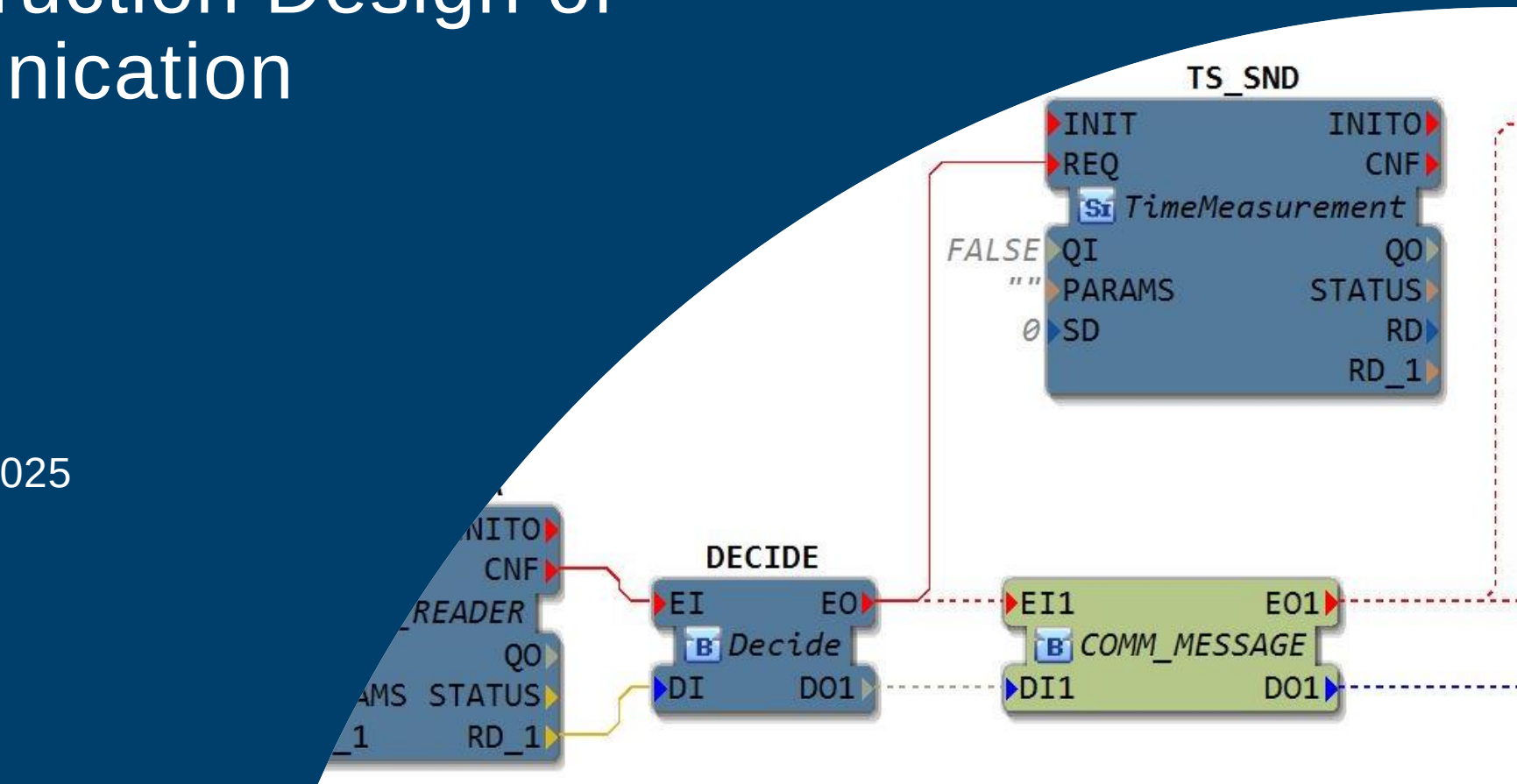
Carl von Ossietzky
Universität
Oldenburg

Correct-by-Construction Design of Industrial Communication

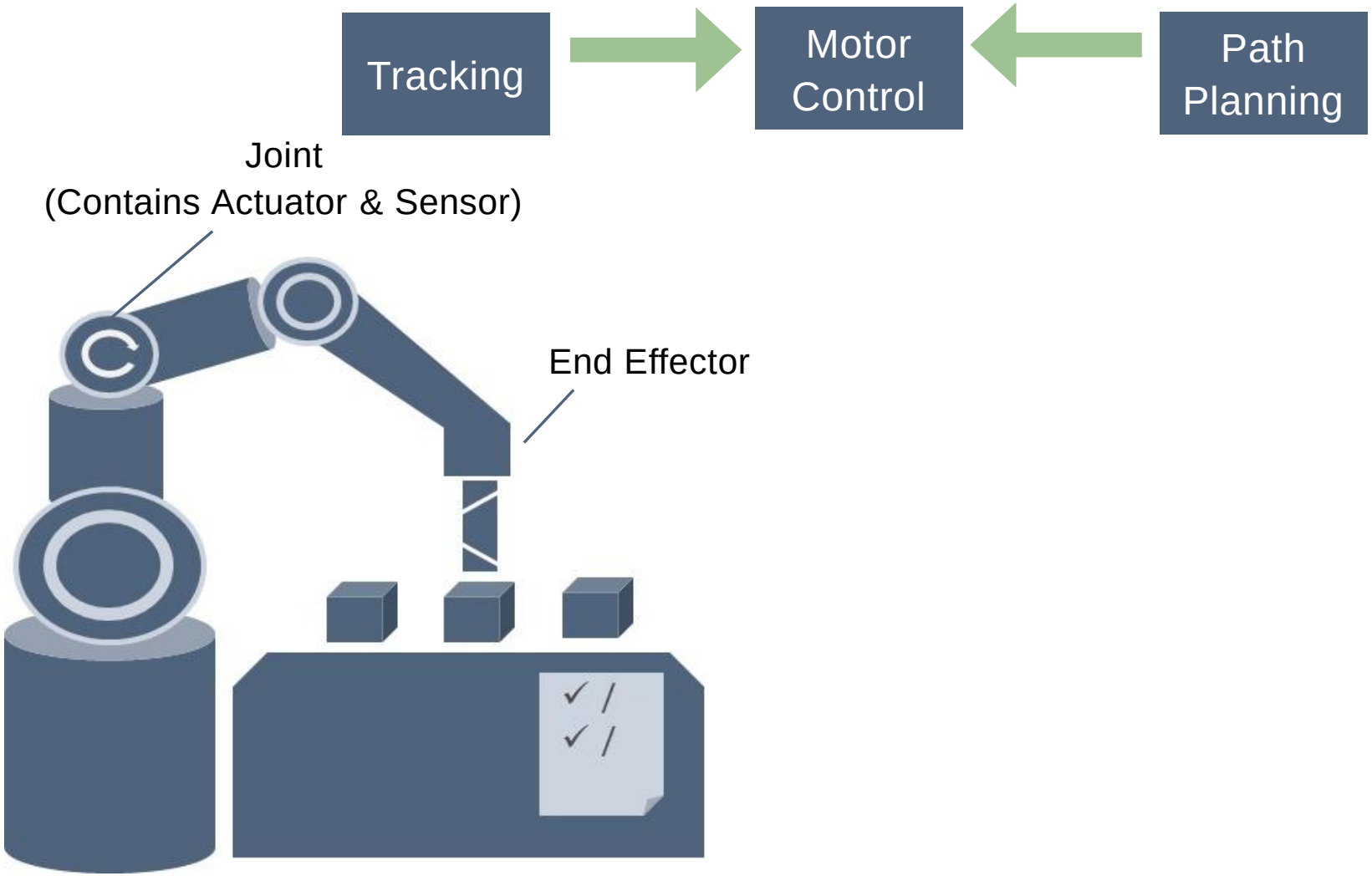
SECPPS Workshop

SE Conference

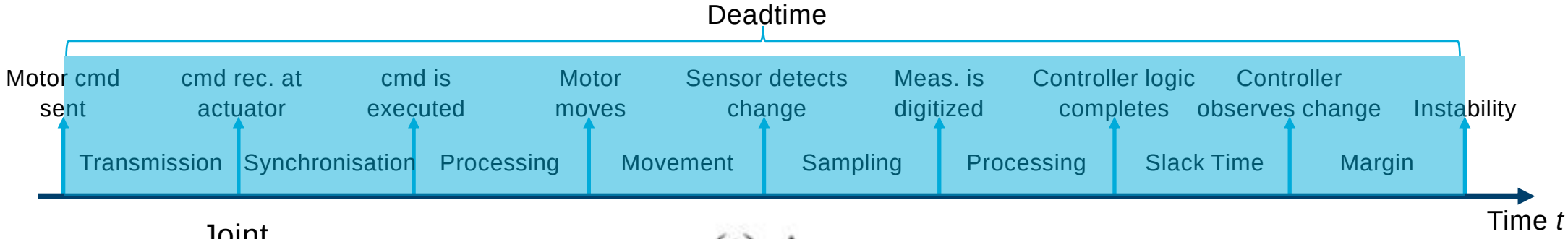
Dr.-Ing. Friederike Bruns, 25.02.2025

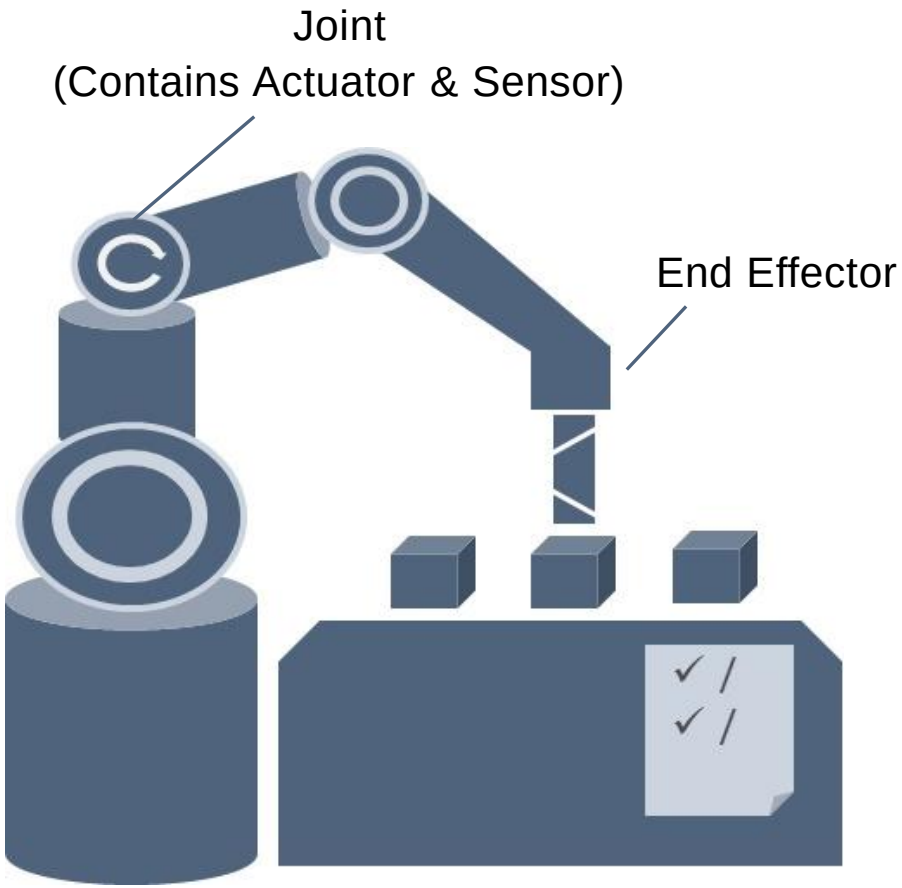


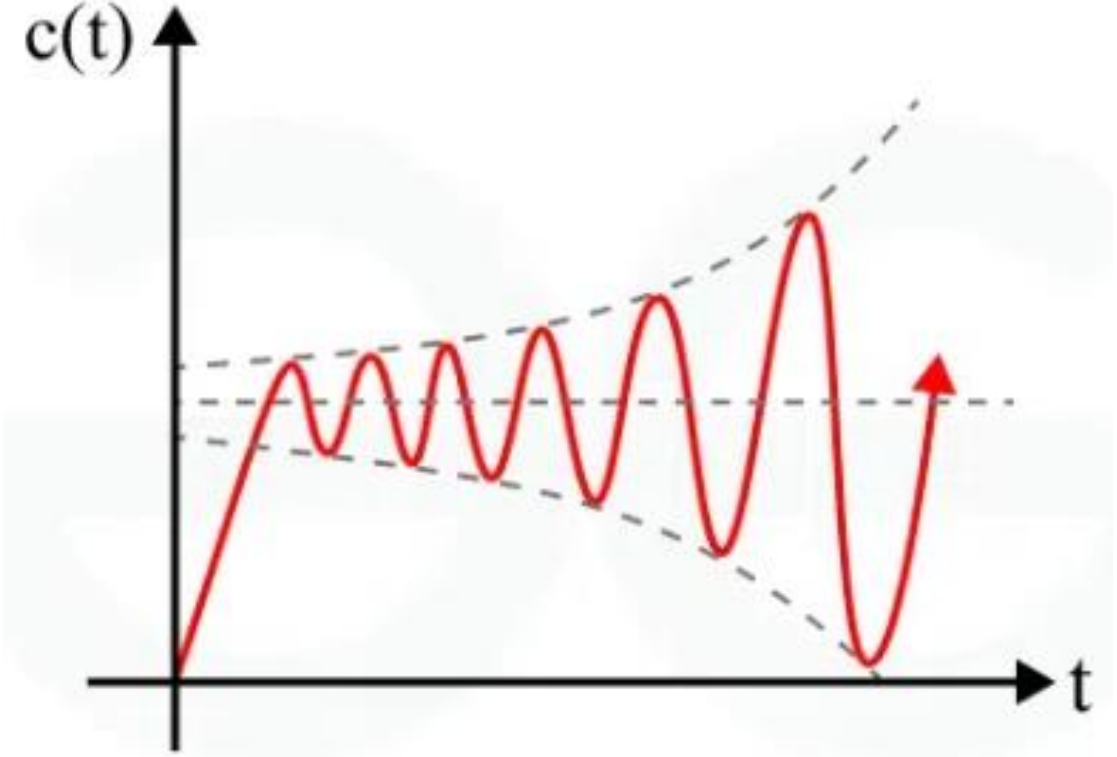
Industrial Distributed Control Systems (IDCS)



