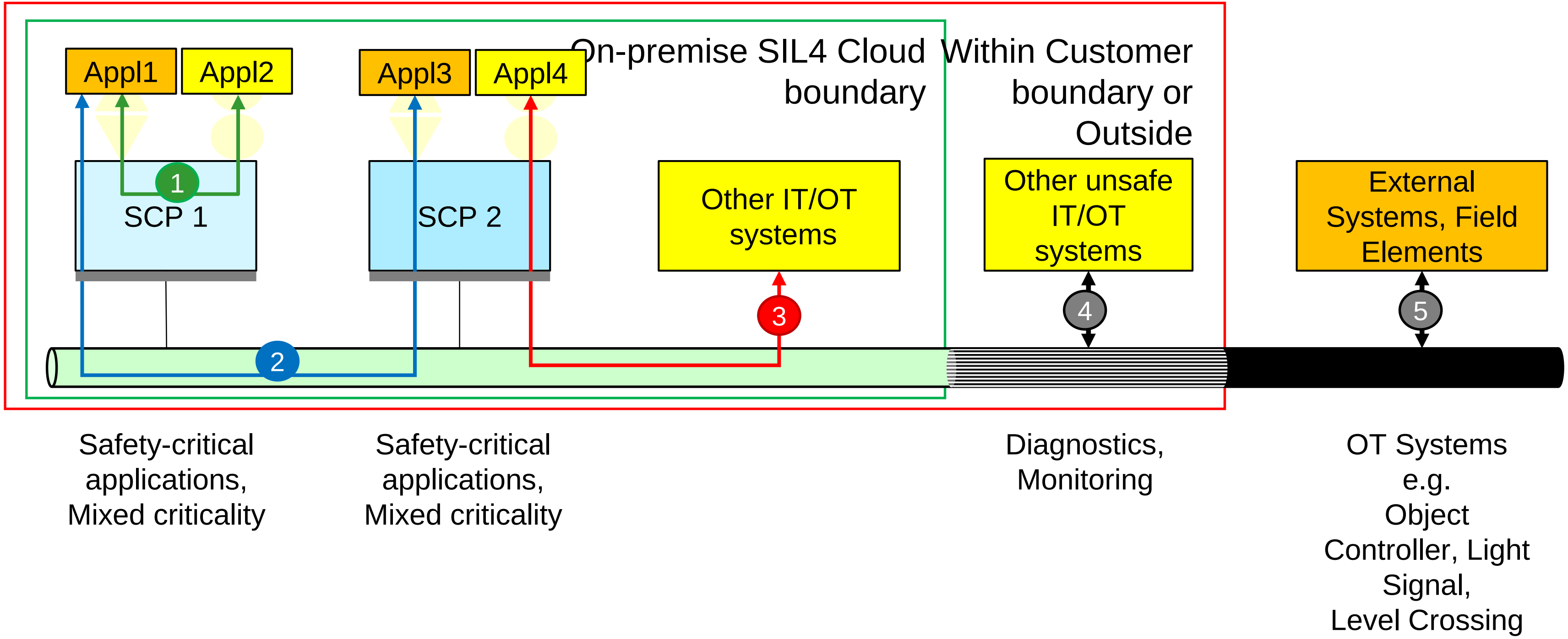


[1]

RCA - **R**eference **C**CS **A**rchitecture (RCA).
OCORA- **O**pen **C**CS **O**n-board **R**eference **A**rchitecture
CCS- Command Control and Signaling

