HIS 2022
HIGH INTEGRITY SOFTWARE CONFERENCE
#HISConf2022
his-conference.co.uk

RCA OCORA Safe Computing Platform Using Open Standards

Angel Martinez
Senior Software Engineer
Real-Time Innovations (RTI)

Mario Brotz
Director R&T
SYSGO GmbH

October 11, 2022

Agenda

1. Welcome and introduction
2. RCA/OCORA Safe Computing Platform (SCP)
3. SCP Overview, including virtualization
4. SCP communication realized with DDS
5. Applicability to other use cases
6. Summary
7. Q&A

Who are we?

- RTI develops the #1 software framework for autonomy
  - DDS-based connectivity framework enables real-time communication in systems at scale, including safety-certified systems
  - Headquarters in Silicon Valley with offices in Colorado, Granada and Singapore
  - 1800+ designs, 750+ research programs across industries

- SYSGO is the leading European operating system vendor for embedded systems
  - 30 years experience in certification of complex systems with high safety and security requirements
    - Part of the Thales Group since 2012
  - Headquarters near Mainz, Germany
  - Solutions in Avionics, Automotive, Defense, Industrial, Medical, Railway and Space markets

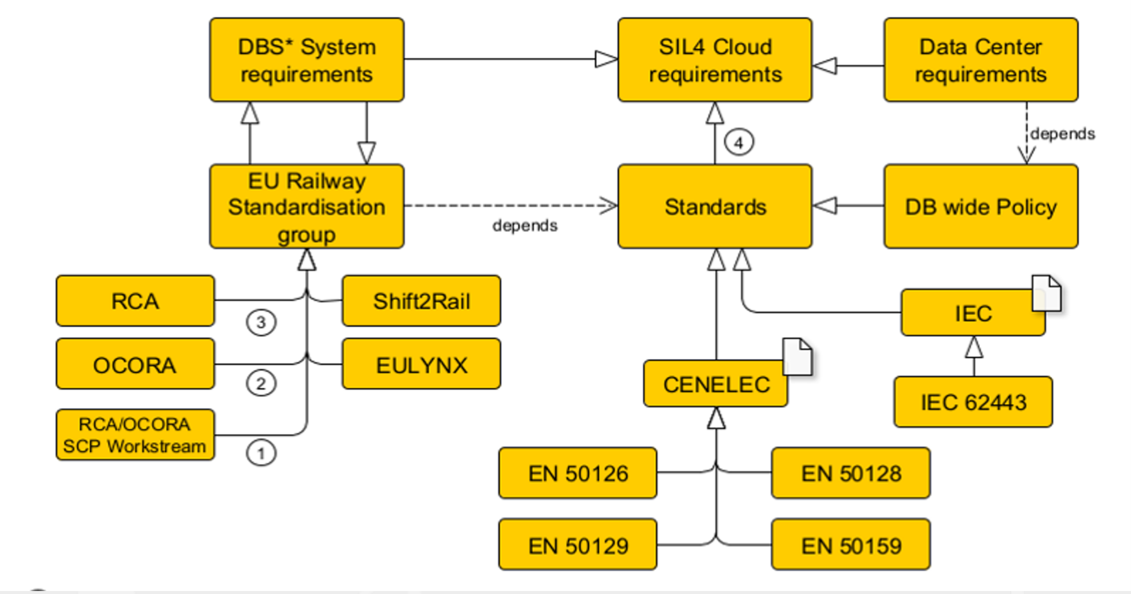
SYSGO EMBEDDING INNOVATIONS

rti

RCA and OCORA: Transforming Digital Operations via Safe Computing Platform

- RCA and OCORA consortia (European Rail Operators) has a vision to encapsulate Safety applications from the underlying compute platform.

- After consolidating requirements for railway track side and rolling stock applications, a vision of a Safe Computing Platform (SCP) was born.



- SYSGO and RTI among many other industry partners have contributed in consecutive specification work to refine and detail a SCP specification.

SYSGO EMBEDDING INNOVATIONS

rti

Digital Transformation of Railway Applications – Trend and Motivation

- Fact: Higher loads on Passenger and Cargo for rail infrastructure moving forward
- New applications that are needed:
  - AI based traffic management
  - Automated train operation up to GOA4 with environmental perception and localization
  - Command, Control and signaling for ETCS level 3 moving block
  - Fully automated incident and prevention, mitigation and resolution
  - Establishment of private cloud infrastructure to accommodate SIL4 applications and reduction of Total Cost of Ownership

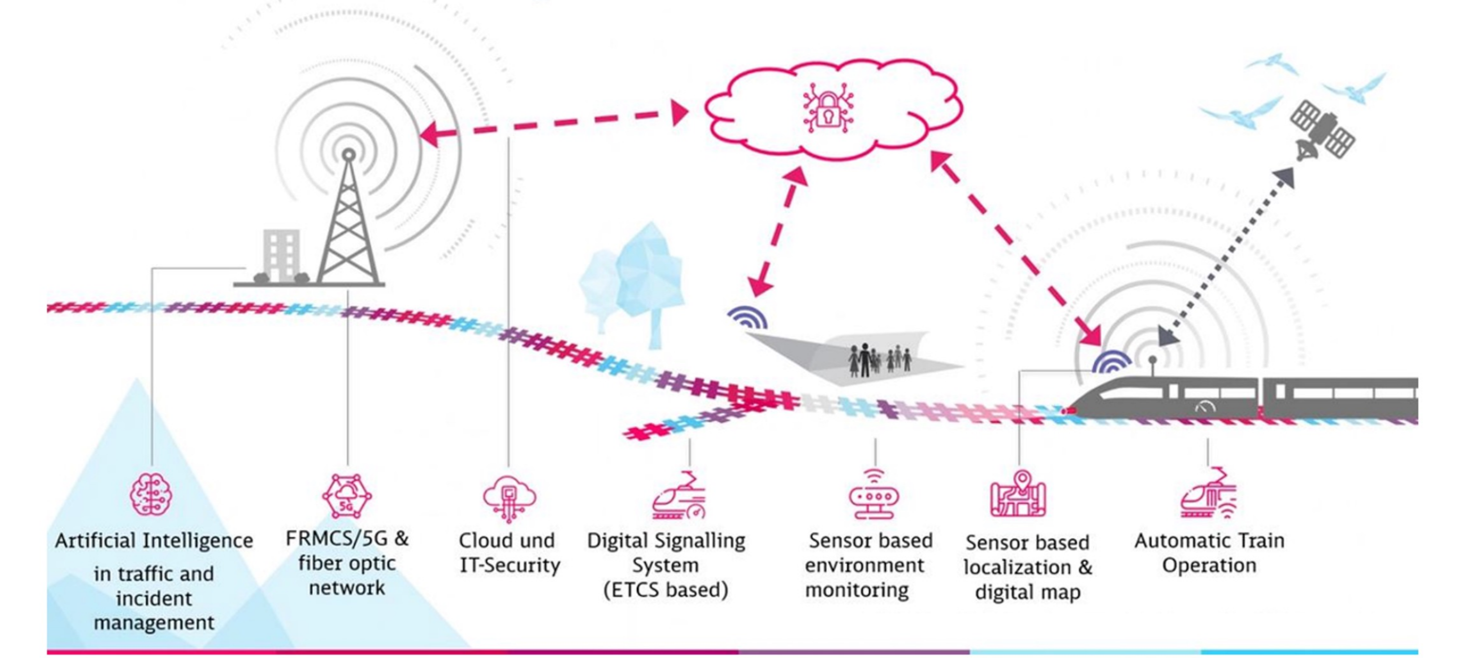
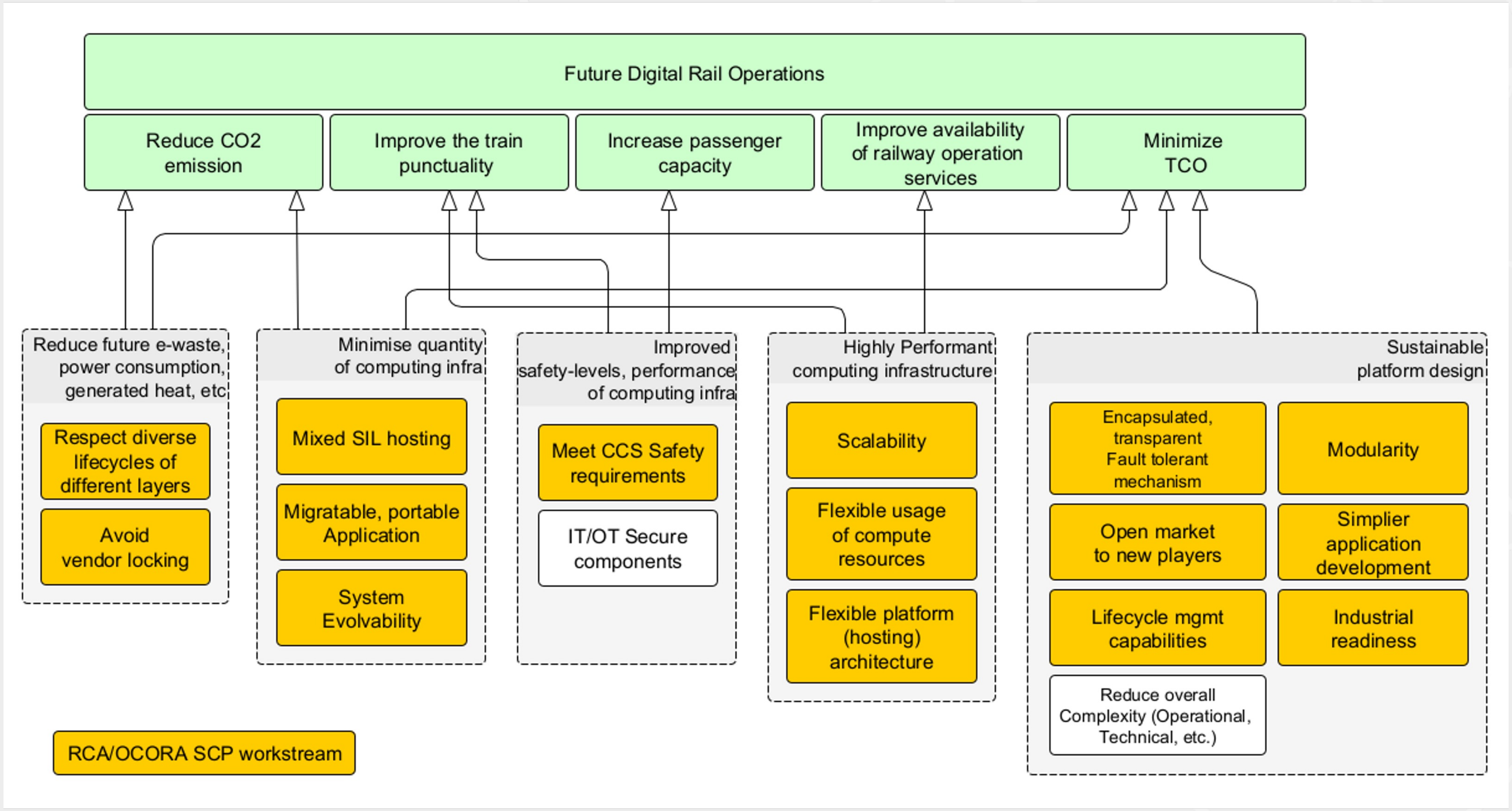

Artificial Intelligence in traffic and incident management
FRMCS/5G & fiber optic network
Cloud und IT-Security
Digital Signalling System (ETCS based)
Sensor based environment monitoring
Sensor based localization & digital map
Automatic Train Operation