Why Time Delay Matters in IDCS

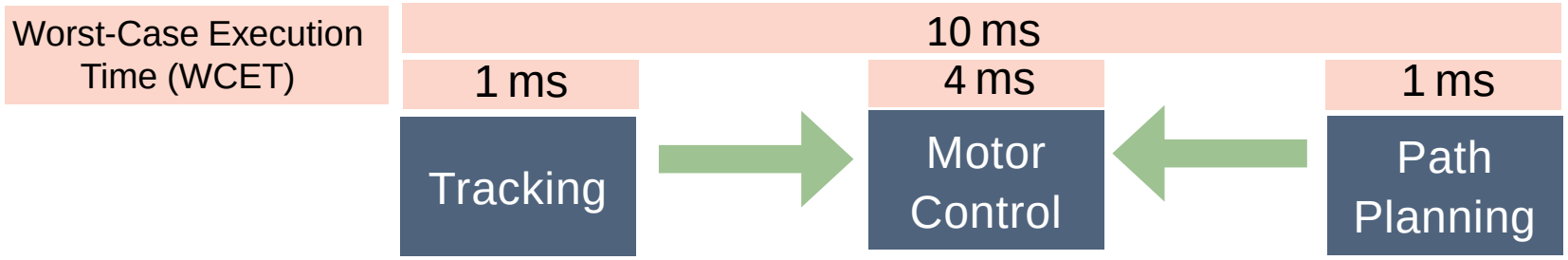


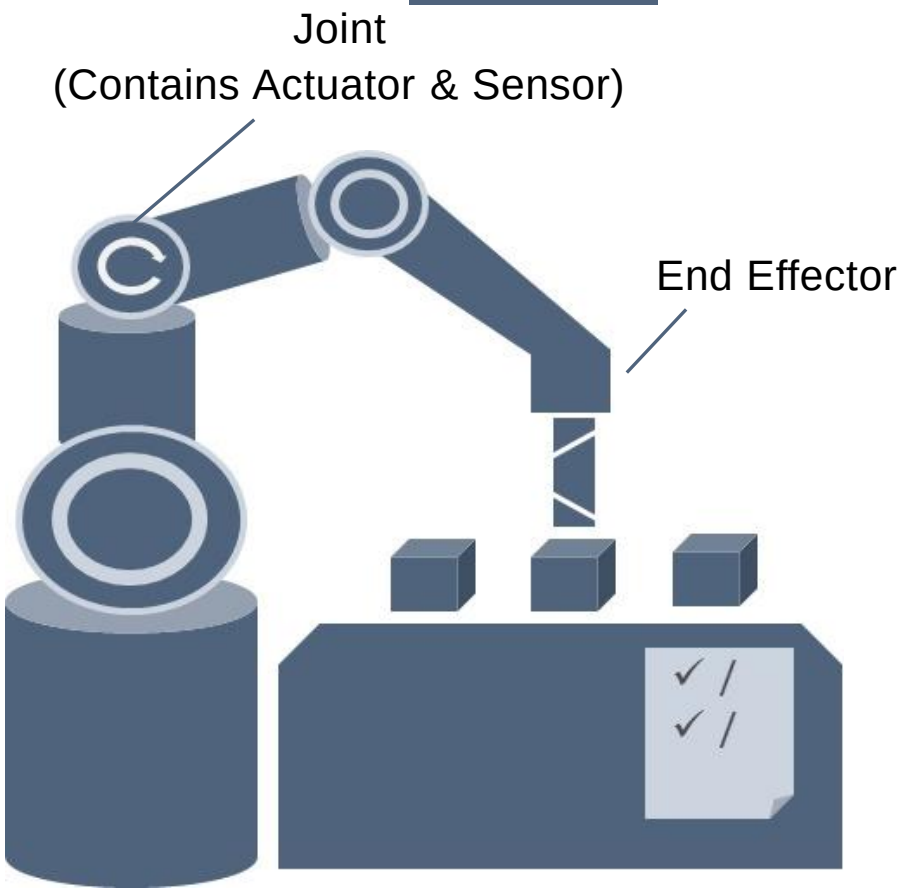




- Controller has to use old information
- Controller has to predict the future
- ➢ Effectively lowers the sampling time

Time in IDCS and Network Communication



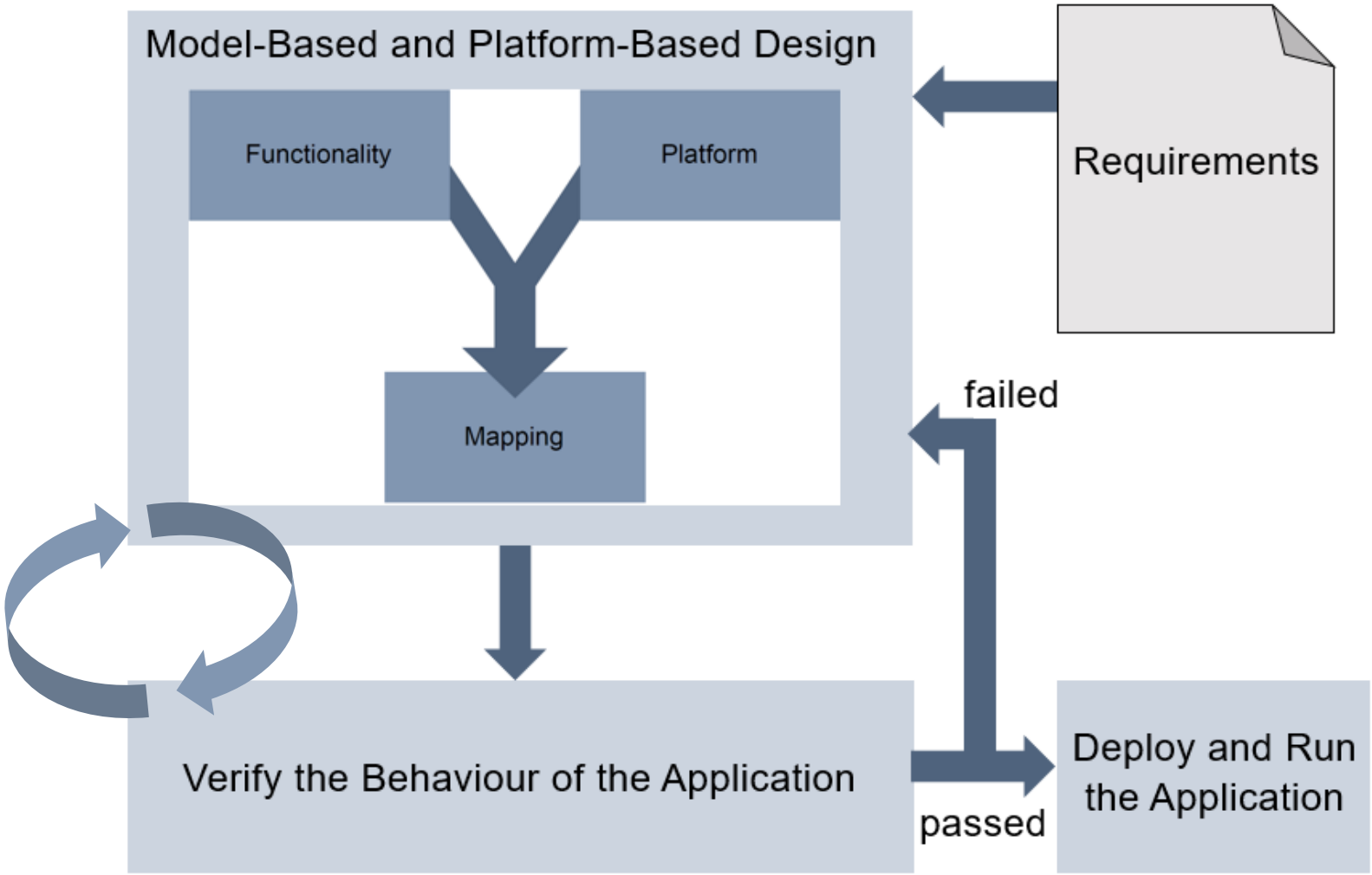


1. Publish data at sending device
2. Transmit data over wire
3. Accept data at receiving device

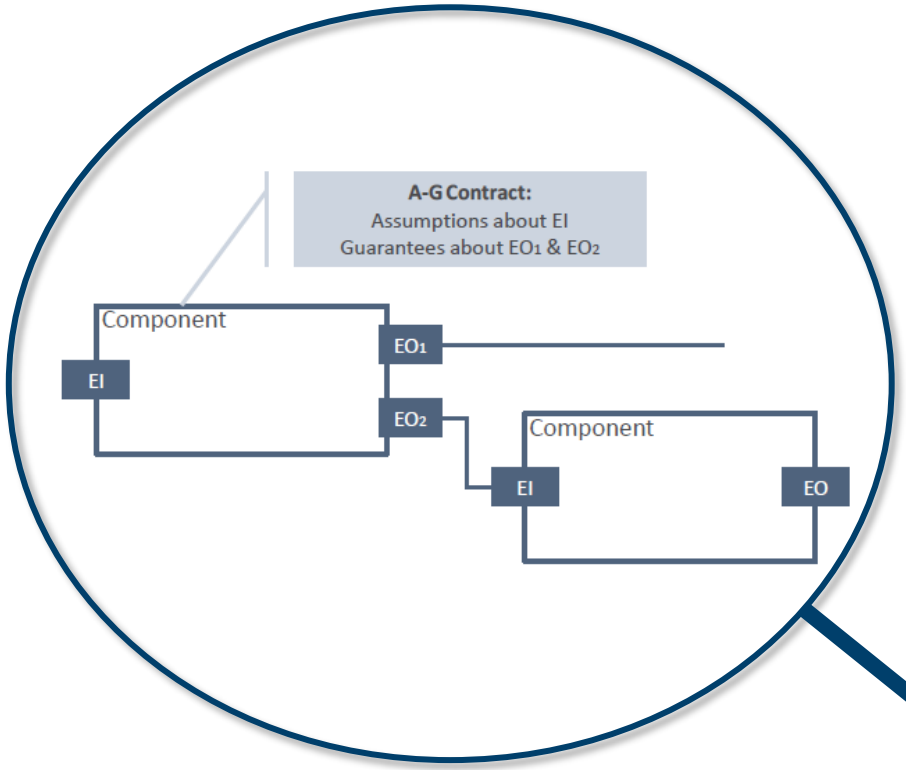
- Time Division Multiple Access (TDMA)
  - Deterministic and synchronised network
  - Separate time-critical from best-effort traffic
- Sub-millisecond latency, minimal jitter (<1%), …
- Specify network with respect to the control tasks

F. Bruns, J. Walter and W. Nebel, „A Detailed Analysis of Timing Effects in an IEC 61499 Ethernet/TSN Communication Scenario", In *27th IEEE IES International Conference on Emerging Technologies and Factory Automation (ETFA),* Stuttgart, Germany, 2022, IEEE, doi: 10.1109/ETFA52439.2022.9921436.

General Modelling Procedure for Industrial Control Systems

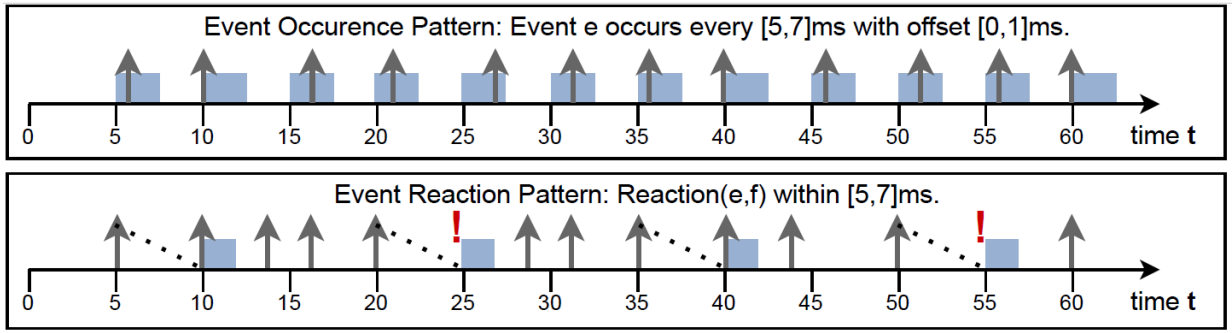


Contract-Based Design



- Continuous refinement to avoid costly design reiterations
- Hierarchical decomposition
- Virtual Integration Test: $C \geq C_1 \otimes \ldots \otimes C_n$
- Outcome
  - Failed: Adjust the model(s) or contract(s)
  - Passed: Further refinement or deployment

MULTIC Timing Specification Language (MTSL)



Formalisation of IEC 61499 Semantics

Formal verification requires formalisation of IEC 61499 semantics

An application A is characterised by the tuple (FBs, E, D, M, ExB).
Within this characterisation:

– FBs refer to a set of periodic and modular *function blocks*

– E specifies a set of *events* that trigger the execution of FBs

– D defines a set of *data connectors*

– M defines a *mapping of FBs* to execution resources

– ExB refers to the behaviour of the application based on the *execution and data processing* with FBs

Semantic Loopholes
- IEC 61499 allows different interpretations of an application
- Varied behaviour depending on the runtime and limited support for real-time (Smodic'06, Prenzel'22)

Assumption
Consider a static and deterministic FB network
➢ Introduce Rendezvous FBs if needed to merge two event streams into one.

Formalisation of IEC 61499 Semantics: Timing

Formal Definition of FBs (Dubinin'08)

Restrict FBs to provide deterministic behaviour:

- Guarantee a bounded execution time
- Mitigate the risk of unbounded execution resulting from infinite loops

The timing behaviour of a periodic FB is characterised by the tuple (ρ, o, ϵ, δ). Within this characterisation:

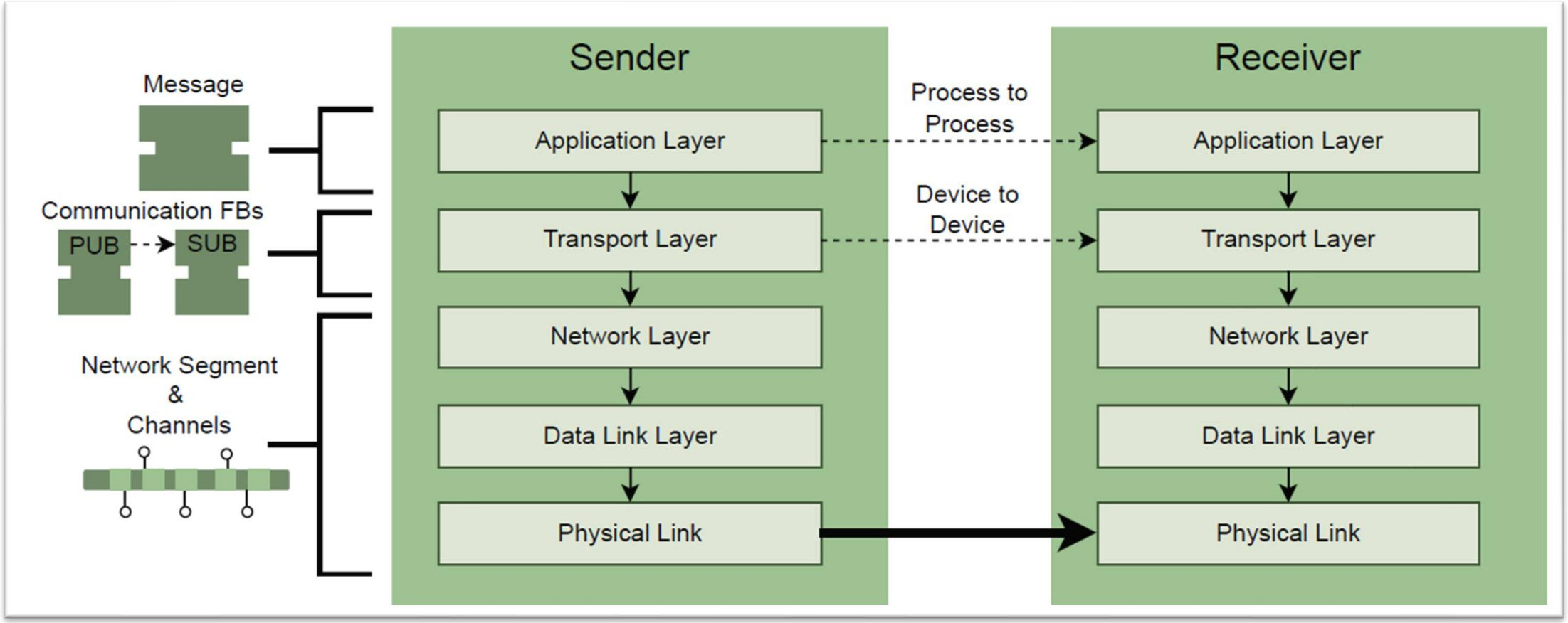
– ρ is defined as the *period* of an FB

– o characterises the *offset* relative to the starting point of ρ

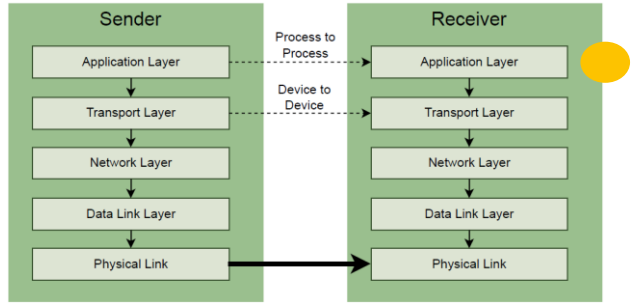
– ϵ refers to the *upper bound of the execution time* for the FB