SIL4 Communication Requirements

Communication Categories



SIL4 Communication Requirements

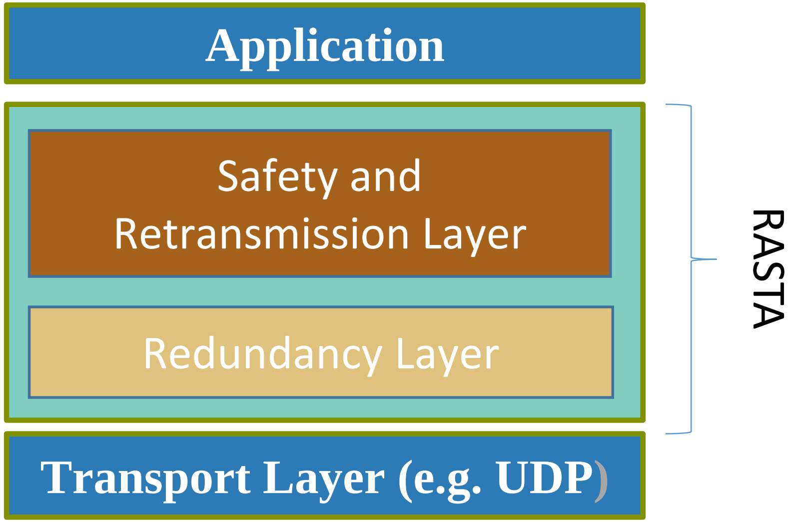
Requirements

- According to the OCORA requirements for the SCP, the following non-exhaustive list of requirements arise for future communication infrastructures:

Requirement	Description
R1	Communication protocol evolves independently from a specific computing platform realization
R2	Computing platform shall support point-to-point, point-to-multipoint and publish-subscribe communication model to support different application communication models
R3	Safe communication should be applied end-to-end, so that the whole communication link between remote functional applications can be considered safe.
R4	Safe communication protocols will be transparent to Functional Applications
R5	The computing platform provides a communication protocol which is based on open and standardized specification to achieve interoperability.

Railway-specific safety-critical Communication Protocols

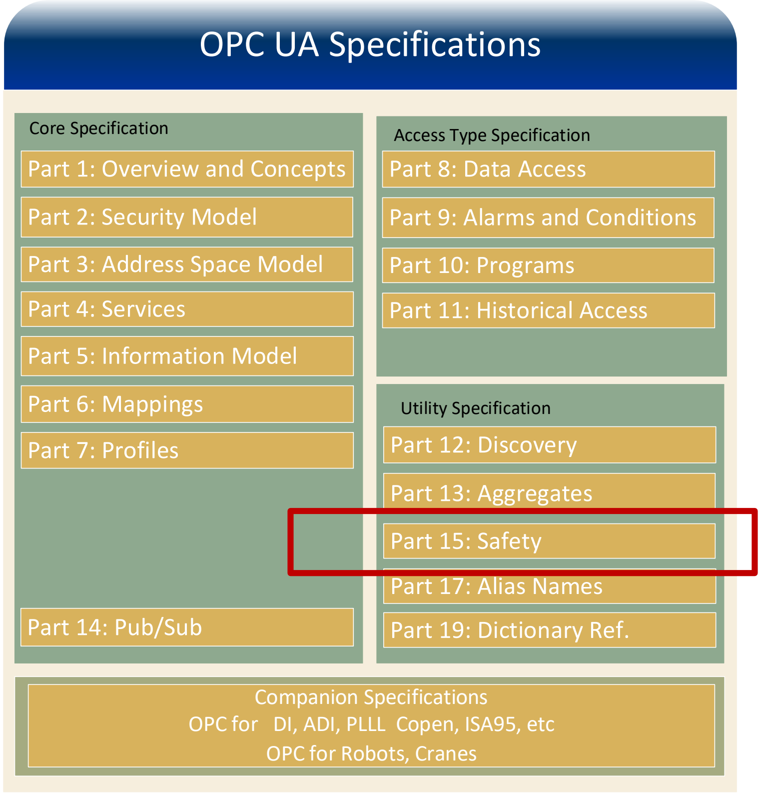
- RaSTA fulfills requirements of EN 50159
- Supports safe data transmission in networks classified as category 1 or 2 (according EN 50159)
- Transmission over cat 3 network →additional means of encryption need to be foreseen
- THALES: Protocol severely restricted in cloud environment
  - Reduced flexibility of P2P protocol
  - Limited integration of security functions
  - → Safe and secure protocols have to be investigated / designed in a cloud environment



Potential SIL4 Communication Protocols

OPC UA

- Set of specifications applicable to software development in industrial domains.
- Systems are intended to exchange information and to use command and control for industrial processes.
- OPC UA defines a common infrastructure model to facilitate this information exchange.
- The specification “OPC UA Safety” describes services and protocols for the exchange of data using OPC UA mechanisms.