Figure 1: Essential technologies needed for future rail operation

Resulting Requirements from the RCA/OCORA Workstreams



Future Digital Rail Operations

Reduce CO2 emission

Improve the train punctuality

Increase passenger capacity

Improve availability of railway operation services

Minimize TCO

Reduce future e-waste, power consumption, generated heat, etc

- Respect diverse lifecycles of different layers
- Avoid vendor locking

Minimise quantity of computing infra

- Mixed SIL hosting
- Migratable, portable Application
- System Evolvability

Improved safety-levels, performance of computing infra

- Meet CCS Safety requirements
- IT/OT Secure components

Highly Performant computing infrastructure

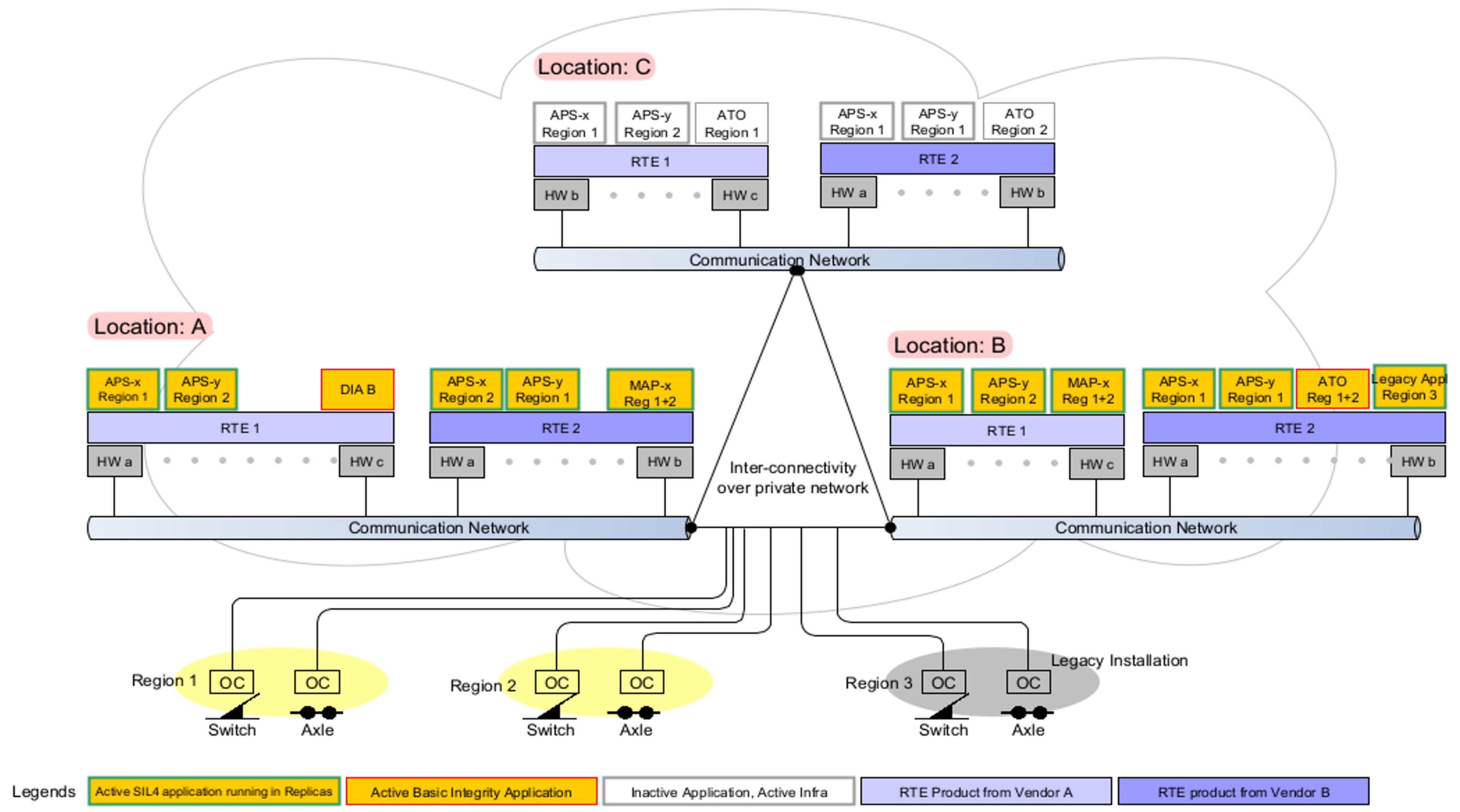
- Scalability
- Flexible usage of compute resources
- Flexible platform (hosting) architecture

Sustainable platform design

- Encapsulated, transparent Fault tolerant mechanism
- Modularity
- Open market to new players
- Simplier application development
- Lifecycle mgmt capabilities
- Industrial readiness
- Reduce overall Complexity (Operational, Technical, etc.)

RCA/OCORA SCP workstream

Safe Computing Platform: A SIL4 Cloud overview for Trackside Applications



A Hypervised-based Approach of a Safe Compute Platform (SCP)

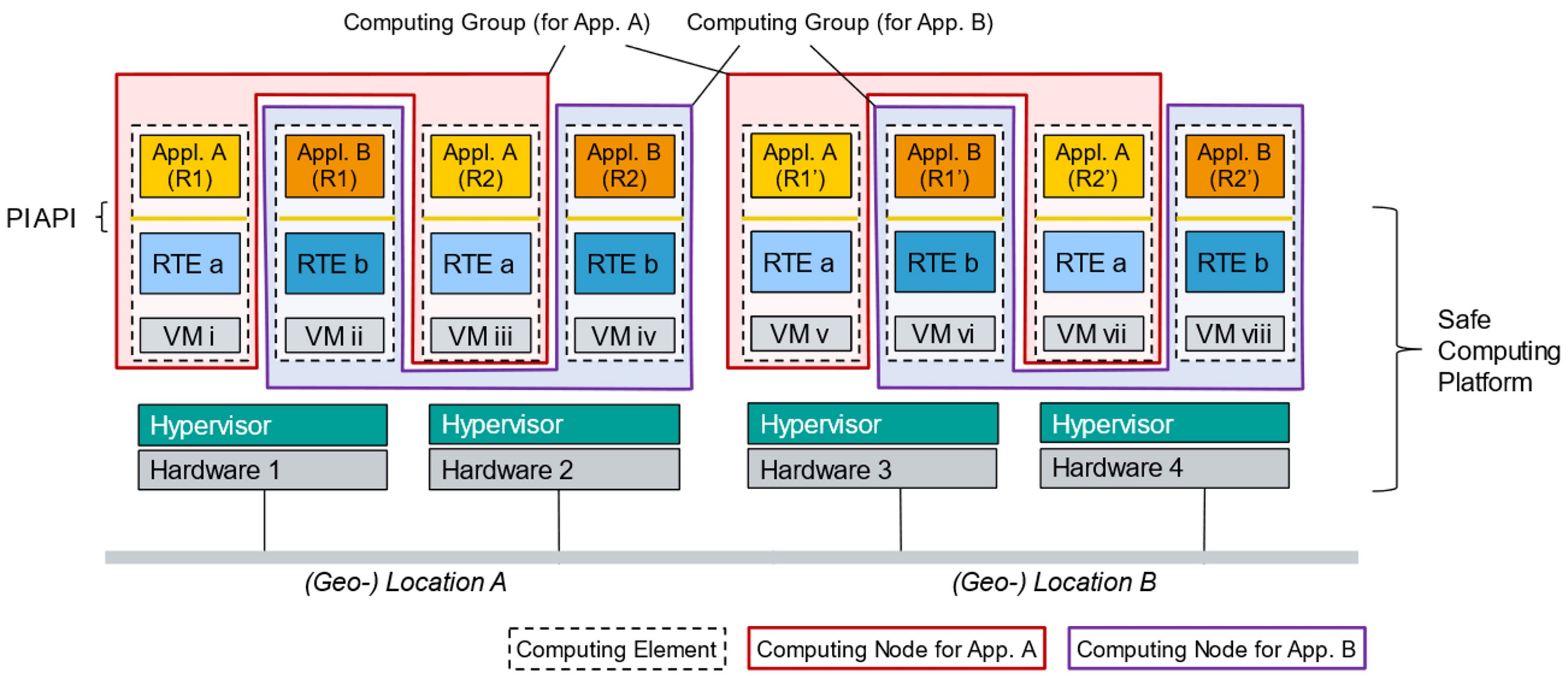
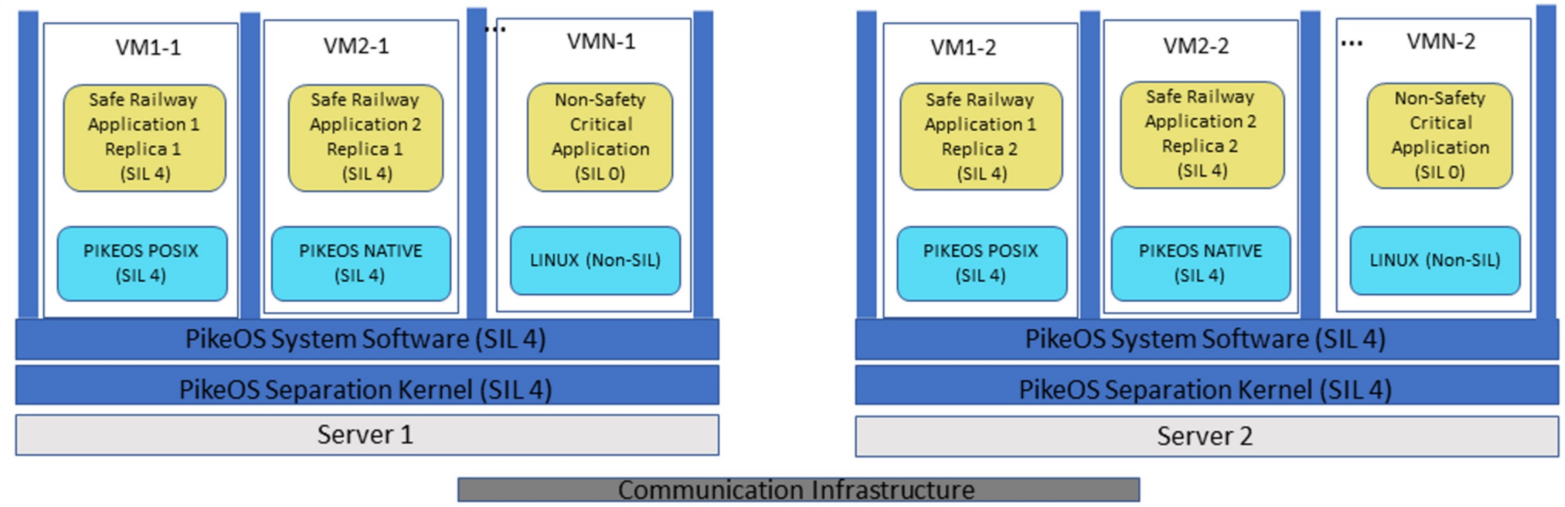


Figure 11: Layers with Virtualisation/Hypervisor for 2 applications each in a 2x2oo2 configuration