– δ specifies the *relative deadline* of an FB

Communication Layers



IEC 61499 Modelling Extension: The Message

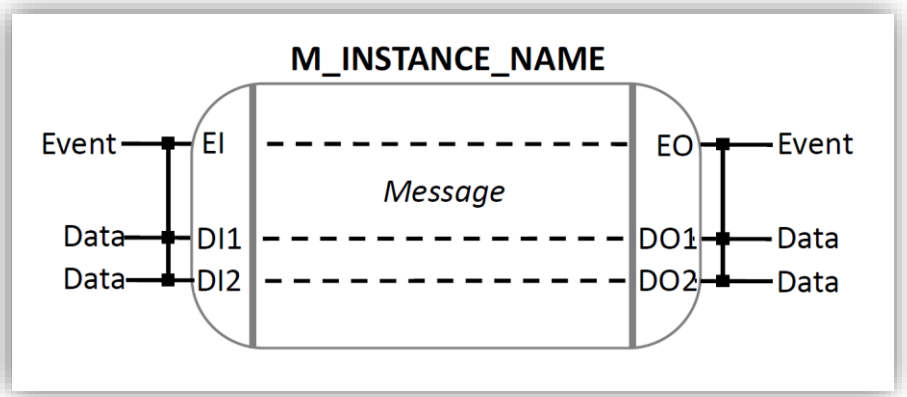


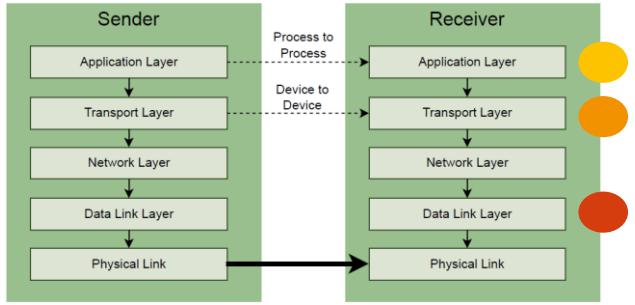
Its interface is determined by the tuple *(EI, EO, DI, DO, IW, OW)* :

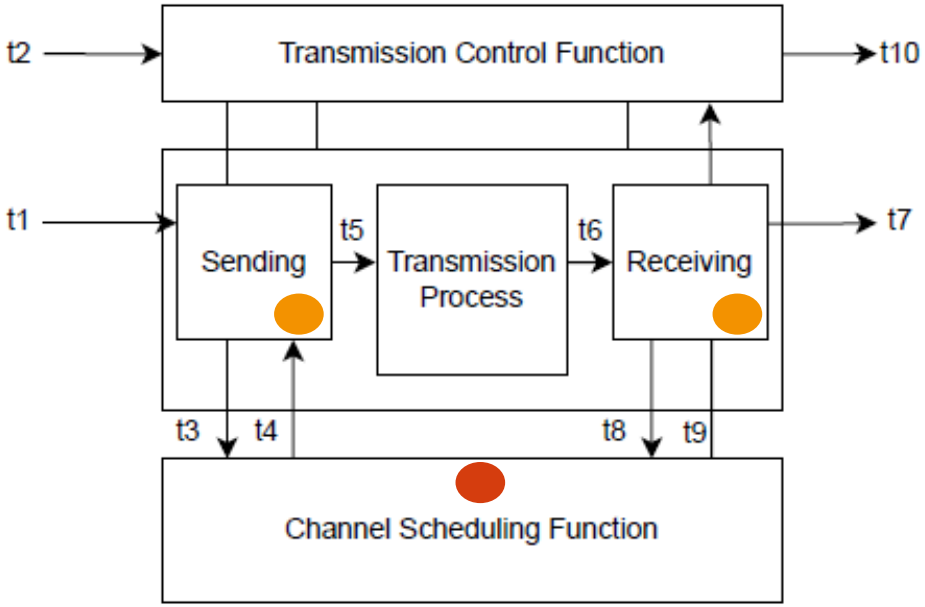
- *with exactly one scalar event at the input and output (EI and EO). These refer to the incoming transmission request event and transmission confirm event.*
- *A* message *has a set of data inputs (DI = di1, di2, ..., dij) and an according number of data outputs (DO = do1, do2, ..., doj).*
- *The event ensures that the transmission is synchronised, so that the event and data transmission only takes place simultaneously.*
- *As a mathematical notation, this is described as WITH-(event data) associations.*
- *For a set of inputs this is described as $IW \subseteq EI \times DI$, and for outputs the notation is $OW \subseteq EO \times DO$.*

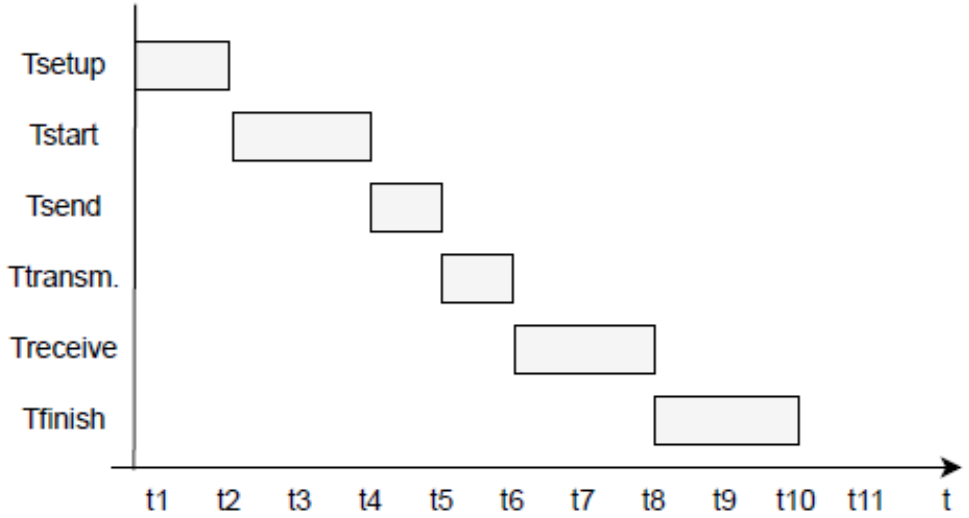
Remark *The scalar event input EI triggers the transmission of the data input set DI.*

IEC 61499 Modelling Extension: The Message

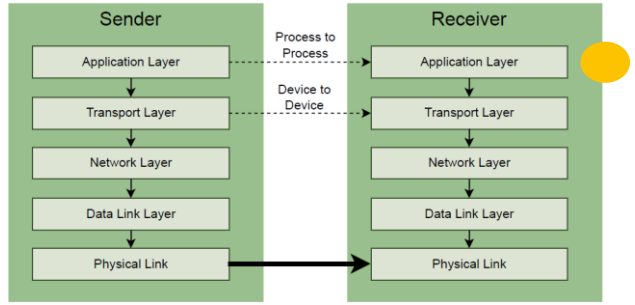


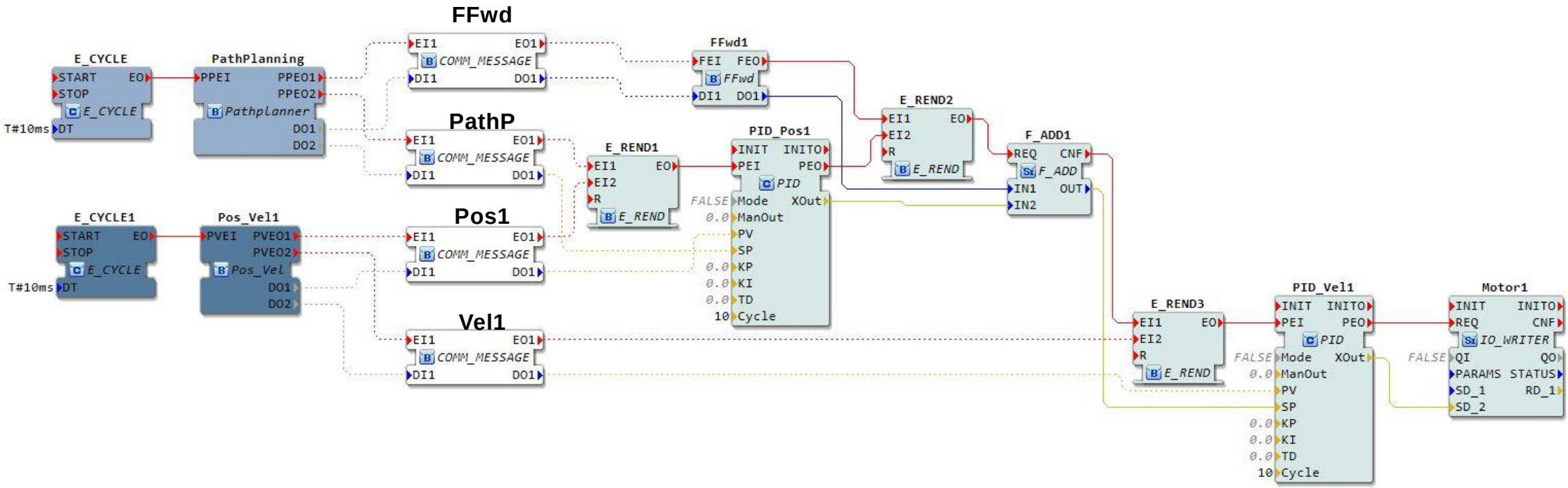






IEC 61499 Modelling Extension: The Message

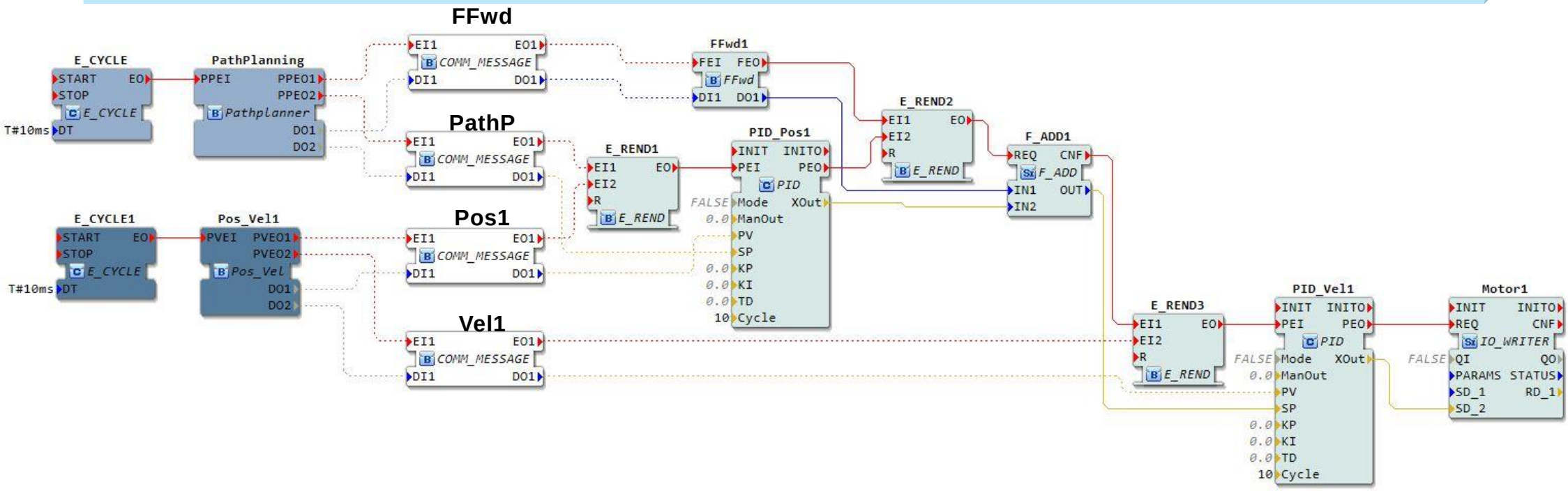




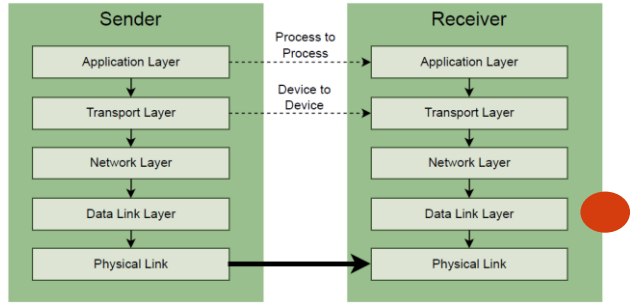
IEC 61499 Modelling Extension: The Message

Characteristics

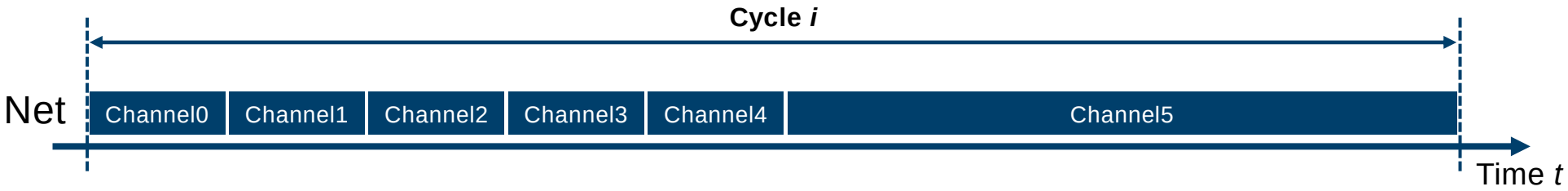
- **Message** FB creates a message (packet with event and data) for transmission when triggered
- Synchronisation point for event and data stream (intentionally just one event I/O)
- **Message** FBs can be equipped with contracts
- Allows explicit mapping to communication resources