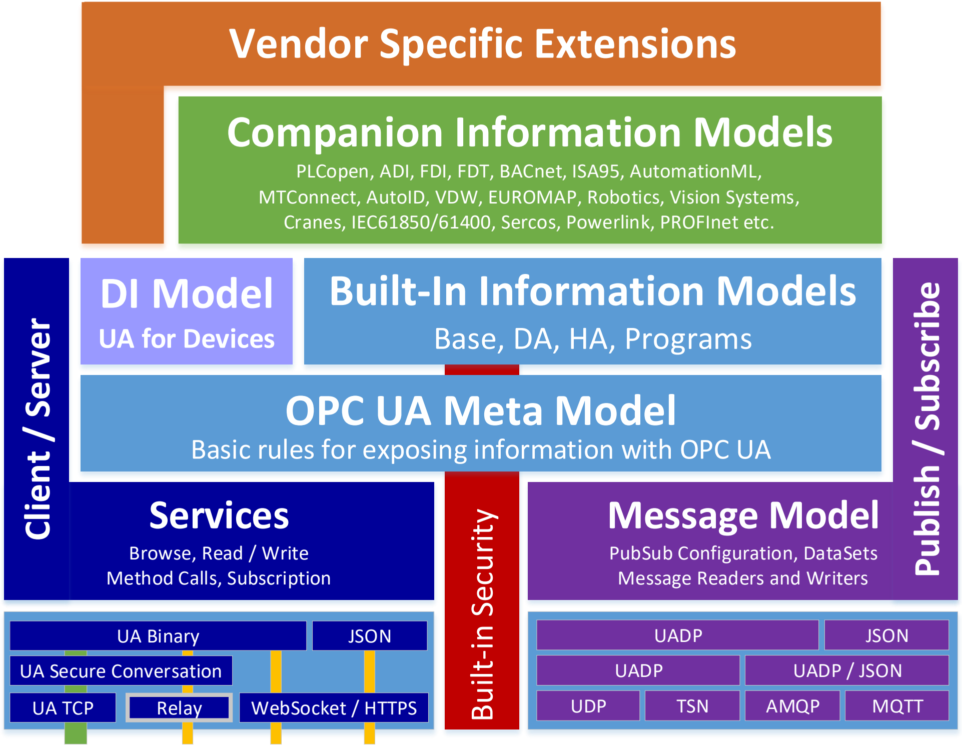
Universität Rostock Traditio et Innovatio