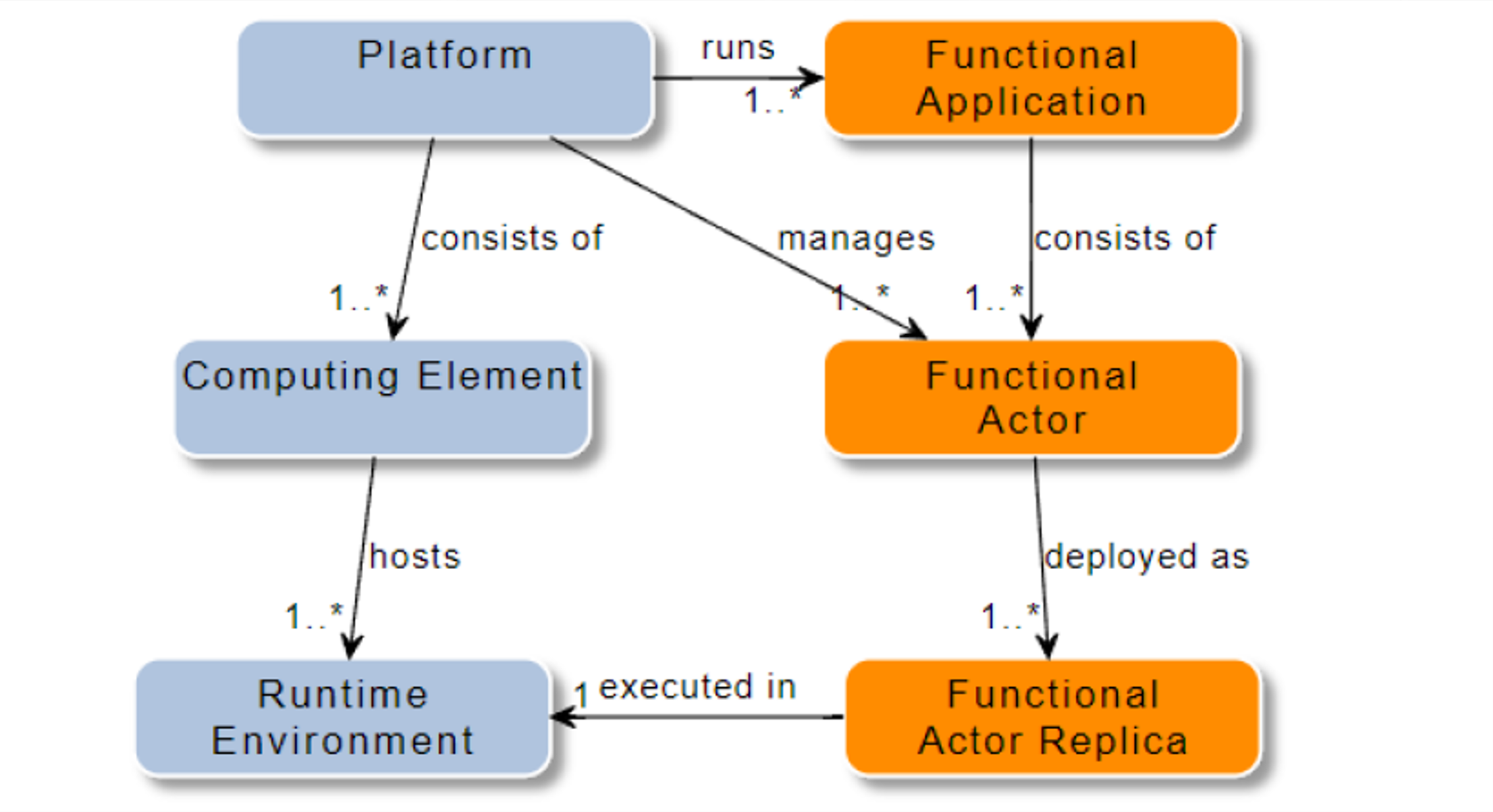
PikeOS as SCP building block

- Hard Real-Time Operating System and Hypervisor (Type 1)
  - Safe and secure virtualization (HW and para)
  - Mixed criticality with multiple guest operating systems
  - Highly portable supporting all important CPU architectures
  - RTOS performance and determinism
- Certifiable
  - According to highest Safety and Security standards
  - Modular certification kits for Railway, Aerospace and Defense, Automotive, Industrial and Medical


VM1-1
Safe Railway Application 1 Replica 1 (SIL 4)
PIKEOS POSIX (SIL 4)
VM2-1
Safe Railway Application 2 Replica 1 (SIL 4)
PIKEOS NATIVE (SIL 4)
...
VMN-1
Non-Safety Critical Application (SIL 0)
LINUX (Non-SIL)
PikeOS System Software (SIL 4)
PikeOS Separation Kernel (SIL 4)
Server 1
VM1-2
Safe Railway Application 1 Replica 2 (SIL 4)
PIKEOS POSIX (SIL 4)
VM2-2
Safe Railway Application 2 Replica 2 (SIL 4)
PIKEOS NATIVE (SIL 4)
...
VMN-2
Non-Safety Critical Application (SIL 0)
LINUX (Non-SIL)
PikeOS System Software (SIL 4)
PikeOS Separation Kernel (SIL 4)
Server 2
Communication Infrastructure

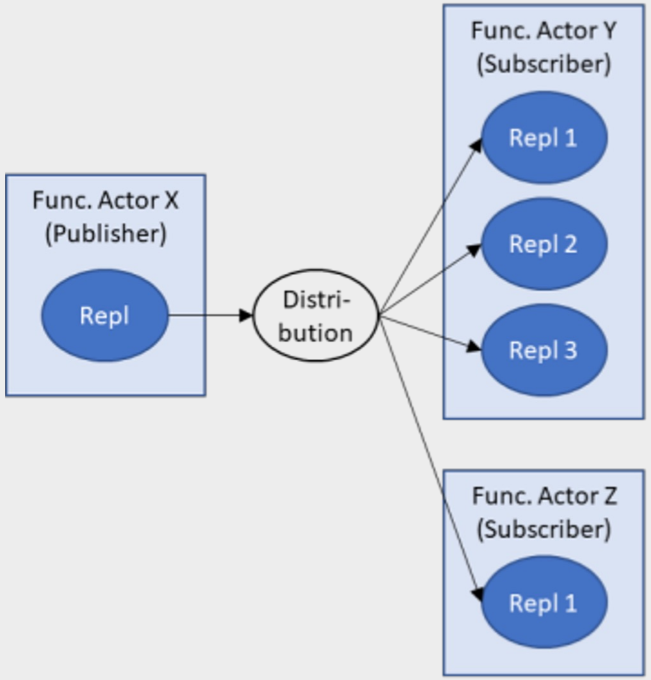
- Multi-Core Performance and Certification
  - Certified according to highest Safety & Security standards on multi-core systems
  - **EN 50128:** PikeOS 4.2 is certified up SIL 2 and PikeOS 5.1 up to SIL 4
  - **Common criteria** separation kernel PikeOS 4.2 for EAL 3+ (next in prep.)
  - Multiple highest level certification artefacts available from ISO 26262 to DO178C DAL A

A Closer Look at the Platform Independent Notions: Replicas for Redundancy

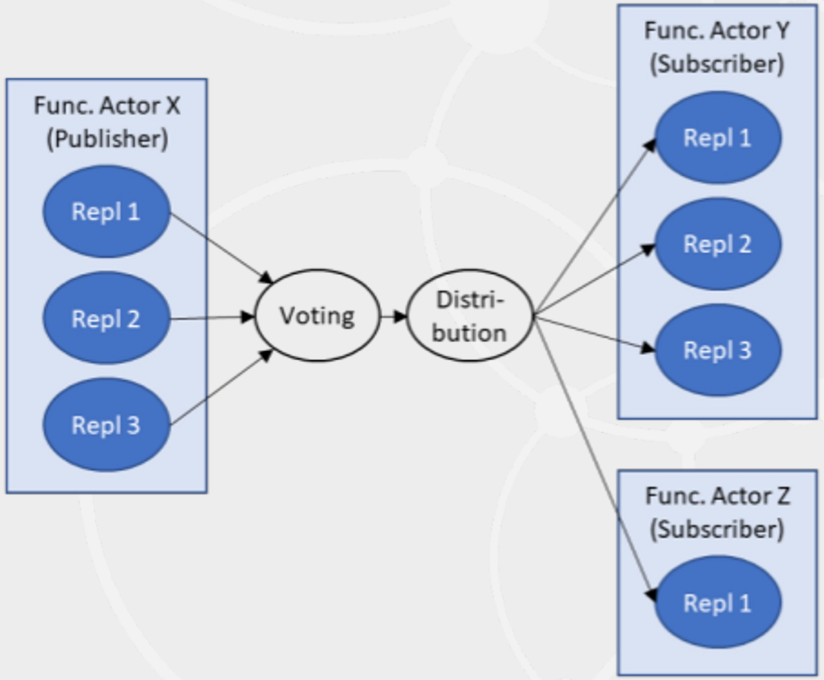


Messaging: Unidirectional Flow (Publish/Subscribe)

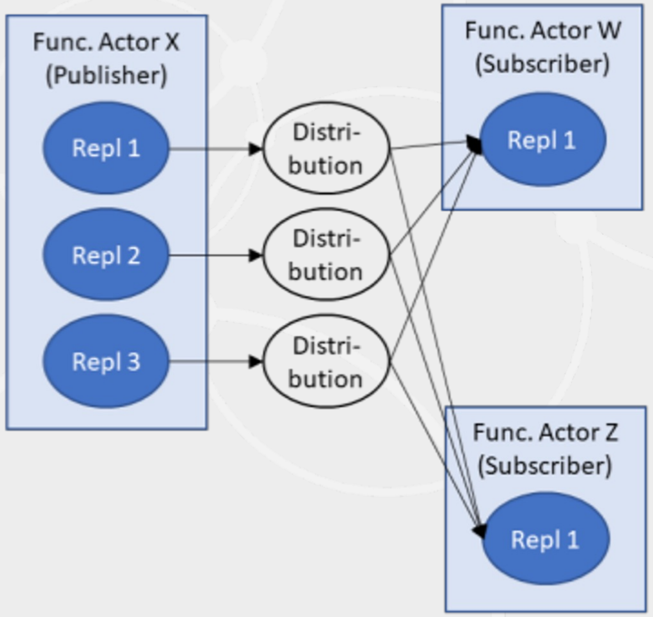
1) Publisher not run in replicas, consequently no voting applied


Func. Actor X (Publisher)
Repl
Distri-bution
Func. Actor Y (Subscriber)
Repl 1
Repl 2
Repl 3
Func. Actor Z (Subscriber)
Repl 1

2) Publisher run in replicas, voting applied

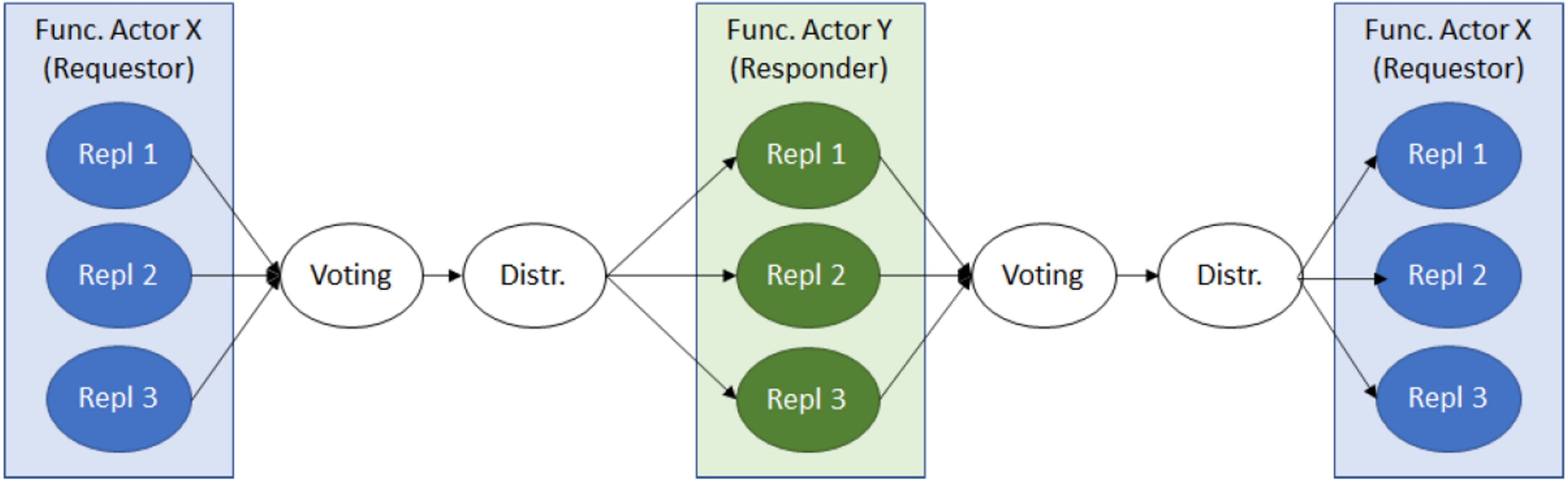

Func. Actor X (Publisher)
Repl 1
Repl 2
Repl 3
Voting
Distri-bution
Func. Actor Y (Subscriber)
Repl 1
Repl 2
Repl 3
Func. Actor Z (Subscriber)
Repl 1

3) Publisher run in replicas, no voting applied (e.g., for logging / diagnostics purposes)