IEC 61499 Modelling Extension: The Channel



- Physical **Channel** within which a **Message** can be transmitted
- Communication pattern (TDMA-based) dictates technical parameters:
  - ➢Overall cycle time, number of **Channels**, each **Channel's** duration and order
  - ➢Stored as part of the network segment specification
- Buffer-Channel:
  1. Synchronisation of network & execution cycle
  2. Safety margin for concurrent traffic outside of the application



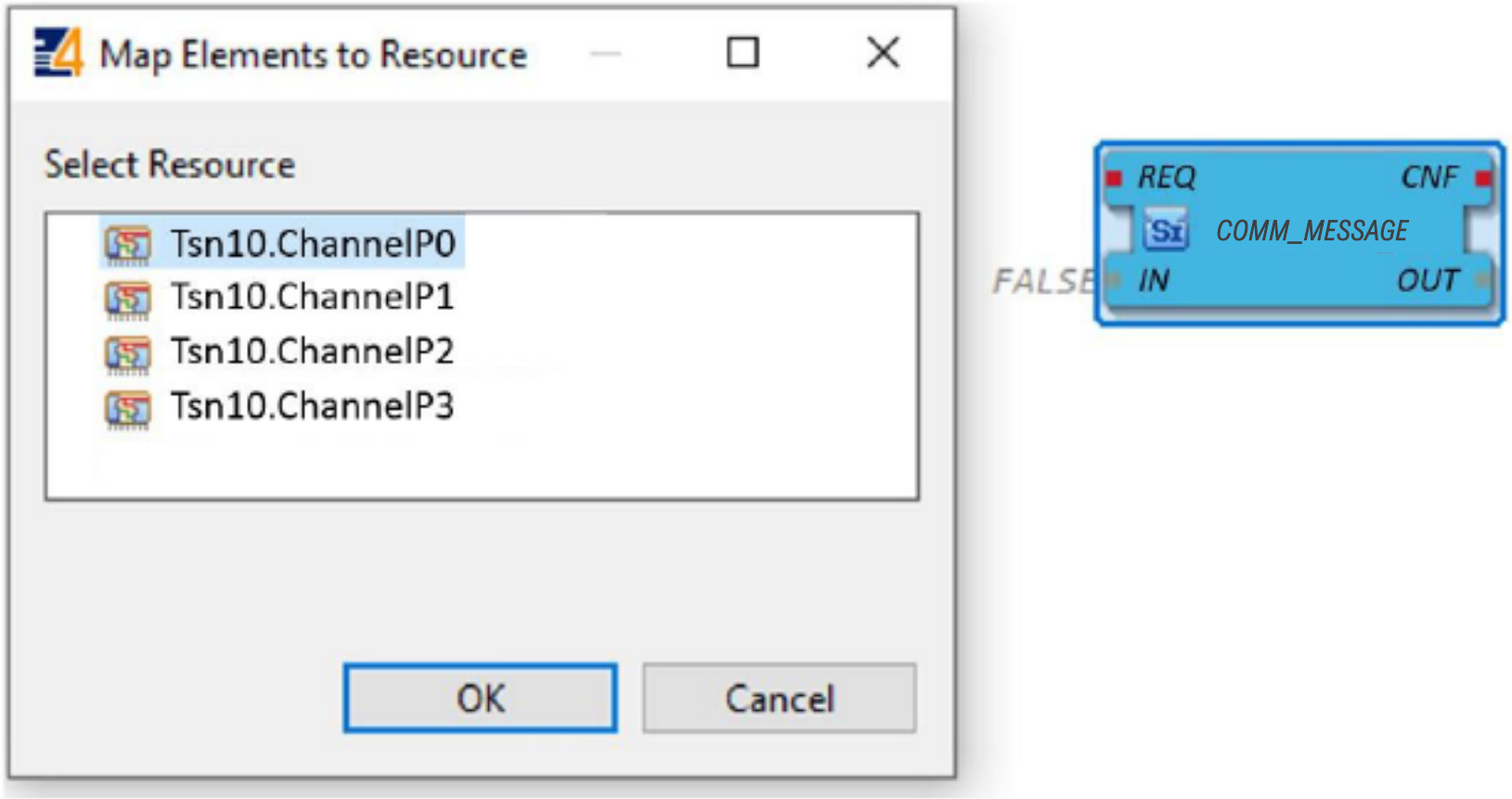
IEC 61499 Modelling Extension: The Channel

Communication Details

Cycle Time: TIME# 10 ms

name	value	type	comment
Channel0	TIME#1ms	TIME	
Channel1	TIME#1ms	TIME	
Channel2	TIME#1ms	TIME	
Channel3	TIME#1ms	TIME	
Channel4	TIME#1ms	TIME	
Channel5	TIME#5ms	TIME	

IEC 61499 Modelling Extension: Mapping



F. Bruns, B. Wiesmayr and A. Zoitl, „Supporting Model-Based Network Specification for Time-Critical Distributed Control Systems in IEC 61499", In *19th IEEE International Conference on Automation Science and Engineering (CASE),* Auckland, New Zealand, 2023, IEEE, doi: 10.1109/CASE56687.2023.10260604

Mapping Process

– Mapping specifies order and timing of **Messages** (time-triggered sending)

– Direct and manual schedule specification

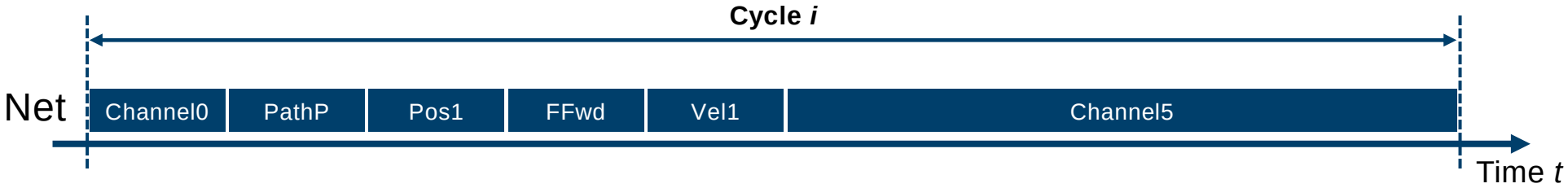
– Could support automated scheduling strategies

Focus:

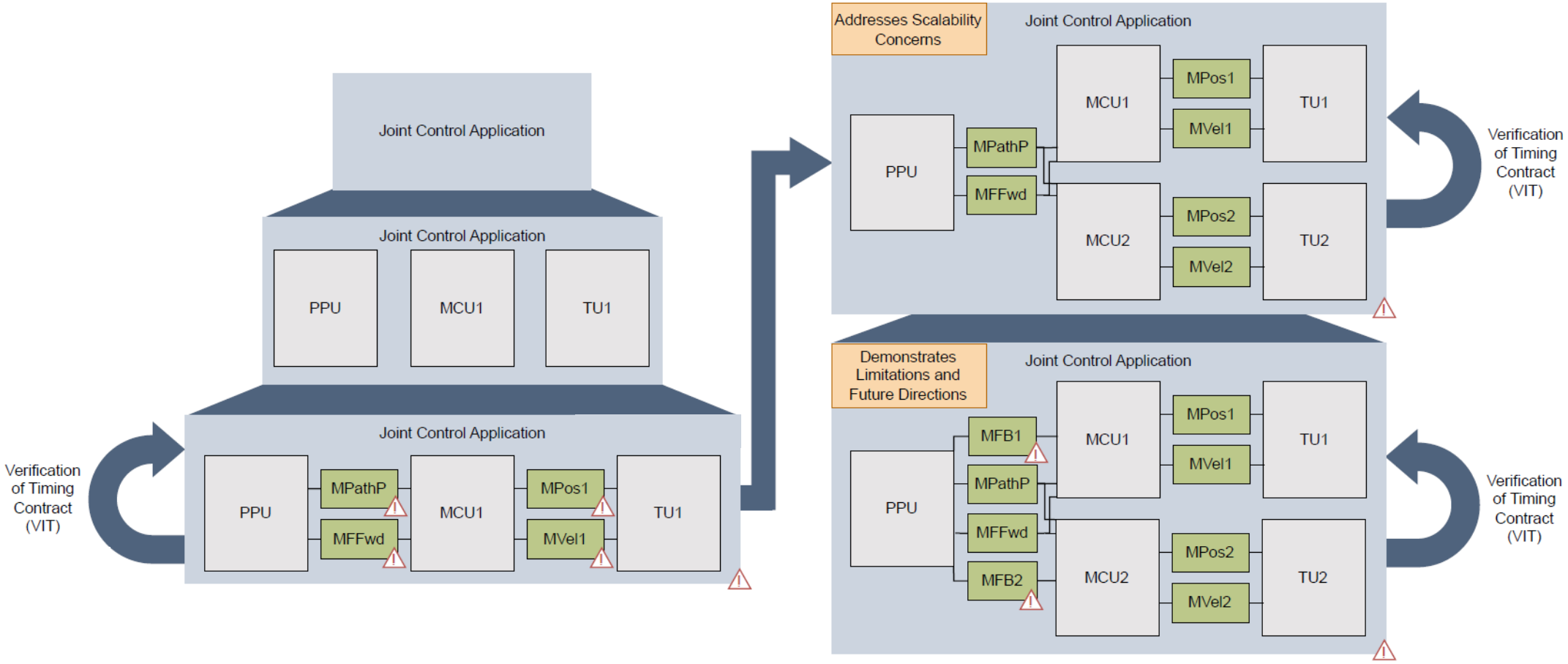
– Find a feasible schedule that does not violate timing requirements!

– Consider and analyse entire set of FBs to determine required order

– Resulting set of ordered **Messages** inherit exact timing information from the mapping



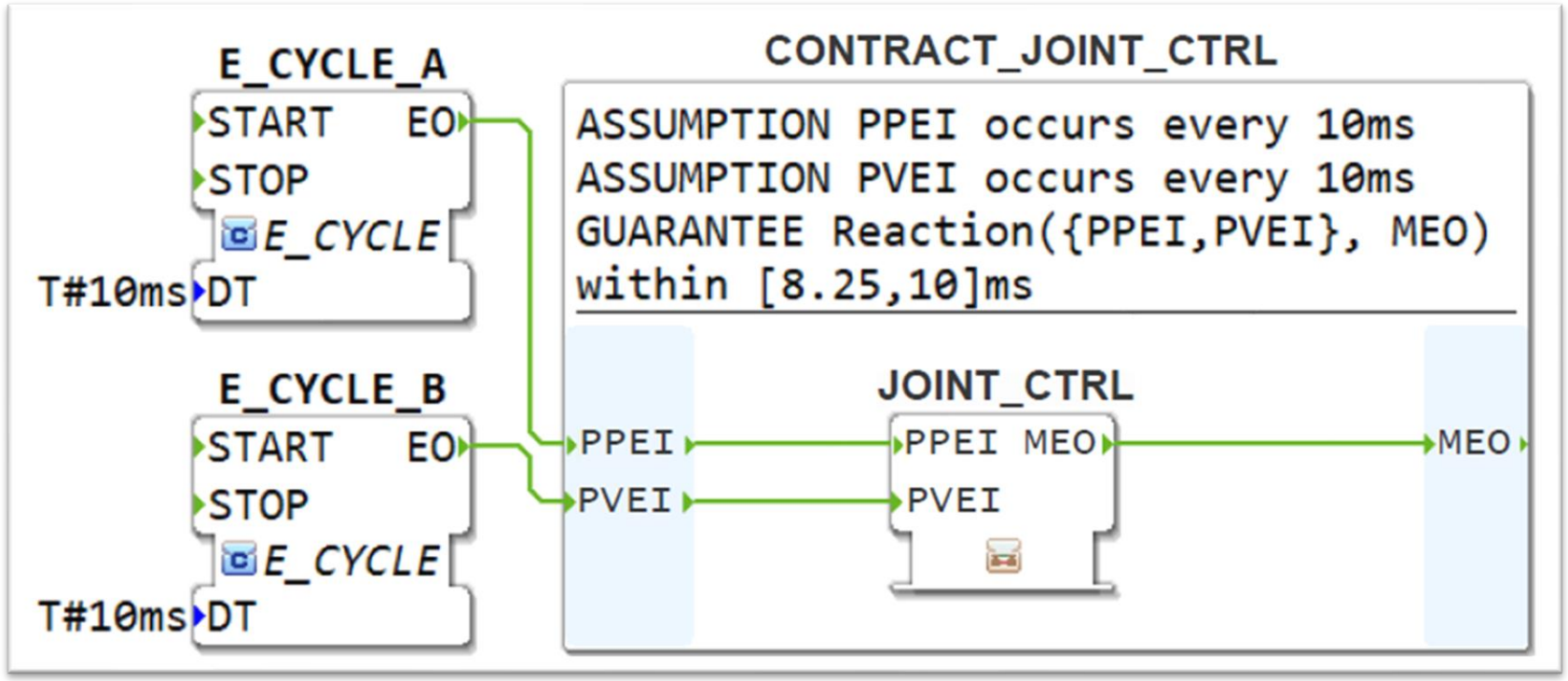
Use Case Example



Joint Control Application with Timing Specification

– A-G contracts can be specified for a single FB or group of FBs (Subapp)