Institute of Applied Microelectronics and Computer Engineering

Potential SIL4 Communication Protocols

OPC UA

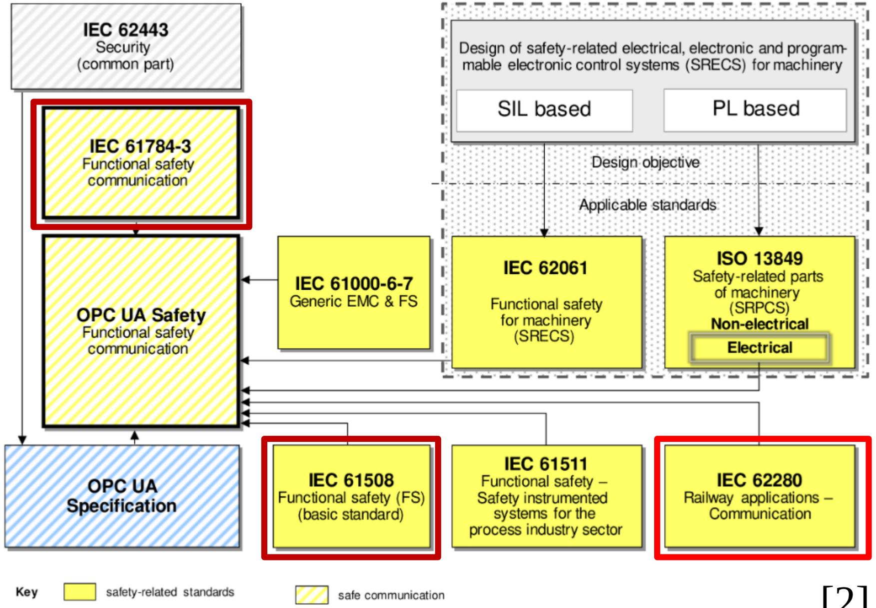
- OPC UA, is a *platform independent* **service oriented architecture** that integrates all the functionality of the individual OPC UA specifications into one extensible framework.



Potential SIL4 Communication Protocols

OPC UA

- OPC UA Safety extends OPC UA to fulfill functional safety requirements as defined in the IEC 61508 and IEC 61784-3 standards.
  - IEC 61508 is the basis of many derived standards in functional safety context therefore it should be considered as feasible to use OPC UA Safety as well in railway domain
  - IEC 62280 (EN50159)



[2]

"OPC UA Safety specifies a safety communication layer (SCL) allowing safety-related devices to use the services of OPC Unified Architecture (OPC UA) for the safe exchange of safety-related data." [2]