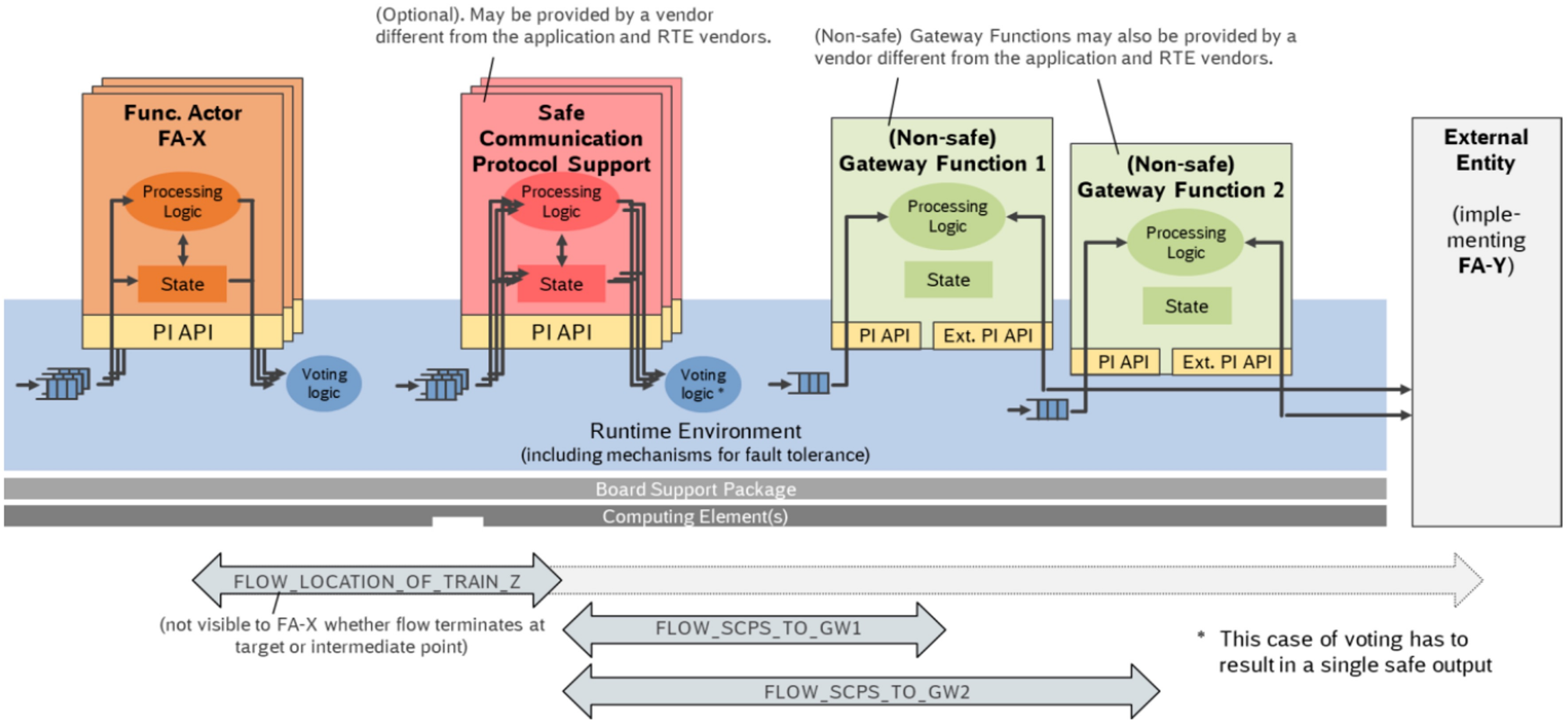

Func. Actor X (Publisher)
Repl 1
Repl 2
Repl 3
Distri-bution
Distri-bution
Distri-bution
Func. Actor W (Subscriber)
Repl 1
Func. Actor Z (Subscriber)
Repl 1

Note: While omitted from the figure for brevity, the displayed options would also apply in the case of multiple publishers and any constellation of subscribers

Messaging: Bi-directional Flow (Request/Response)



Gateway approach



(Optional). May be provided by a vendor different from the application and RTE vendors.
(Non-safe) Gateway Functions may also be provided by a vendor different from the application and RTE vendors.
Func. Actor FA-X
Processing Logic
State
PI API
Voting logic
Safe Communication Protocol Support
Processing Logic
State
PI API
Voting logic *
(Non-safe) Gateway Function 1
Processing Logic
State
PI API
Ext. PI API
(Non-safe) Gateway Function 2
Processing Logic
State
PI API
Ext. PI API
External Entity
(imple-menting FA-Y)
Runtime Environment
(including mechanisms for fault tolerance)
Board Support Package
Computing Element(s)
FLOW_LOCATION_OF_TRAIN_Z
(not visible to FA-X whether flow terminates at target or intermediate point)
FLOW_SCPS_TO_GW1
FLOW_SCPS_TO_GW2
* This case of voting has to result in a single safe output

Gateway Interactions

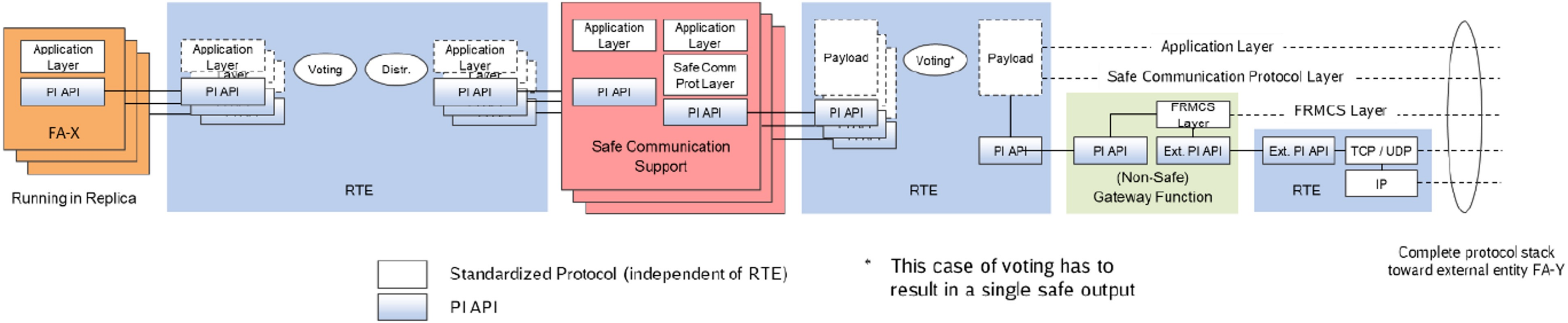
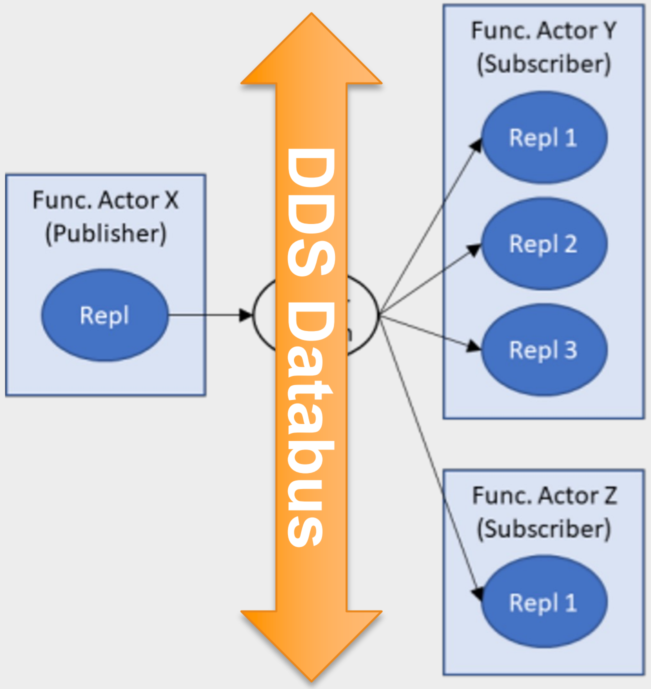


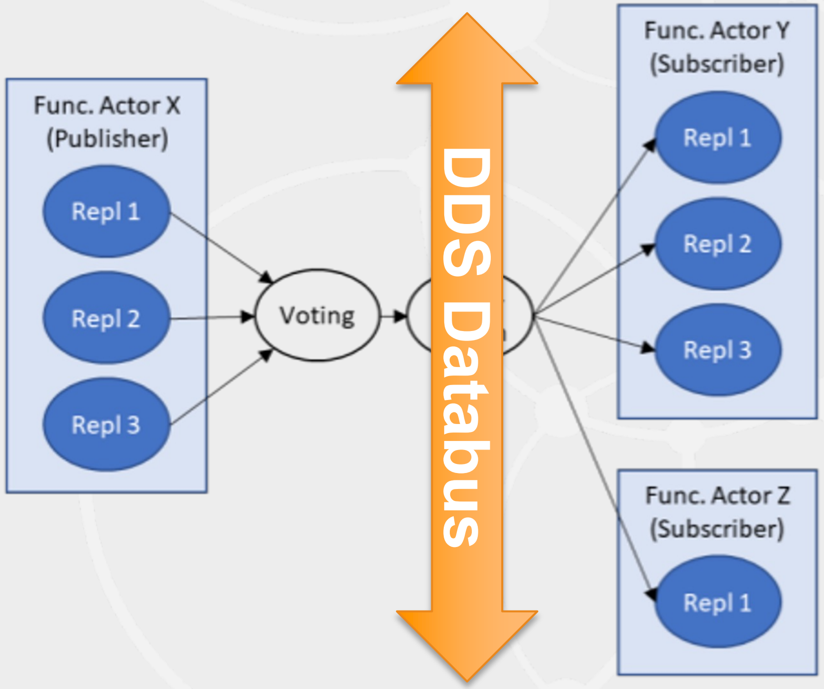
Figure 15. Contribution of the involved entities in the protocol stack used toward the external entity.

Messaging: Unidirectional Flow (Publish/Subscribe)

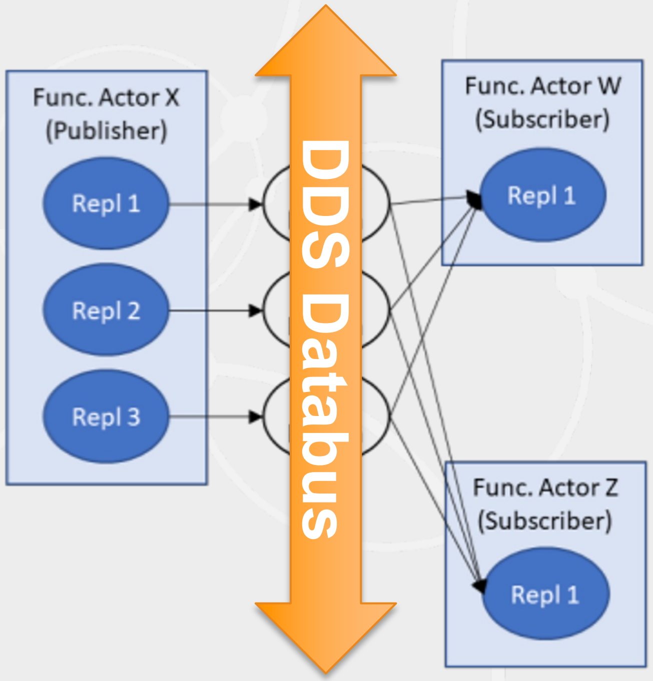
1) **Publisher not run in replicas, consequently no voting applied**