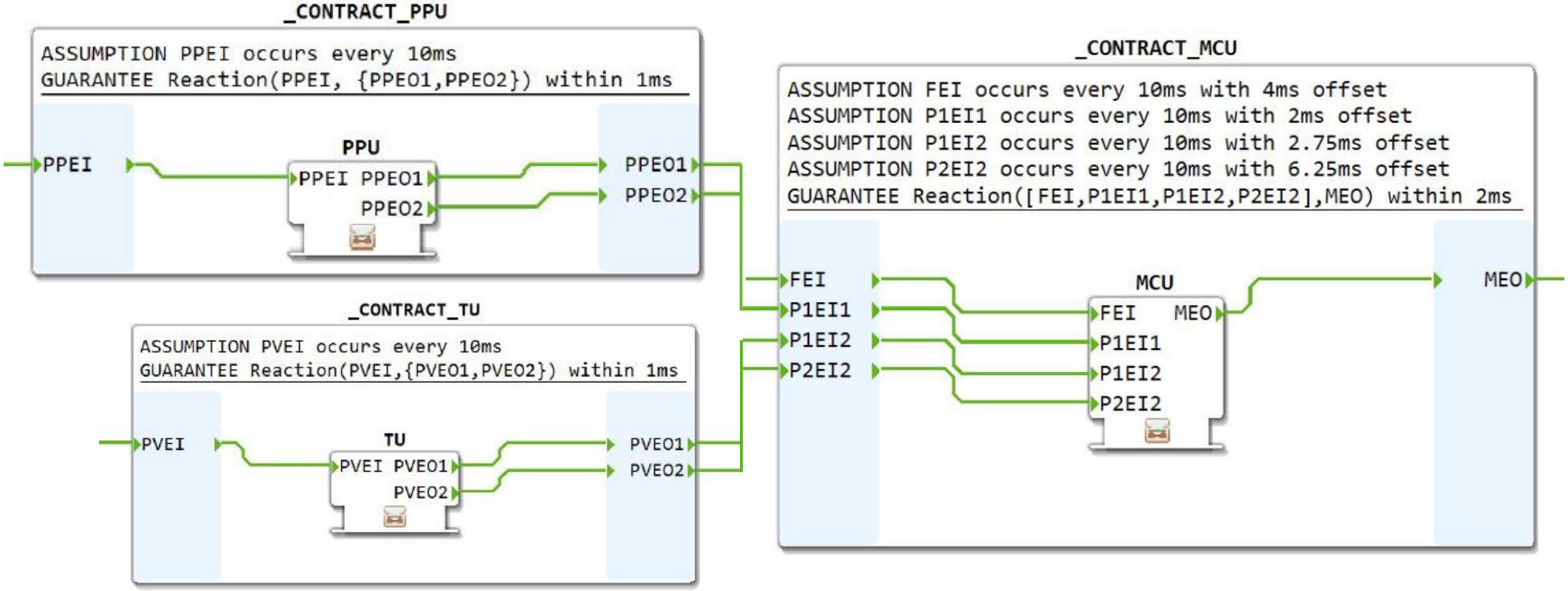
– Specification based on MTSL



F. Bruns, S. Mehlhop, B. Wiesmayr and A. Zoitl, „Enabling Automated Timing Verification: A Unified Approach for Industrial Distributed Control Systems", In 25*th IEEE International Conference on Industrial Technology (ICIT),* Bristol, UK, 2024, IEEE

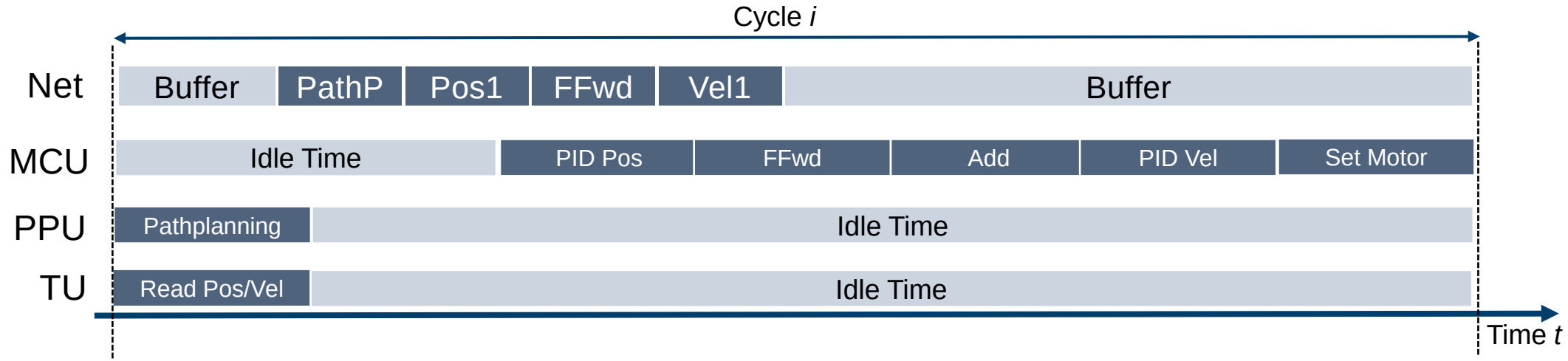
Joint Control Application – Refinement Step

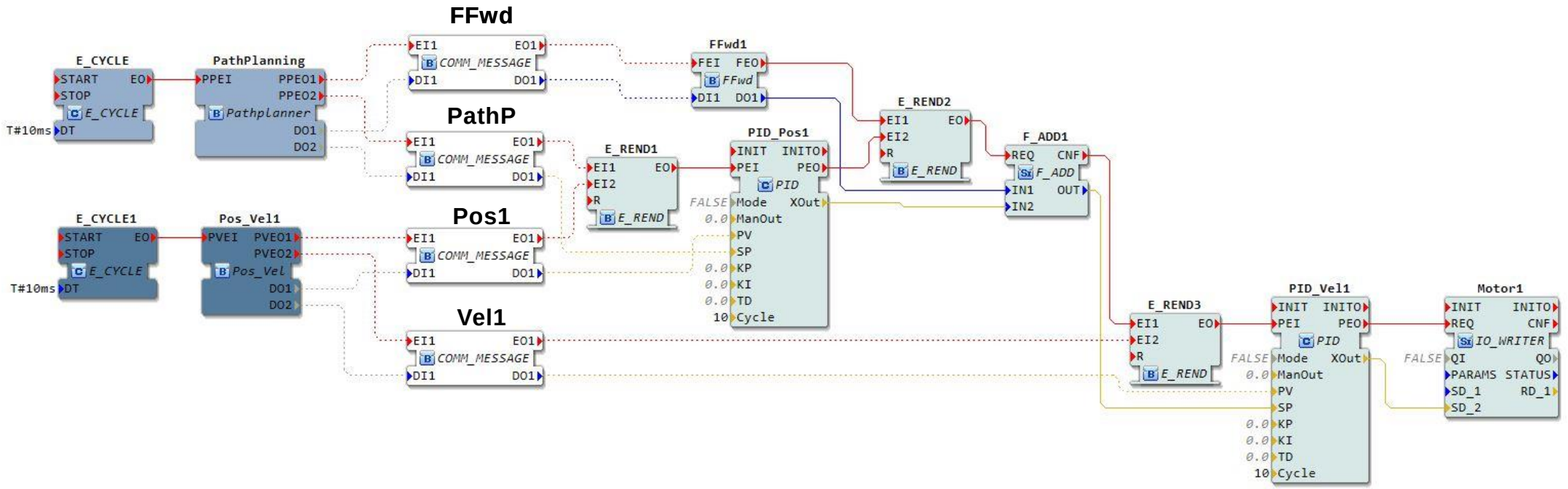
– Does the composition of the sub-contracts still fulfil the top-level contract?



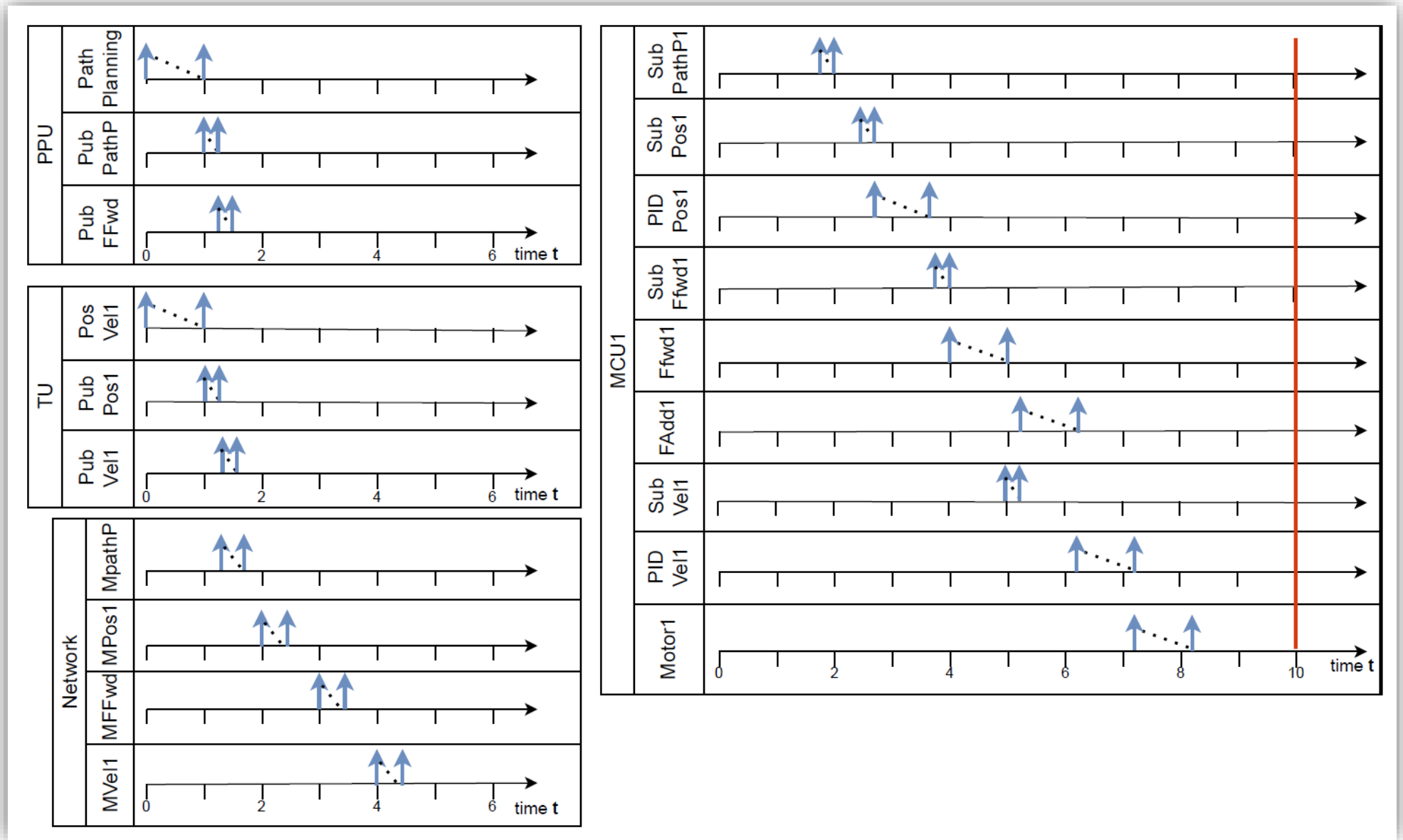
{E_1,E_2} refers to simultaneously occurring events
[E_1,E_2] refers to events that occur in unspecified order