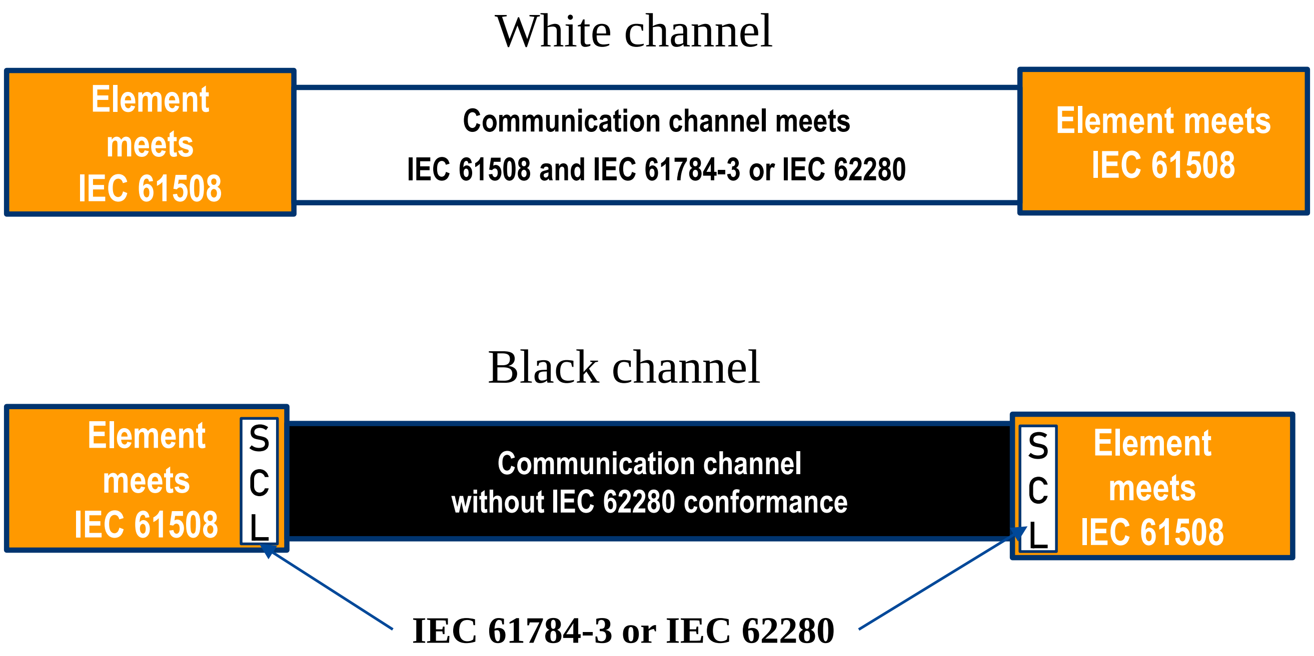
Potential SIL4 Communication Protocols

DDS

- Open standard DDS middleware provides a data centric connectivity framework
  - based on a publish-subscribe model for a real-time system
- DDS-RTPS protocol: (real-time publish-subscribe)
  - enables seamless interoperability across vendor implementations, programming languages and platforms.
- DDS enables modular application development and reliable and real-time data exchange
- QoS mechanism to ensure reliability
  - detect communication errors i.e. lost messages, data corruption
- Additional features for security: access control, data flow path enforcement and data encryption

DDS's comprehensive QoS and security mechanisms make it a potential candidate for safe communication in railways.

Black communication channel

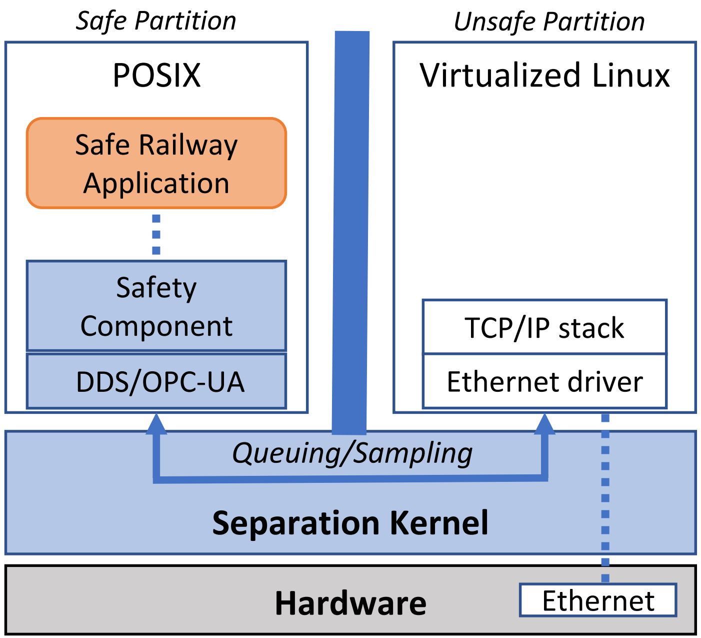


SCL: safe communication layer

Source: https://www.functional-safety.solutions/

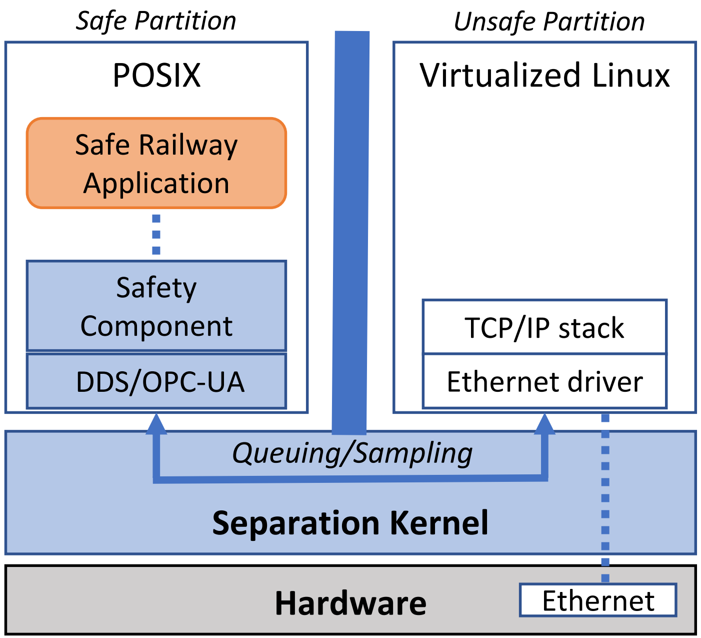
Safe Communication Architecture for Railway Systems