2) **Publisher run in replicas, voting applied**

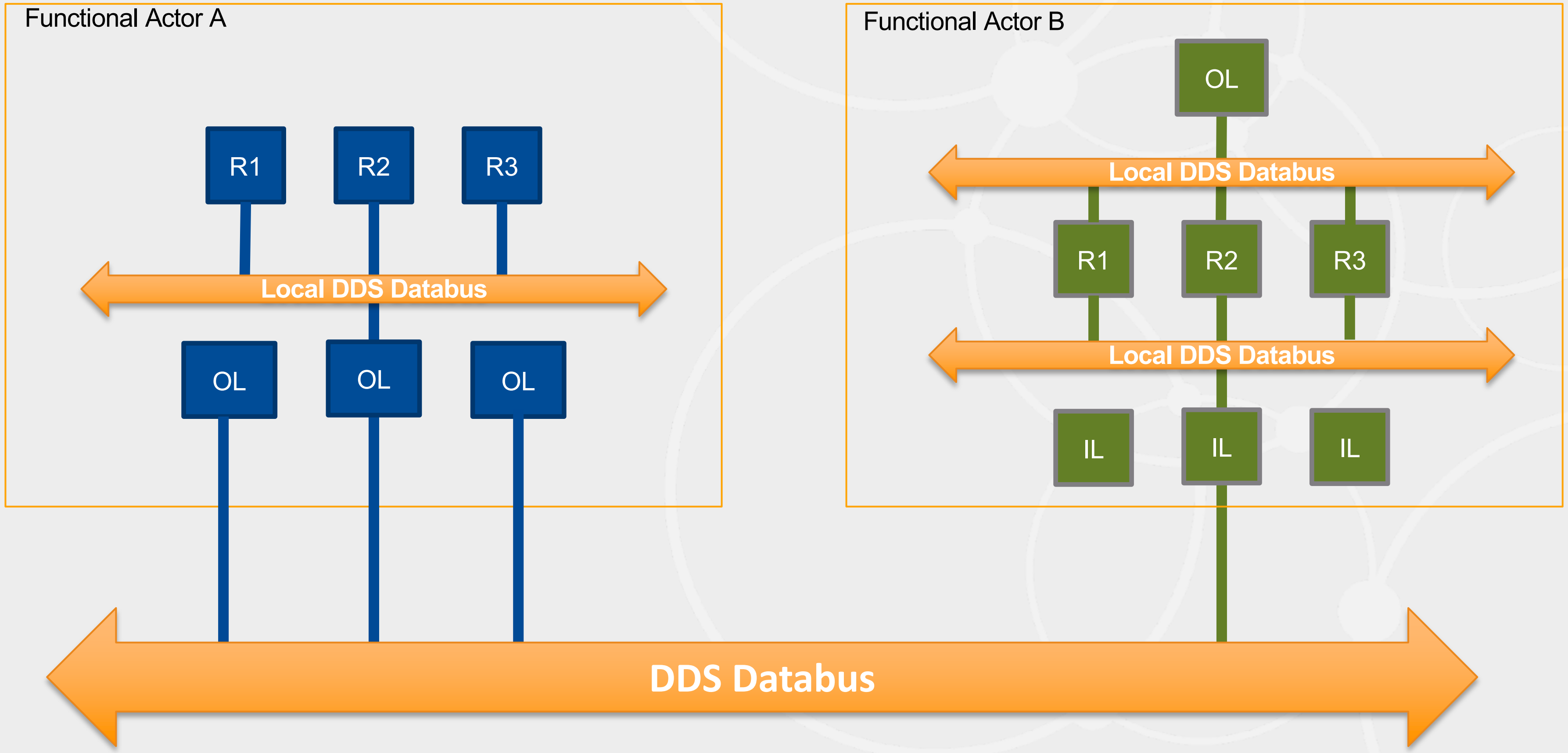


3) **Publisher run in replicas, no voting applied (e.g., for logging / diagnostics purposes)**



Note: While omitted from the figure for brevity, the displayed options would also apply in the case of multiple publishers and any constellation of subscribers

SCP Architecture with DDS Databus (example)



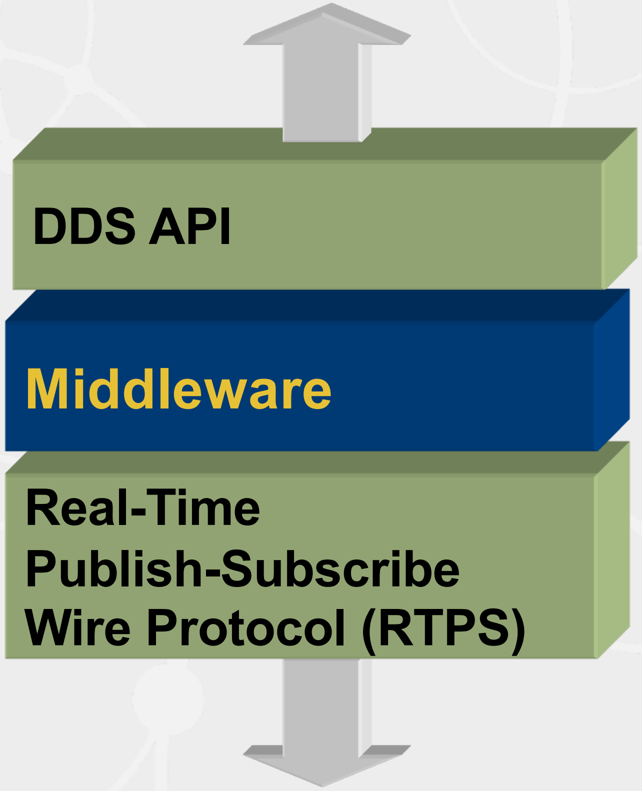
OL: Output Logic
IL: Input Logic
RX: Replica X

OL and IL may include voting logic

Data Distribution Service® (DDS™)

- OMG® Standard
  - – APIs for portability
  - – Wire Protocol for interoperability
- Automatic Discovery
- Peer to Peer (no broker)
- Data-Centric Publish-Subscribe
- Quality of Service Configuration

Cross-vendor portability



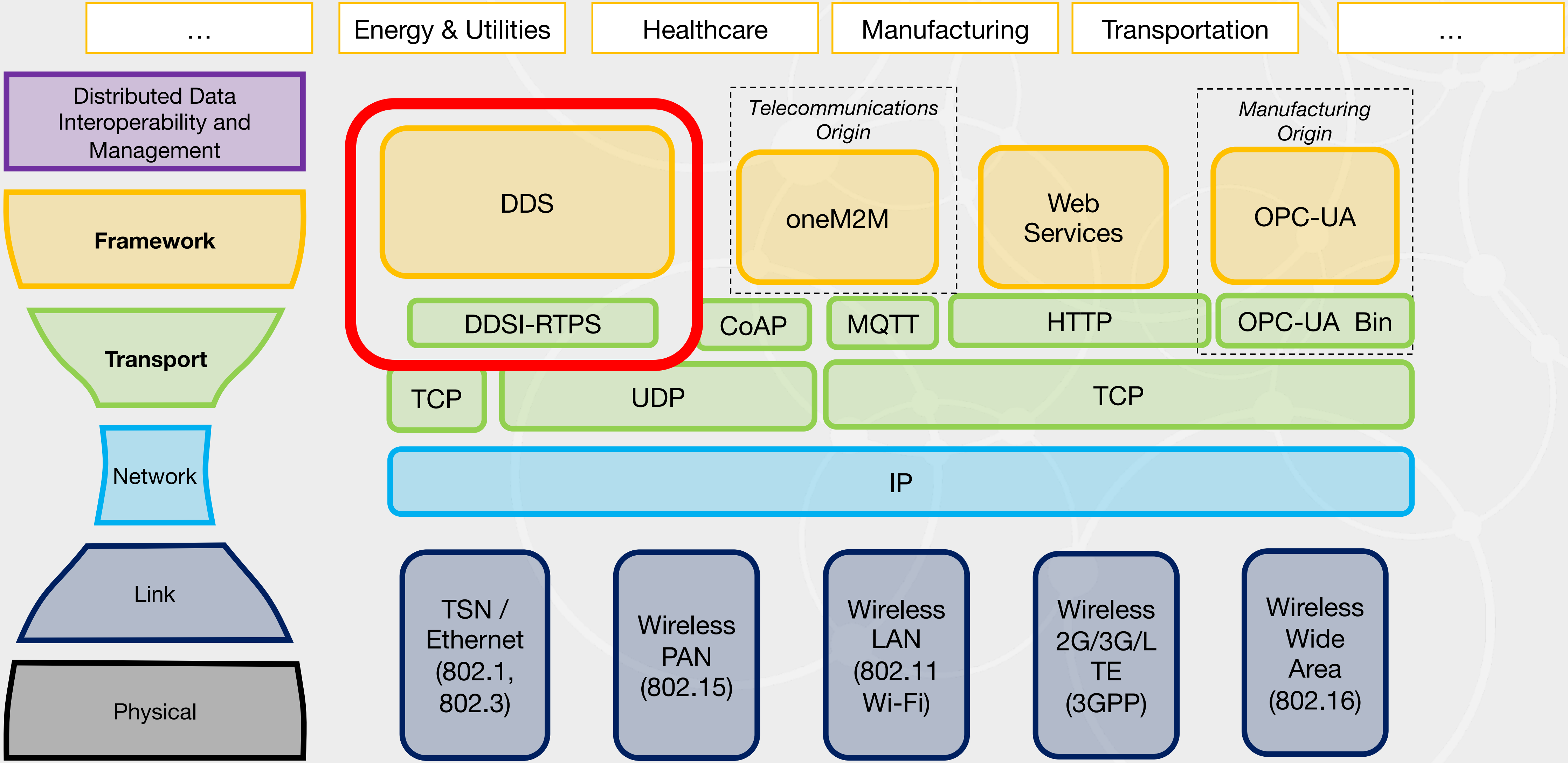
DDS API

Middleware

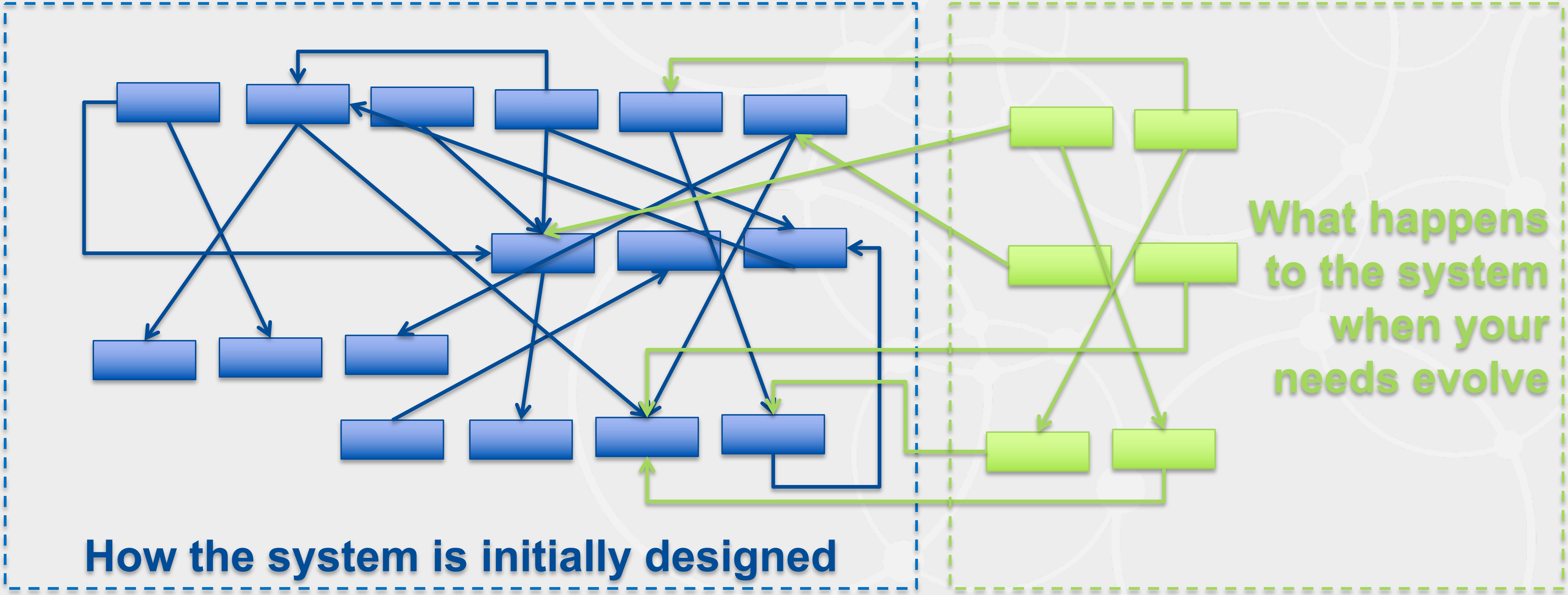
Real-Time Publish-Subscribe Wire Protocol (RTPS)