Joint Control Application

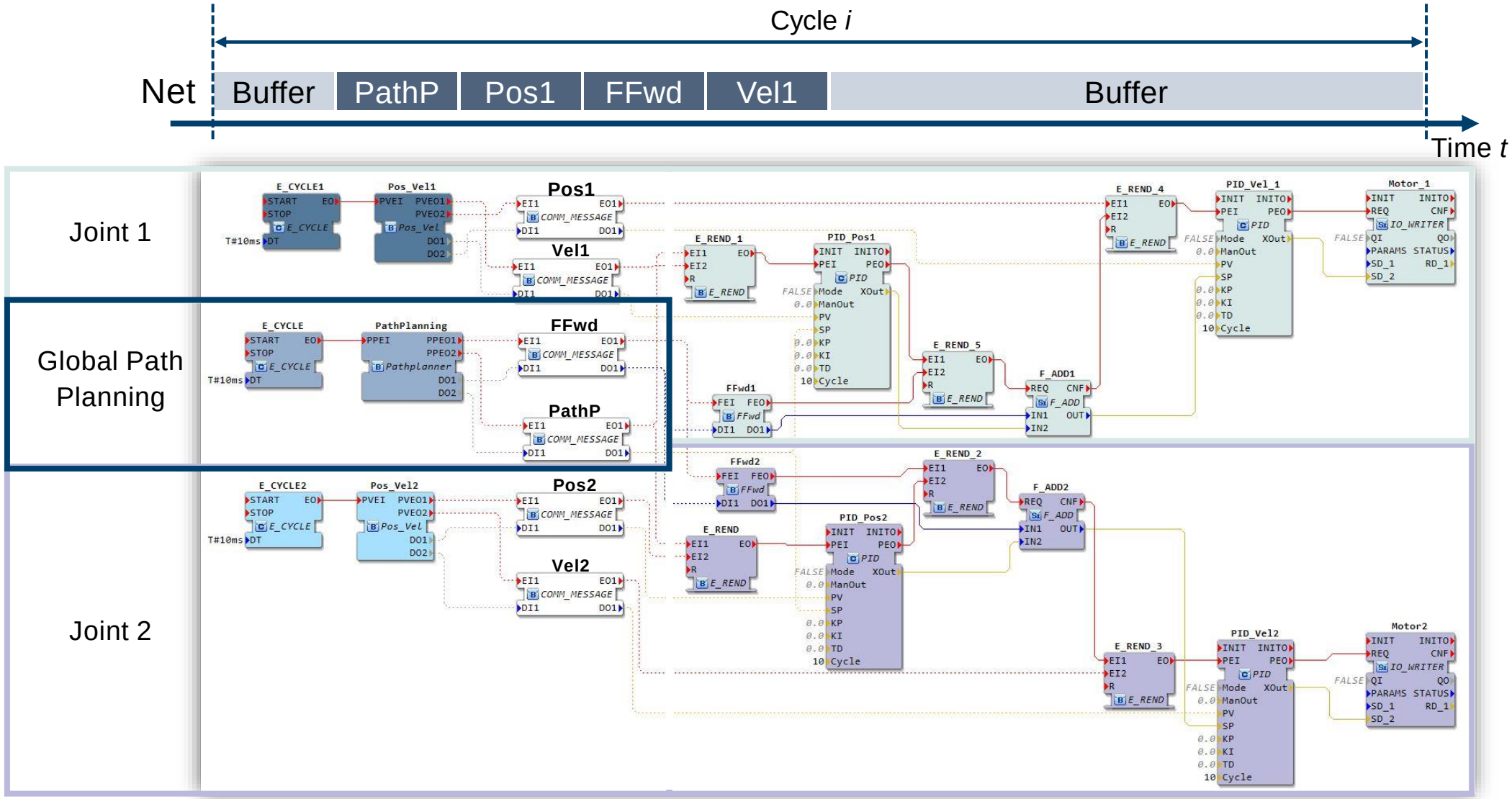




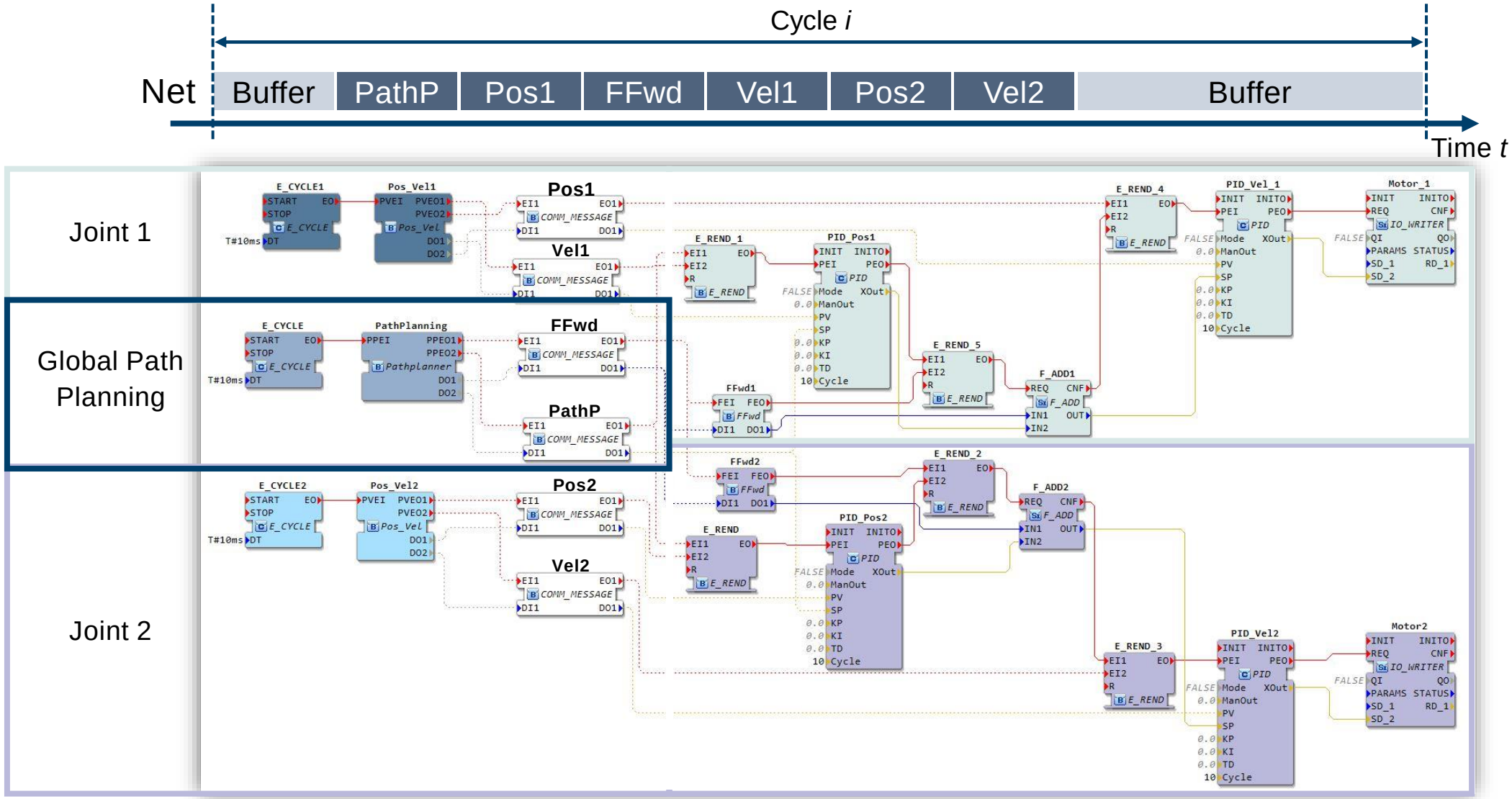
A Possible Time Trace



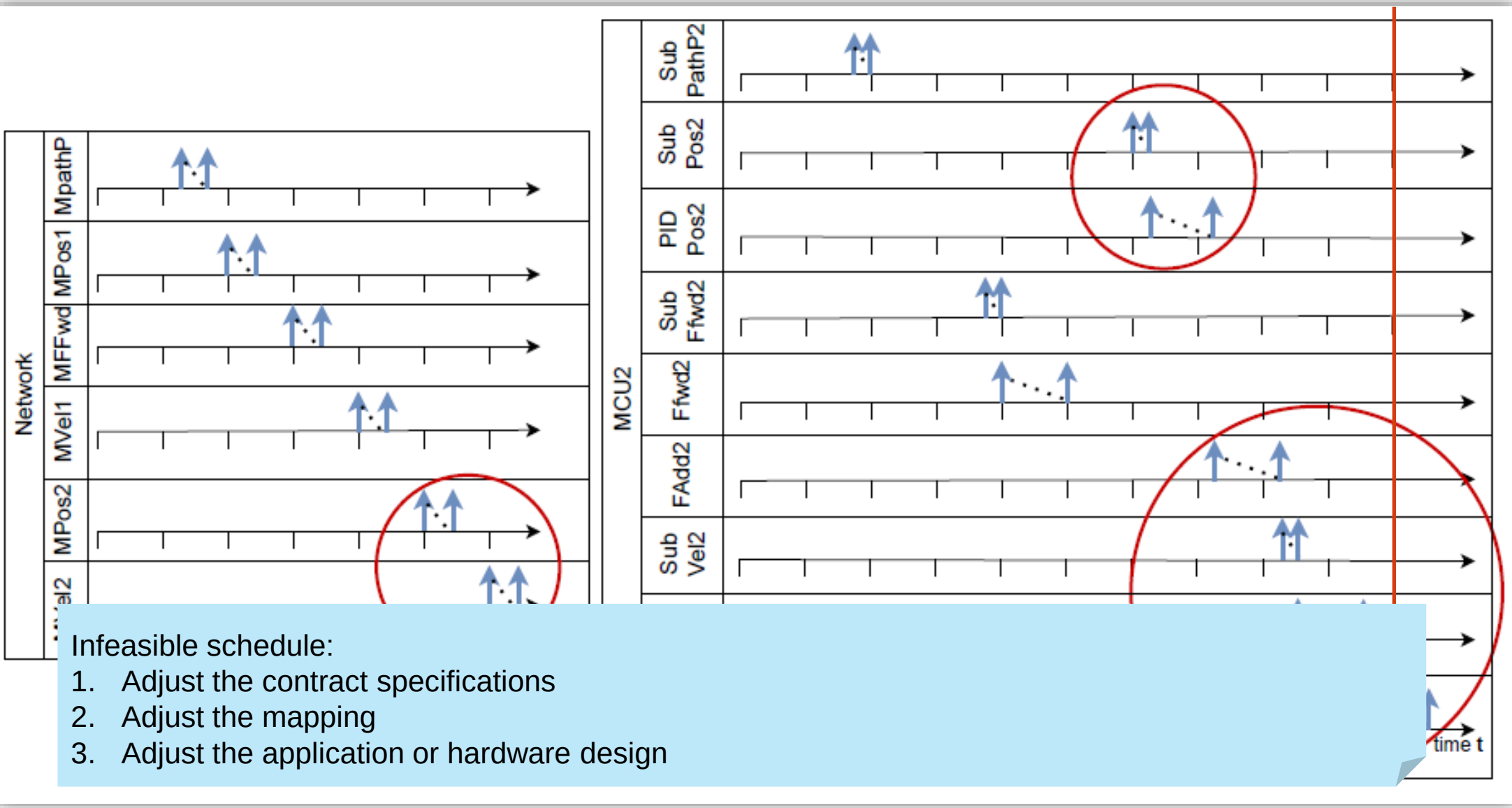
Joint Control Application Extended



Joint Control Application Extended



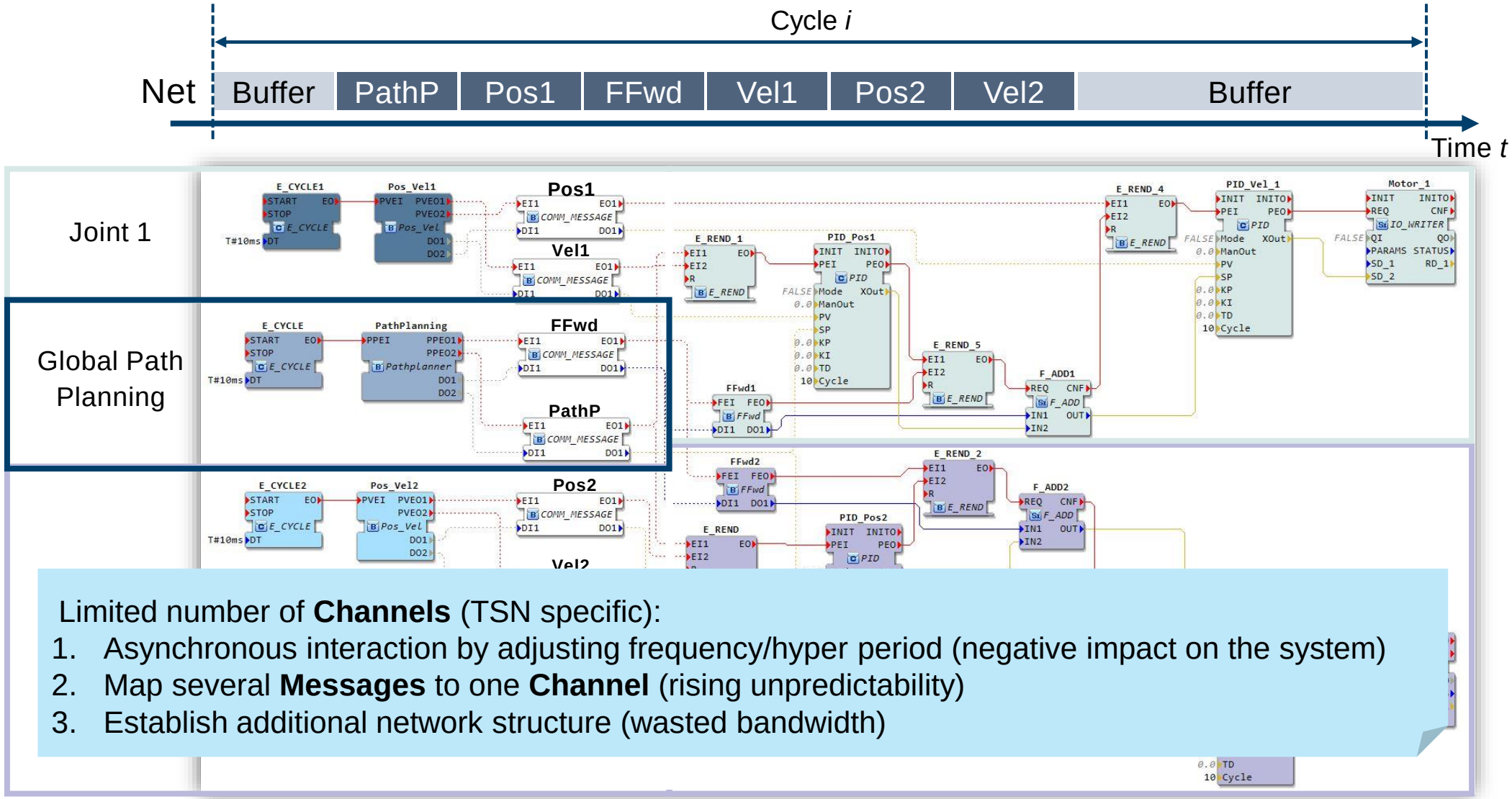
A Possible Time Trace with Multiple Contract Violations



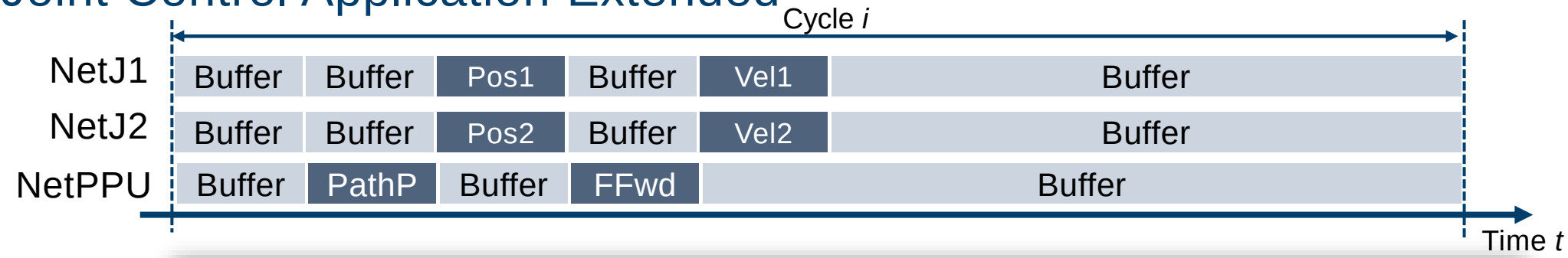
Infeasible schedule:

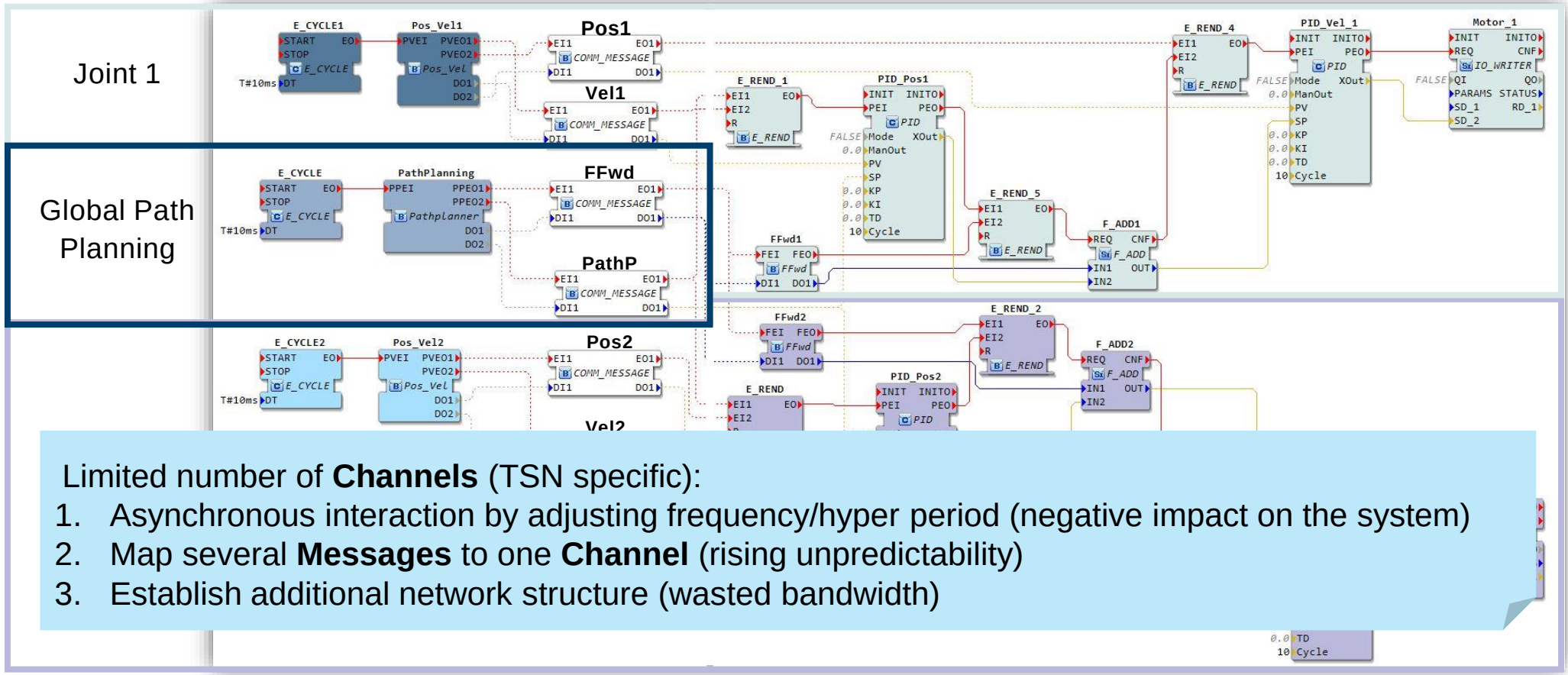
1. Adjust the contract specifications
2. Adjust the mapping
3. Adjust the application or hardware design