- Safe partition
  - communication middleware such as DDS or OPC UA
  - with a POSIX runtime
  - along with the safety-critical railway application,
  - and safety component
- Unsafe partion
  - TCP/IP stack and Ethernet driver inside an unsafe virtualized Linux partition
  - which provides the black channel
- Separation kernel
  - isolates the safety-critical partition from the non-safety-critical partition
  - applications running inside these partitions are allowed to communicate via inter-partition queuing/sampling ports provided by the separation kernel.



Safe Communication Architecture for Railway Systems

- DDS/OPC UA middleware framework running inside the safe partition on a separation kernel provides a Modular Open Systems Approach (MOSA)
- It creates a common data communication framework for railway applications that can communicate across any data transport while providing fault tolerance, resiliency and security



Comparation of OPC UA and DDS

Basic Features

DDS

- Publish Subscribe Pattern
- Data Centric Approach
- Guaranteed Real Time Response
- Relational Data Model
- Easy Integration of Software Modules

OPC UA

- Client Server & Publish/Subscribe
- Device Centric

- Object Oriented Data Model
- Simpler Software for Device Interchangeability

Comparison of Safety Protocols

	RaSTA	DDS	OPC UA Safety
Communication Pattern PubSub architecture	P2P	PubSub, Point-to-Multipoint	PubSub, Point-to-Multipoint
EN 50159 key properties (Authenticity, Integrity, Timeliness, Sequence)	supported	supported	supported
Open Standard with strong international support	No (used in Railway industry)	Yes	Yes
Safety features (excerpt)	- Black channel principle - Detection of communcation errors	- Black channel principle - Changing communication partner during runtime - Detection of communication errors	- Black channel principle - Changing communication partner during runtime - Detection of communication errors - Safety multicast
Security features	Limited (Secure Code)	Extensive (Authentication, access control, cryptography, logging)	Adequate (Secure Channel)

Evaluation

- Proposed safe communication architecture fulfils all requirements R1 to R5 with the integration of potential SIL4 communication protocols
  - support different communication pattern with the integration of DDS and OPC UA Safety (R2)
  - allows for changing the safety communication partners at runtime by transparently exchanging data (R4)
- DDS and OPC UA protocols are based on an open standard and have strong international support (R5)
- By covering the EN 50159 key properties, they are potential candidates for the railway sector
- With suitable safety measures, which have to be integrated into the application appropriately, OPC UA and DDS are able to support communications up to SIL4 (R3)
- OPC UA supports semantic interoperability and large-scale application scenarios and is therefore suitable for EN 50159 category 1 and 2 networks

Conclusion

- Comparison of potential application layer communication protocols from industrial domains with a railway-specific safety-critical protocols
- OPC UA and DDS protocols have the potential to be used in on-premise SIL4 cloud for safety-critical communication
- Safe communication architecture for railway was presented
- Safety-critical communication protocols needs to be examined further

Thank you for your attention

Frank.Golatowski@uni-rostock.de

References

[1] An Approach for a Generic Safe Computing Platform for Railway Applications, https://github.com/OCORA-Public/, (accessed Jan. 28, 2022).

[2] OPCFoundation, “OPC 10000-15 Unified Architecture Part 15 Safety,” OPC UA Online Reference. https://reference.opcfoundation.org/v104/Safety/docs/ (accessed Apr. 04, 2022).

Universität Rostock Traditio et Innovatio

Institute of Applied Microelectronics and Computer Engineering