Cross-vendor interoperability

Key Connectivity Standards Positioned on the Stack



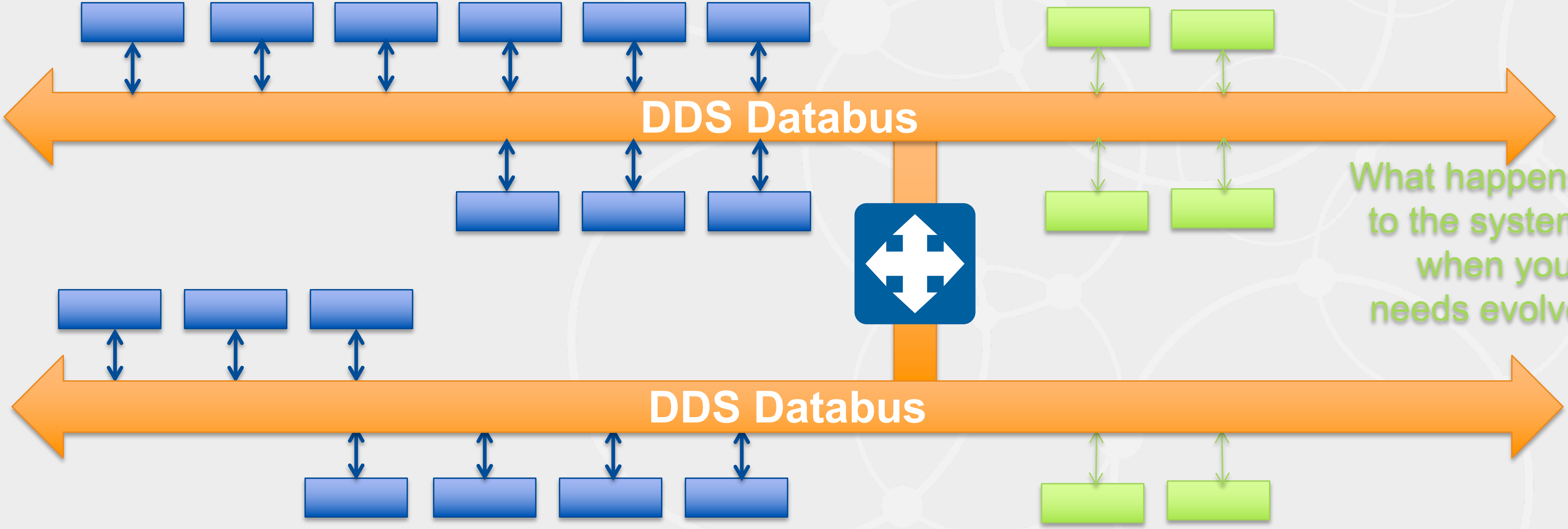
Challenges in Traditional Message-Centric Architectures



How the system is initially designed

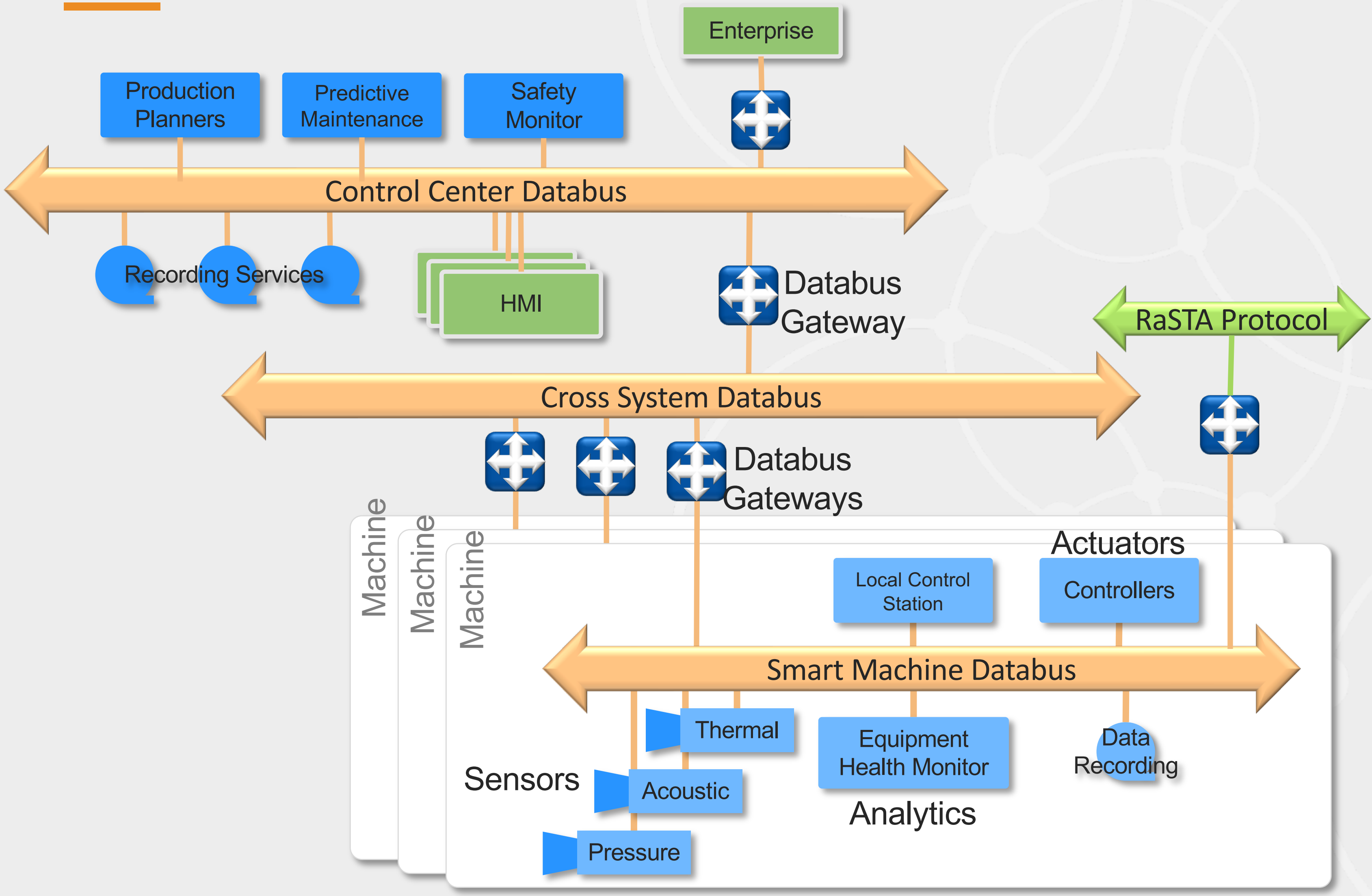
What happens to the system when your needs evolve

DDS enables the Flexibility needed for Future-proof Design



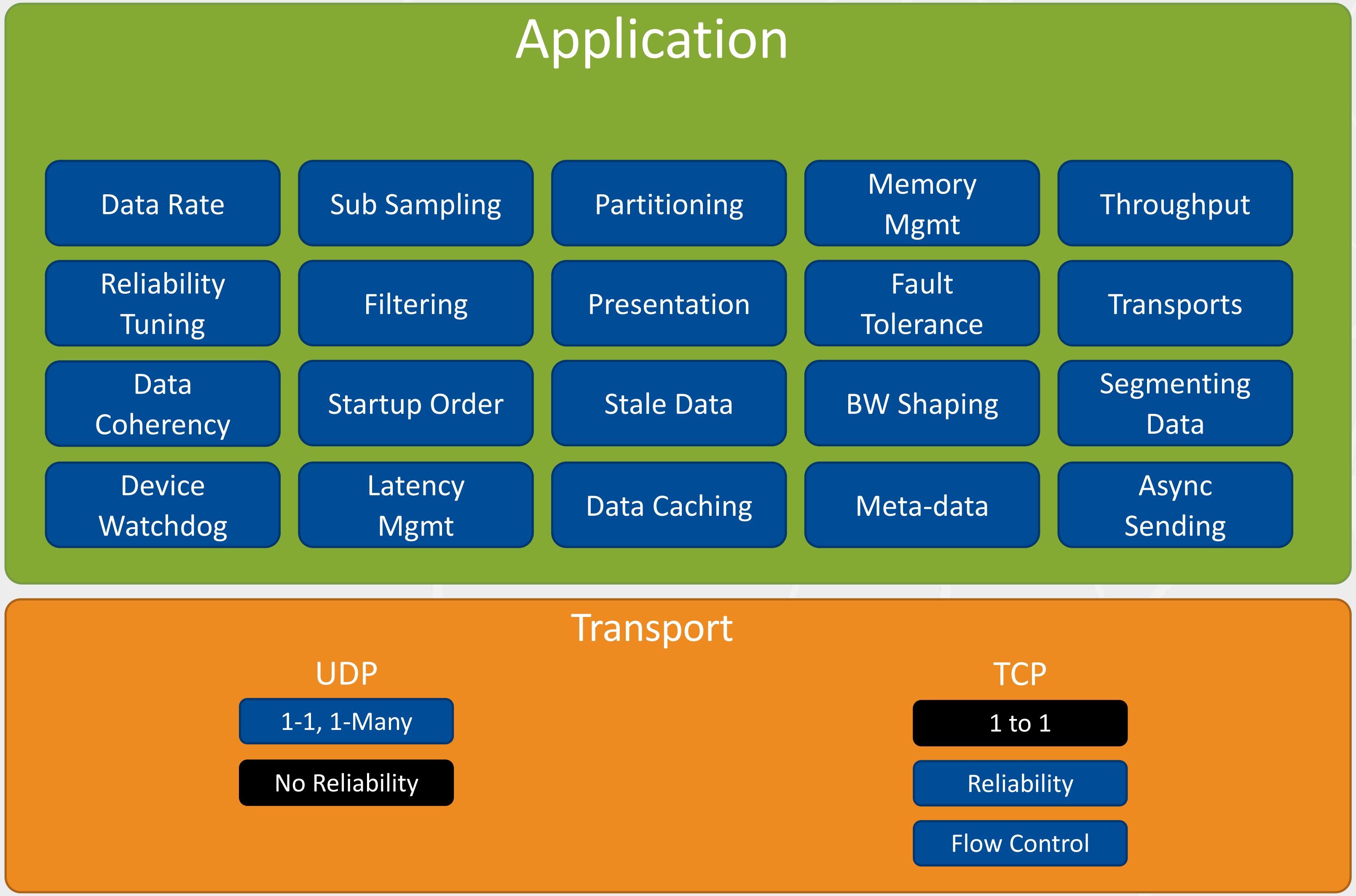
What happens to the system when your needs evolve

Layered Databus Architecture Pattern



- Common across these industrial IoT systems
- Fast, reliable, scalable
- From IIC Industrial Internet Reference Architecture (IIRA) v1.8