Joint Control Application Extended



Joint Control Application Extended

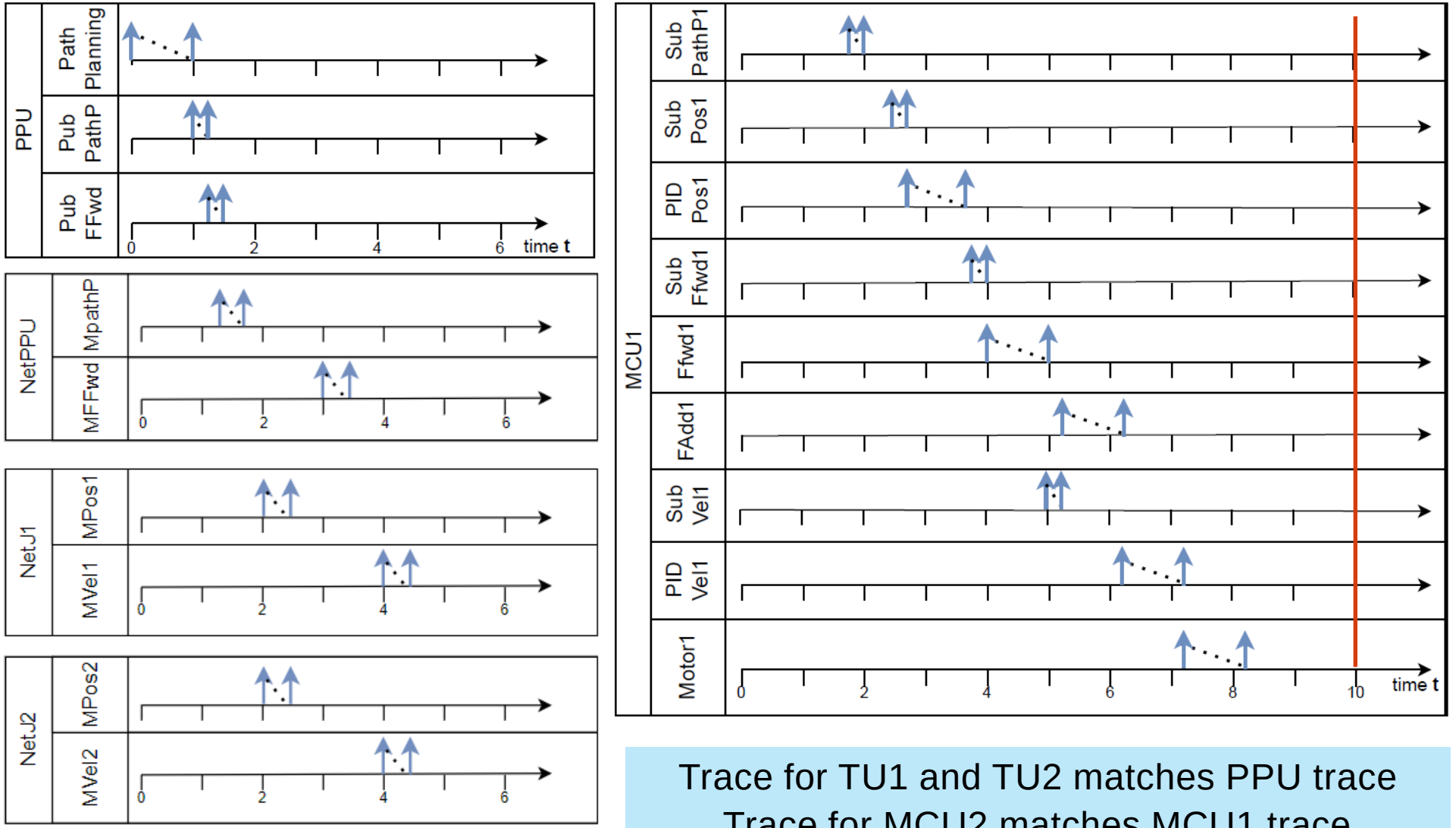




Limited number of **Channels** (TSN specific):

1. Asynchronous interaction by adjusting frequency/hyper period (negative impact on the system)
2. Map several **Messages** to one **Channel** (rising unpredictability)
3. Establish additional network structure (wasted bandwidth)

A Possible Time Trace



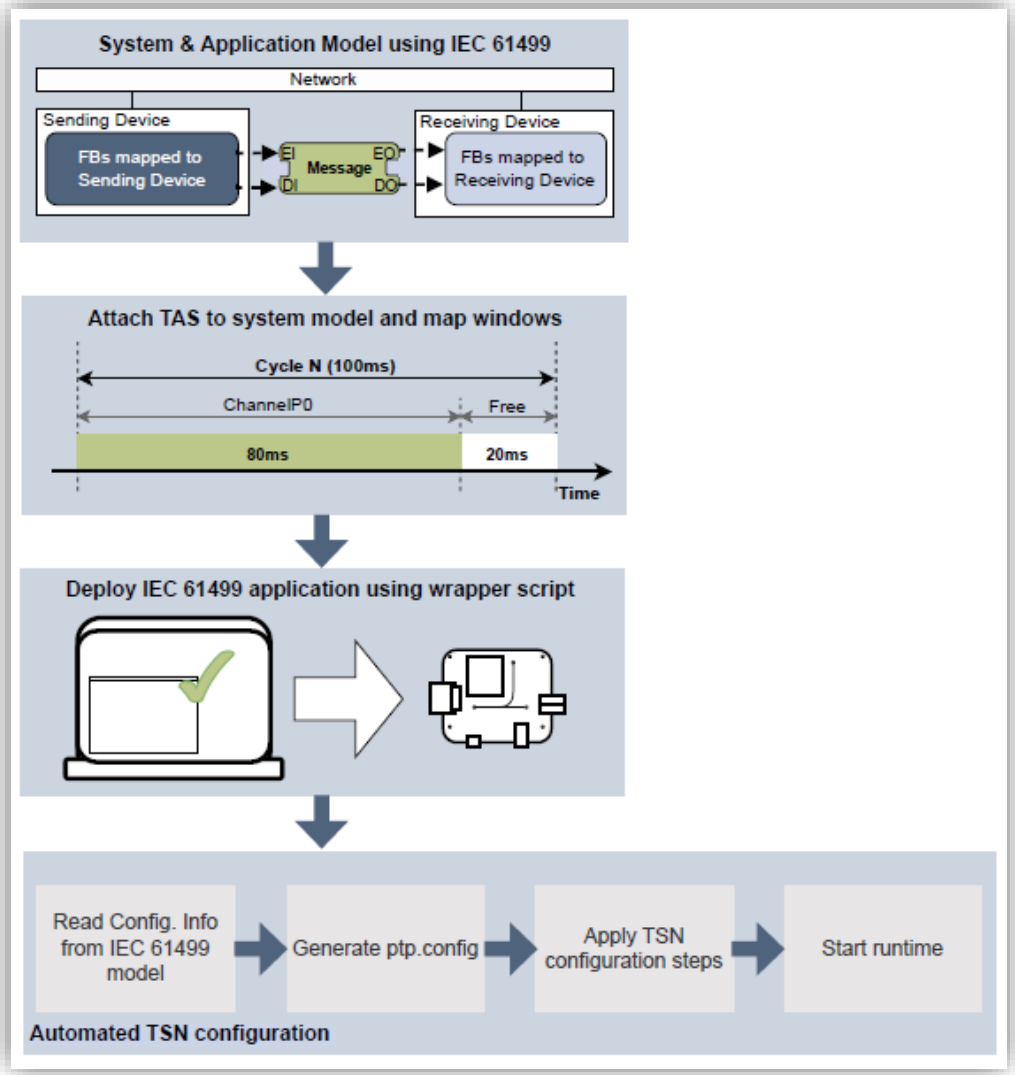
Trace for TU1 and TU2 matches PPU trace
Trace for MCU2 matches MCU1 trace

Automated Network Configuration

- Deployment using a wrapper script
- Automated execution of all configuration steps based on the provided information

Results:

- Varying number of higher & lower performant platforms
- No adjustments for Linux-based platforms
- Significantly streamlined process



B. J. Mackenzie, F. Bruns and W. Nebel, „Model-Based Automation of TSN Configuration for Industrial Distributed Systems", In *21st IEEE International Conference on Industrial Informatics (INDIN)*, Lemgo, Germany, 2023, IEEE, doi: 10.1109/INDIN51400.2023.10218085

Carl von Ossietzky Universität Oldenburg

Contributions & Future Work

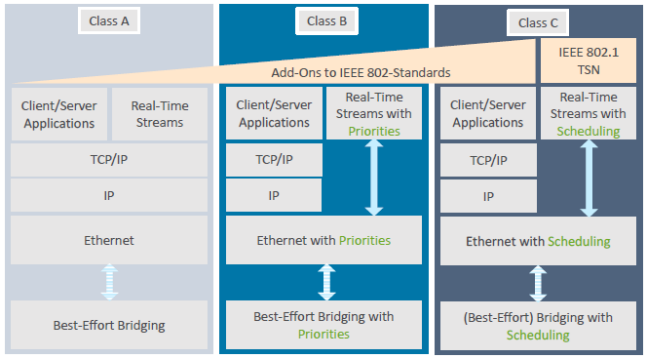
Main Contributions

- IEC 61499 extension for modelling network communication: Message, Channel, Mapping
- Enabled timing verification for IDCS
- Automated Network Configuration

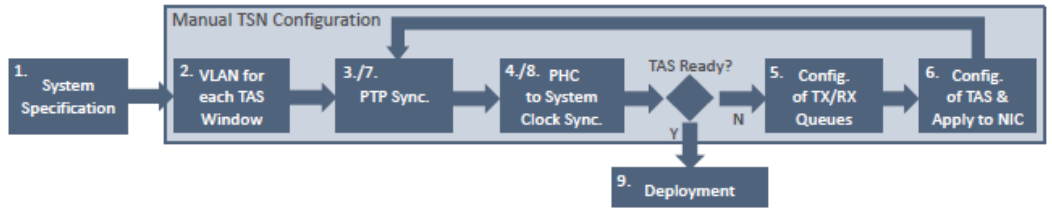
The extension is about to be standardised

Future Work

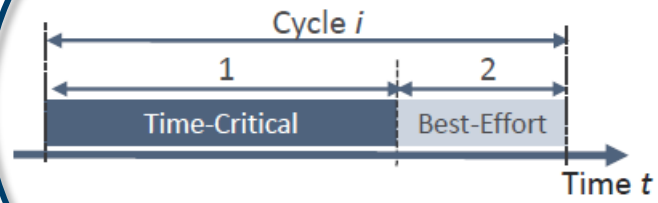
- Generating optimised schedules
- Use contracts as a basis for fault detection (offline and at run-time)
- Optimisation techniques for control systems (e.g., from an energy point of view)
- Model-based robust control and reduction of sensitivity against disturbances and faults
- Integration of uncertainty quantification



Ethernet Classification

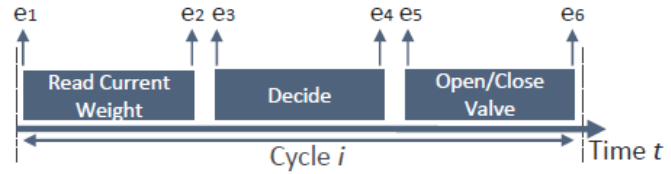


Time-Sensitive Networking (TSN)

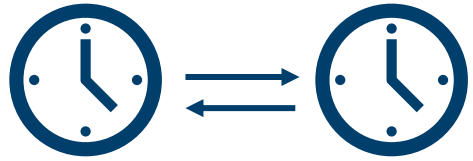


Real-Time Behaviour

Feature	Time-triggered	Event-triggered
Sporadic messages		✓
Periodic messages	✓	
Flexibility		✓
Predictability	✓	

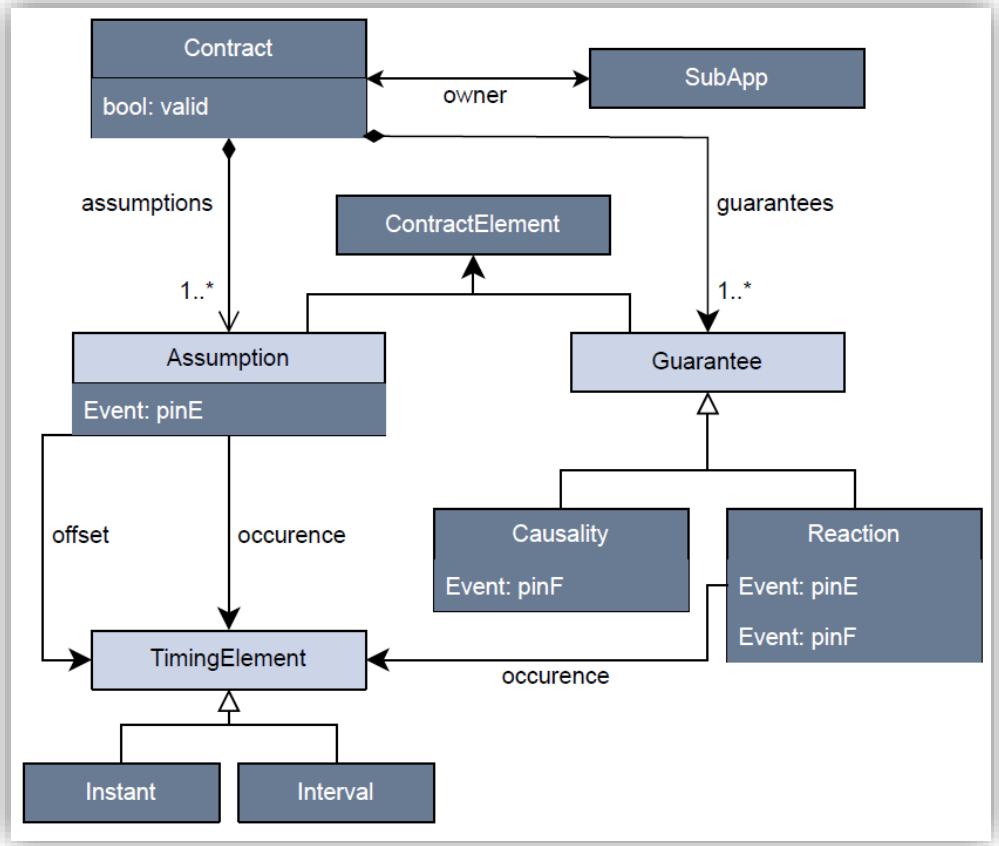


Execution Cycle



Time Synchronisation

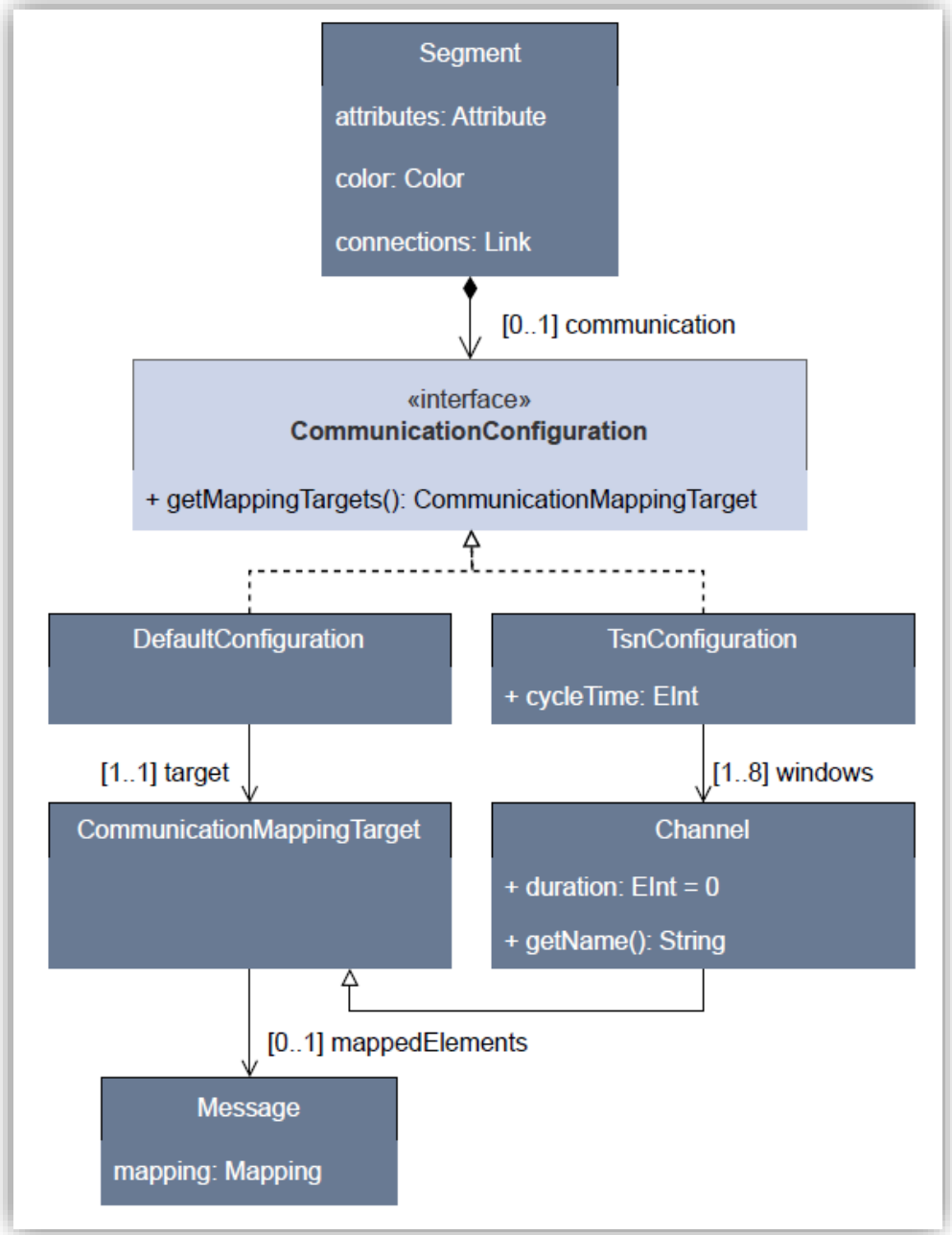
Integration of Timing Specifications in IEC 61499



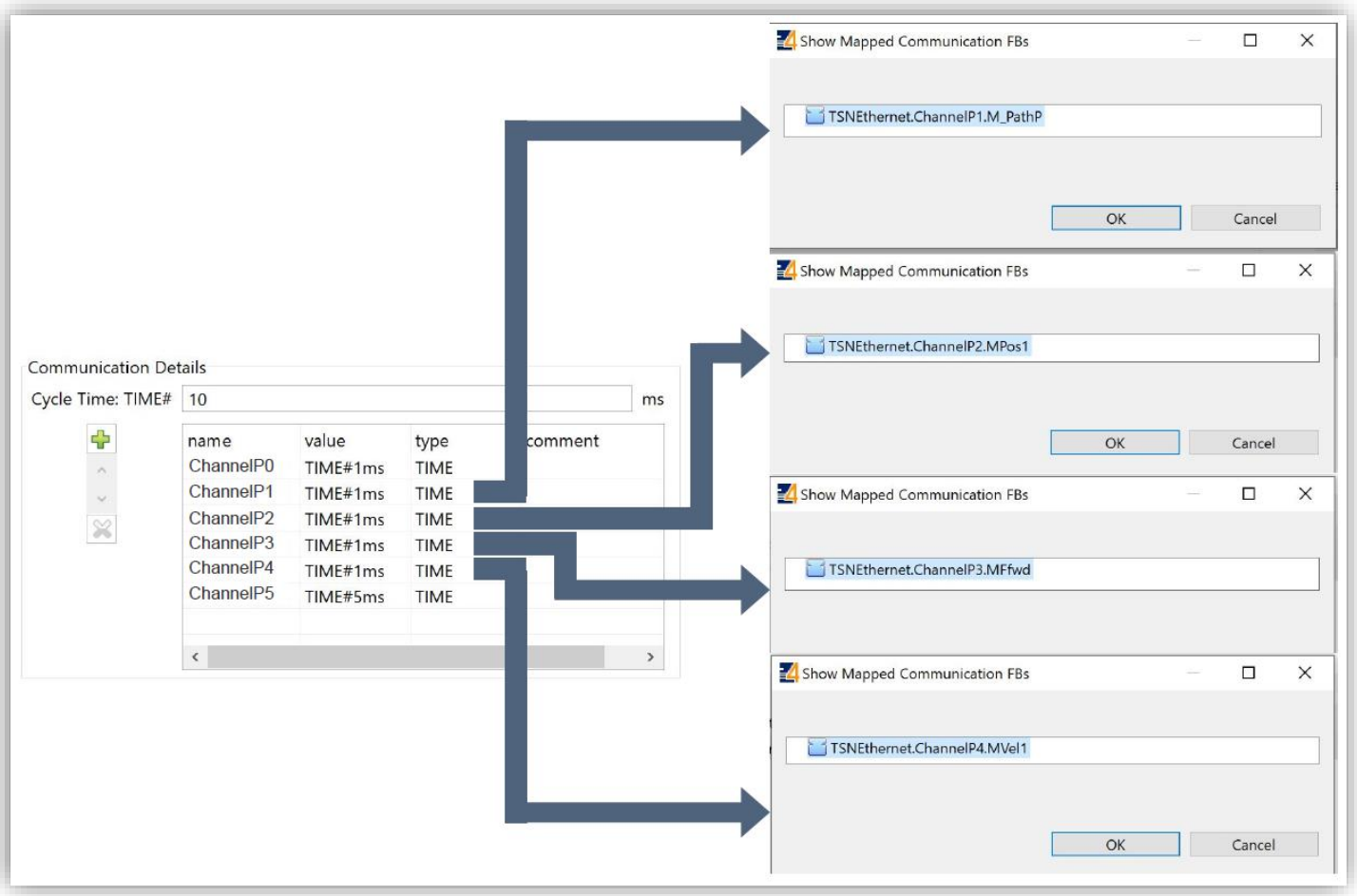

```
1 <SubApp Name="_CONTRACT_ValveCtrlApp" Comment="
2       A: IN occurs every [10, 10]ms;
3       G: Reaction(IN,OUT) within [10, 10]ms">
4       <SubAppInterfaceList>
5               <SubAppEventInputs>
6                       <SubAppEvent Name="REQ" Type="Event" Comment="">
7                       </SubAppEvent>
8               </SubAppEventInputs>
9               <SubAppEventOutputs>
10                      <SubAppEvent Name="CNF" Type="Event" Comment="">
11                      </SubAppEvent>
12              </SubAppEventOutputs>
13              ... <!--VarDeclarations-->
14      <SubAppNetwork>
15       .....
16      </SubAppNetwork>
17 </SubApp>
```

IEC 61499 Modelling Extension

- DefaultConfiguration
  - Single communication
  - Specifically tailored for best-effort traffic
- TsnConfiguration
  - Concrete implementation of the concept
  - Parameters: cycleTime, a list of up to 8 Channels each with its specified duration
  - Limitation of 8 Channels could be easily adapted, when there are respective changes to the TSN standard



Mapping Process



- Basis for systematic mapping
- Overview of all messages mapped to channels
- Enables automation processes

XML Specifications

CHANNEL

```
1 <SegmentType Name="EthernetTSN" Comment="">
2       <Identification .../>
3       <VersionInfo .../>
4       <CompilerInfo/>
5       <VarDeclaration Name="CycleTime" Type="TIME"
6               InitialValue="T#10ms" Comment="Cycle Time"/>
7       <VarDeclaration Name="ChannelP0" Type="TIME"
8               InitialValue="" Comment=""/>
9       <VarDeclaration Name="ChannelP1" Type="TIME"
10              InitialValue="" Comment=""/>
11       ...
12       <VarDeclaration Name="ChannelP7" Type="TIME"
13              InitialValue="" Comment=""/>
14 </SegmentType>
```

MESSAGE

```
1 <Application Name="App" Comment="">
2       ...
3       <FB Name="MsgWith1DataPin" Type="MESSAGE_1"
4               Comment="" .../>
5       <FB Name="MsgWith2DataPins" Type="MESSAGE_2"
6               Comment="" .../>
7       .... <!-- connections -->
8 </Application>
```

Mapping

```
1 <Mapping From="App.Message0"
2       To="Tsn10.ChannelP0"/>
3 <Mapping From="App.Message1"
4       To="Tsn10.ChannelP1"/>
```

Timing Information for all FBs

Function Block	Offset [ms]	WCET [ms]	Function Block	Offset [ms]	WCET [ms]
Pathplanning	0	1	**Sub_PathP1**	1.75	0.25
Pub_FFwd	1.25	0.25	**Sub_Pos1**	2.5	0.25
Pub_PathP	1	0.25	**PID_Pos1**	2.75	1
M_FFwd	3	0.5	**Sub_FFwd1**	3.75	0.25
M_PathP	1.25	0.5	**FFwd1**	4	1
Pos_Vel1	0	1	**Sub_Vel1**	5	0.25
Pub_Pos1	1	0.25	**F_ADD1**	5.25	1
Pub_Vel1	1.25	0.25	**PID_Vel1**	6.25	1
M_Pos1	2	0.5	**Motor1**	7.25	1
M_Vel1	4	0.5			

Message FBs Contracts

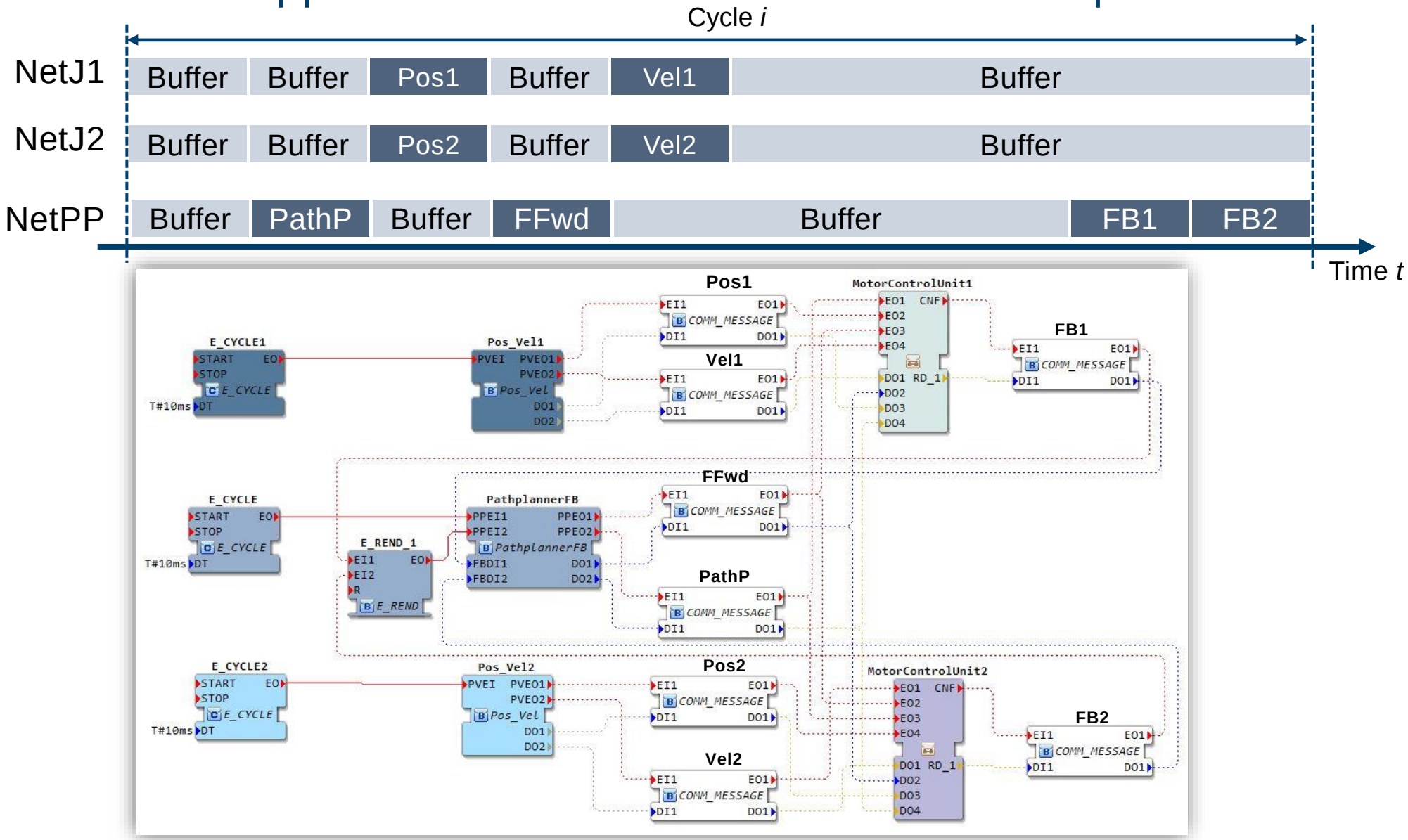
_CONTRACT_MESSAGE_PATHP	
A	MPathPEI occurs every 10 ms with 1 ms offset.
G	Reaction(MPathPEI, MPathPEO) occurs within 1 ms.

_CONTRACT_MESSAGE_POS1	
A	MPos1EI occurs every 10 ms with 1 ms offset.
G	Reaction(MPos1EI, MPos1EO) occurs within 1.75 ms.

_CONTRACT_MESSAGE_FFWD	
A	MFFwdEI occurs every 10 ms with 1.25 ms offset.
G	Reaction(MFFwdEI, MFFwdEO) occurs within 2.75 ms.

_CONTRACT_MESSAGE_VEL1	
A	MVel1EI occurs every 10 ms with 1.25 ms offset.
G	Reaction(MVel1EI, MVel1EO) occurs within 5 ms.

Joint Control Application Extended with Feedback Loop



A Valid Mapping that Does Not Violate Contracts