Common Distributed Application Challenges



Application

Data Rate

Sub Sampling

Partitioning

Memory Mgmt

Throughput

Reliability Tuning

Filtering

Presentation

Fault Tolerance

Transports

Data Coherency

Startup Order

Stale Data

BW Shaping

Segmenting Data

Device Watchdog

Latency Mgmt

Data Caching

Meta-data

Async Sending

Transport

UDP

1-1, 1-Many

No Reliability

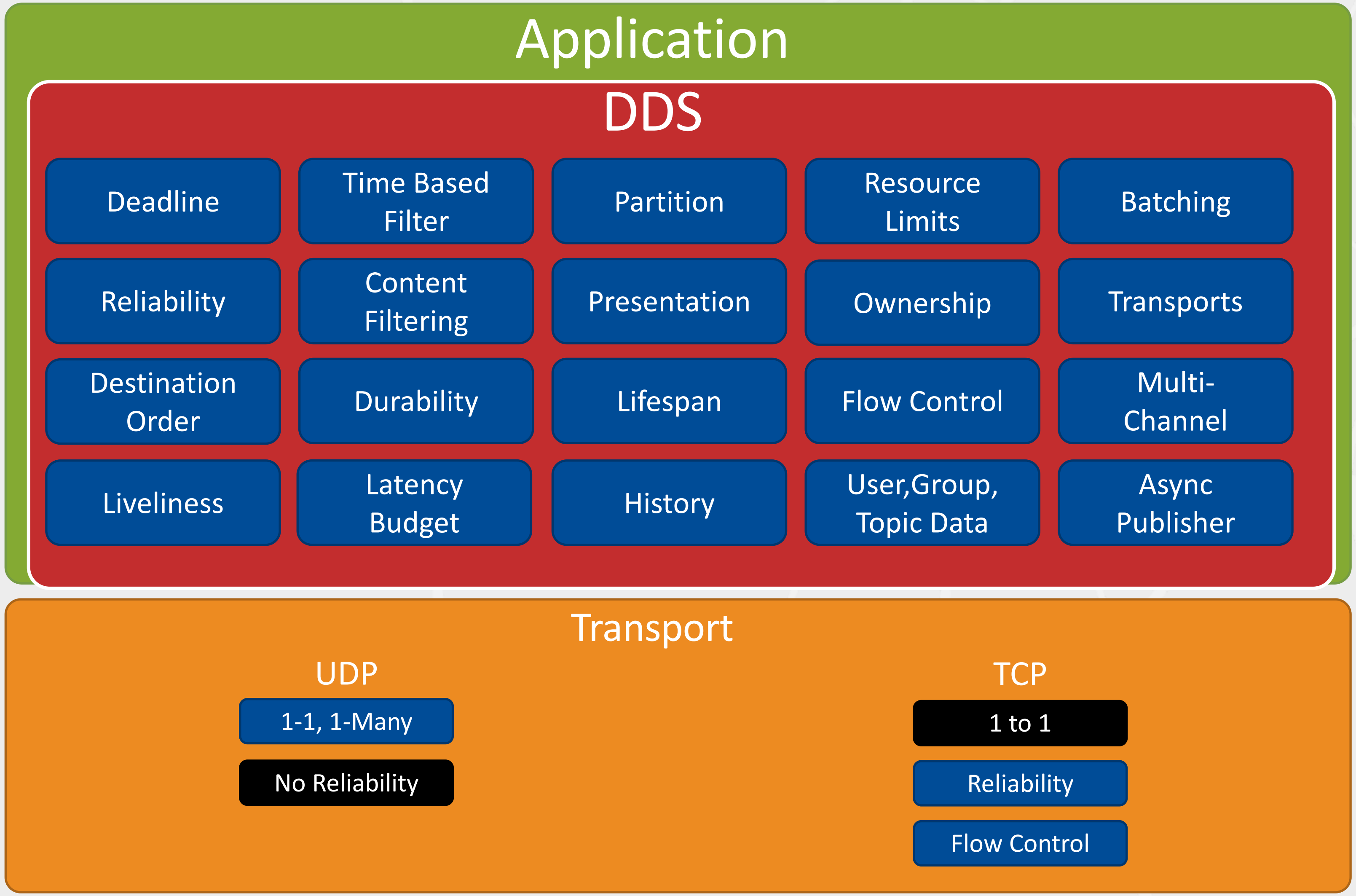
TCP

1 to 1

Reliability

Flow Control

Common Distributed Application Challenges



Application

DDS

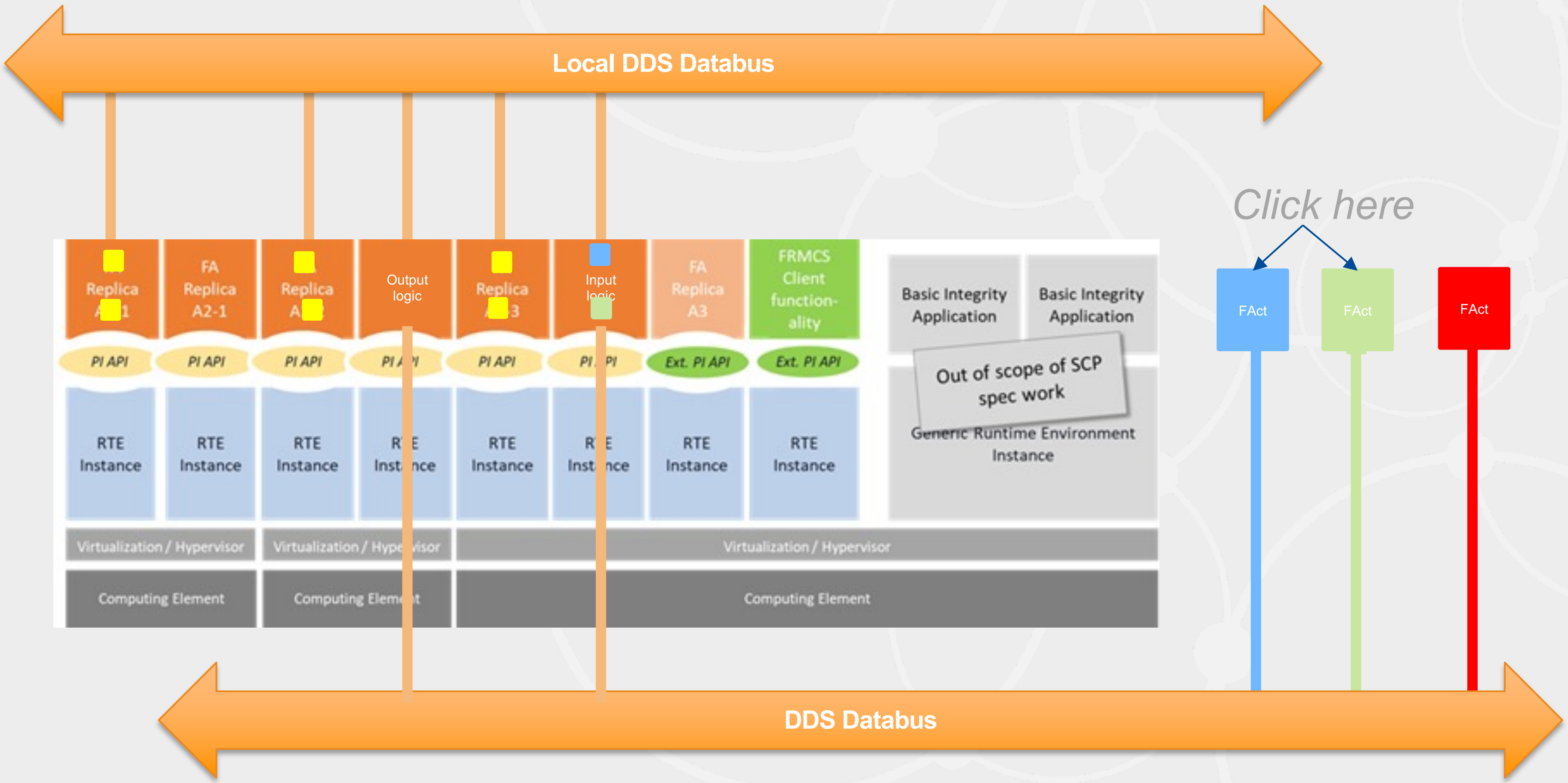
Deadline	Time Based Filter	Partition	Resource Limits	Batching
Reliability	Content Filtering	Presentation	Ownership	Transports
Destination Order	Durability	Lifespan	Flow Control	Multi-Channel
Liveliness	Latency Budget	History	User,Group, Topic Data	Async Publisher

Transport

UDP
- 1-1, 1-Many
- No Reliability

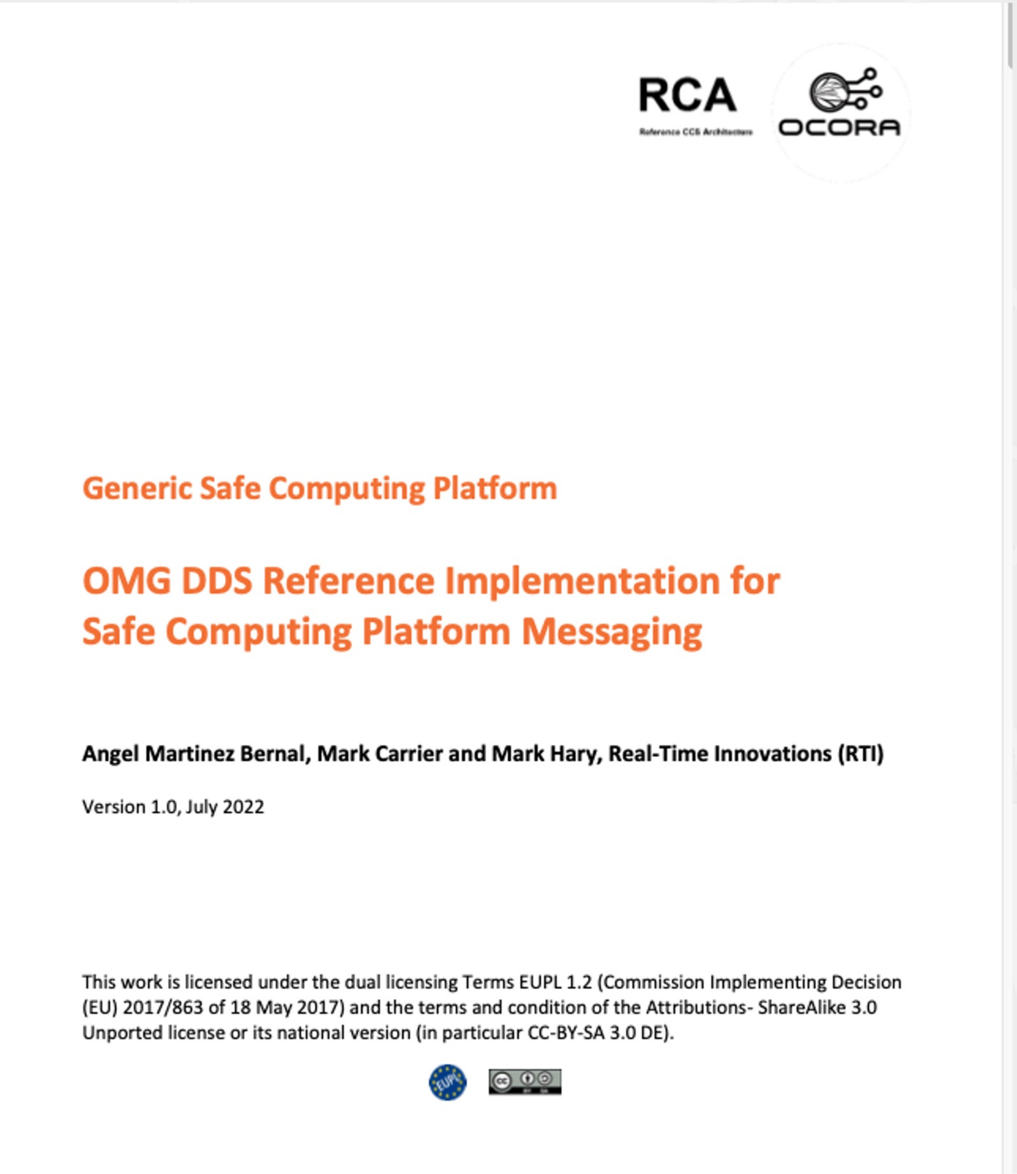
TCP
- 1 to 1
- Reliability
- Flow Control

SCP Architecture with DDS (example)



OMG DDS Reference Implementation for SCP messaging

DDS Reference Implementation



Generic Safe Computing Platform

OMG DDS Reference Implementation for Safe Computing Platform Messaging

Angel Martinez Bernal, Mark Carrier and Mark Hary, Real-Time Innovations (RTI)

Version 1.0, July 2022

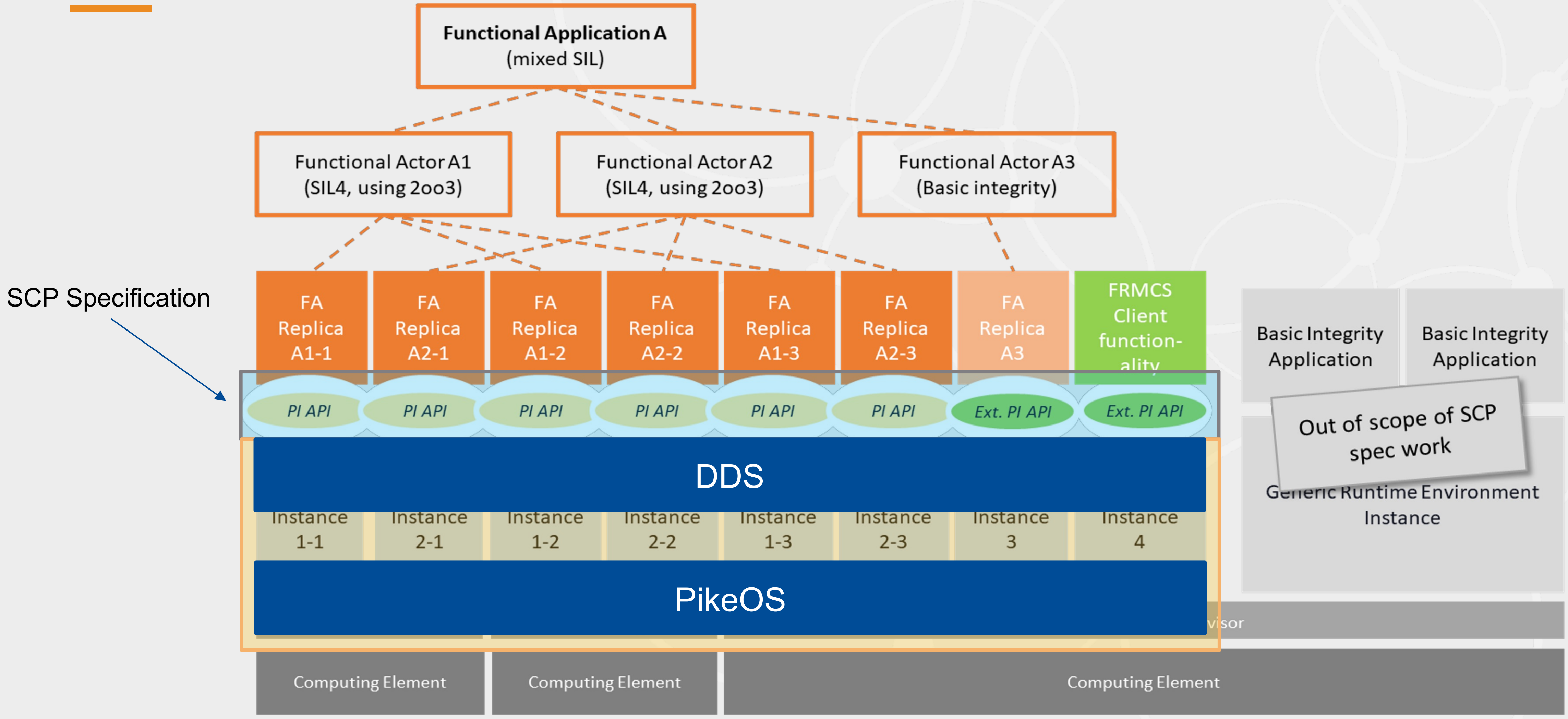
Platform Independent API (PI API)

- DDS Typed messaging API
- Implement *fl_read* and *fl_write*
  - – DataWriter<Foo>::write(const Foo&);
  - – DataReader<Foo>::read(Foo &, SampleInfo &);
- Functional Actors
  - – Publisher → DDS DataWriter
  - – Subscriber → DDS DataReader
- Specifies the QoS to use for **interoperability**

Kind	DDS Entity	Characteristics	DDS Feature	creation	deletion
Unidirectional Flow – One Publisher	SCP Publisher → DataWriter Unkeyed type	Posted messages are delivered in the same order	Automatically done	Enable DataWriters and DataReaders	- Delete DDS Entity or change PARTITION to specific values
		Missing messages are identified by the platform	SAMPLE_LOST status		
	SCP Subscribers → DataReaders	Messages are timestamped by the platform	LIFESPAN		
Unidirectional Flow – Multiple Publisher	SCP Publishers → DataWriters keyed type	Identification and authentication	SECURITY		- Delete DDS Entity or change PARTITION to specific values - Unregister/dispose specific key
		Notification when publisher “dies”	LIVELINESS		
		At most once, at least once	RELIABILITY		
	SCP Subscribers → DataReaders	Maximum delivery time	LATENCY_BUDGET and timestamps		
		Flow knows publishers and subscribers	Properties		

Kind	DDS Entity	Characteristics	DDS Feature	creation	deletion
Bidirectional Flow - Requestor	DataWriter sending requests	Posted messages are received in the exact same order	Automatically done	Enable underlying DataWriters and DataReaders	- Delete underlying DDS Entities or change PARTITION to specific values
		Deliver messages ”exactly once”	RELIABILITY		
	DataReader receiving replies	Notifications about the desired maximum message delivery time exceeded	receive_replies() / wait_for_replies() SAMPLE_LOST status		
		Messages are timestamped by the platform	LIFESPAN		
Bidirectional Flow - Replier	DataReader receiving requests	Notify requestor node when a responding node has been created	SUBSCRIPTION_MATCHED PUBLICATION_MATCHED		
		Notification when requestor / replier “dies”	LIVELINESS		
	DataWriter sending replies	Trust the identity of the requestor / replier	SECURITY		
		Desired maximum message delivery time	LATENCY_BUDGET and timestamps / DEADLINE		

Safe Computing Platform Architecture

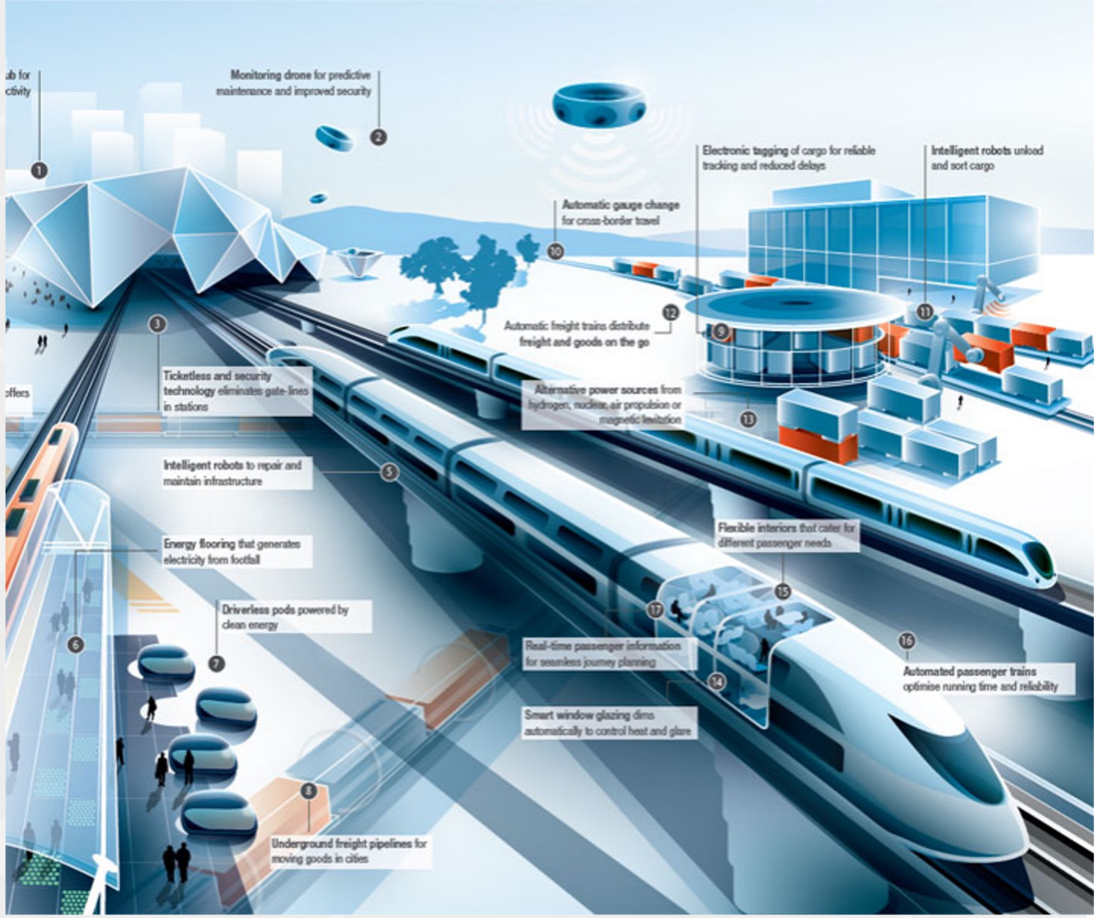


Beyond Rail: SCP Applicability to Other Industries

- The Safe Computing Platform has been designed according to railway standards, with railway requirements in mind

- A Platform Independent (PI) approach could be extended to other industries that require mixed criticality cloud computing

- Examples
  - **V2X**: Collaborative breaking scenarios, intelligent traffic management
  - **D2X**: Battery and flight path management
  - **Industrial Automation**: Co-bot control and interactions


ub for
ctivity
1
Monitoring drone for predictive maintenance and improved security
2
Electronic tagging of cargo for reliable tracking and reduced delays
Intelligent robots unload and sort cargo
Automatic gauge change for cross-border travel
10
Automatic freight trains distribute freight and goods on the go
12
9
11
3
Ticketless and security technology eliminates gate-lines in stations
offers
Alternative power sources from hydrogen, nuclear, air propulsion or magnetic levitation
13
Intelligent robots to repair and maintain infrastructure
5
Flexible interiors that cater for different passenger needs
Energy flooring that generates electricity from footfall
15
Driverless pods powered by clean energy
17
6
7
Real-time passenger information for seamless journey planning
16
14
Automated passenger trains optimise running time and reliability
Smart window glazing dims automatically to control heat and glare
8
Underground freight pipelines for moving goods in cities

Summary

- RCA / OCORA wants to standardize a safe computing platform for onboard/trackside deployments.
- This approach has applicability to other industries.
- PikeOS provides the hard real-time operating system and hypervisor as a core SCP building block.
- Connext DDS provides the real-time, publish-subscribe, safety-certified communications.

SYSGO
EMBEDDING INNOVATIONS
Booth 4

Questions?
Meet us after this talk.

rti
Booth 9

SYSGO EMBEDDING INNOVATIONS rti

Credits and further reading

- Links to reports:
  - Research Report SIL4 Cloud
    - https://digitale-schiene-deutschland.de/Downloads/Report%20-%20SIL4%20Cloud.pdf
  - RCA/OCORA. (2022). Generic Safe Computing Platform: Specification of the PI API between Application and Platform.
    - https://raw.githubusercontent.com/OCORA-Public/Publication/master/06_OCORA%20R2/OCORA-TWS03-030_SCP_Specification_of_the_PI_API_between_Application_and_Platform.pdf
  - RCA/OCORA. (2022). Generic Safe Computing Platform: OMG DDS Reference Implementation for Safe Computing Platform Messaging
    - https://github.com/OCORA-Public/Publication/blob/master/91_SCP_OMG_DDS_Reference_Implementation/SCP_OMG_DDS_Reference_Implementation.pdf
  - Figures and details derived from above reports

Angel Martinez
angel@rti.com

Mario Brotz
mario.brotz@sysgo.com

Q&A

rti.com
sysgo.com

EMBEDDING INNOVATIONS
Booth 4

Meet us after this talk.

Booth 9

October 11, 2022

Thank you!

Angel Martinez
angel@rti.com

Mario Brotz
mario.brotz@sysgo.com

RTI - Booth 9; rti.com
SYSGO - Booth 4; sysgo.com

October 11, 2022