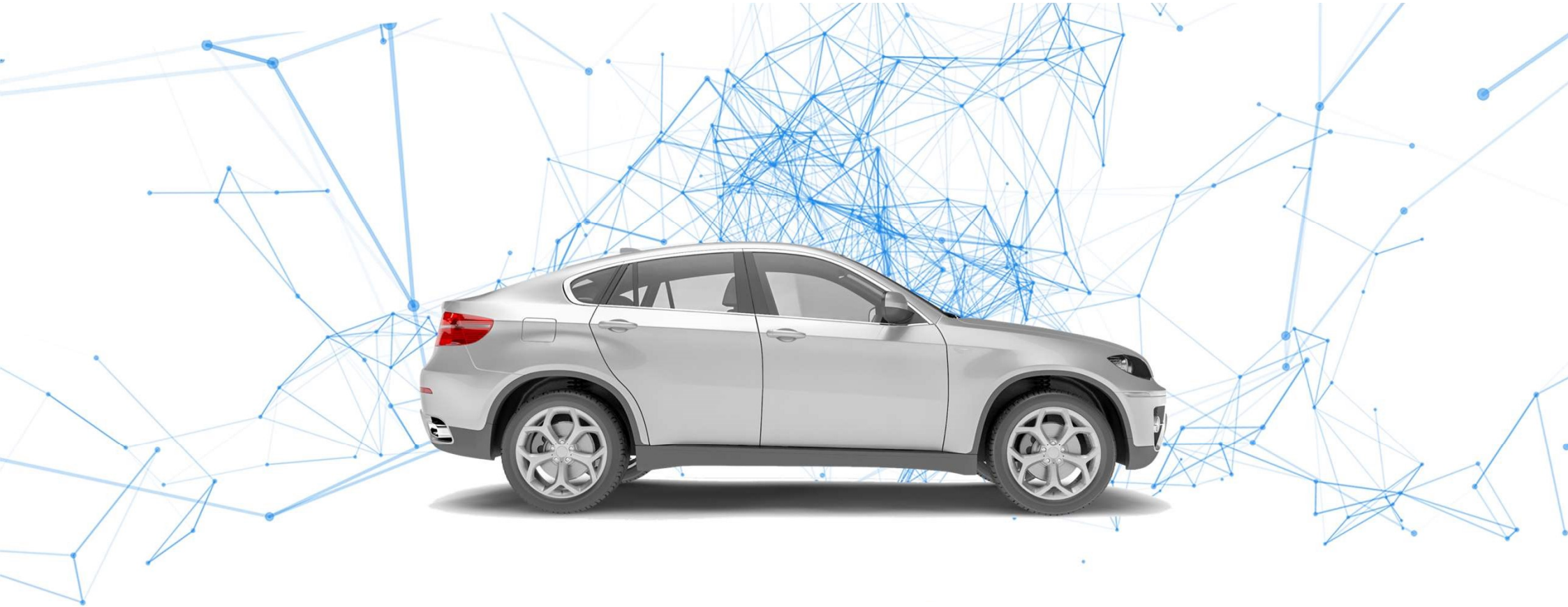


Safety Issues with gPTP and Potential Solutions

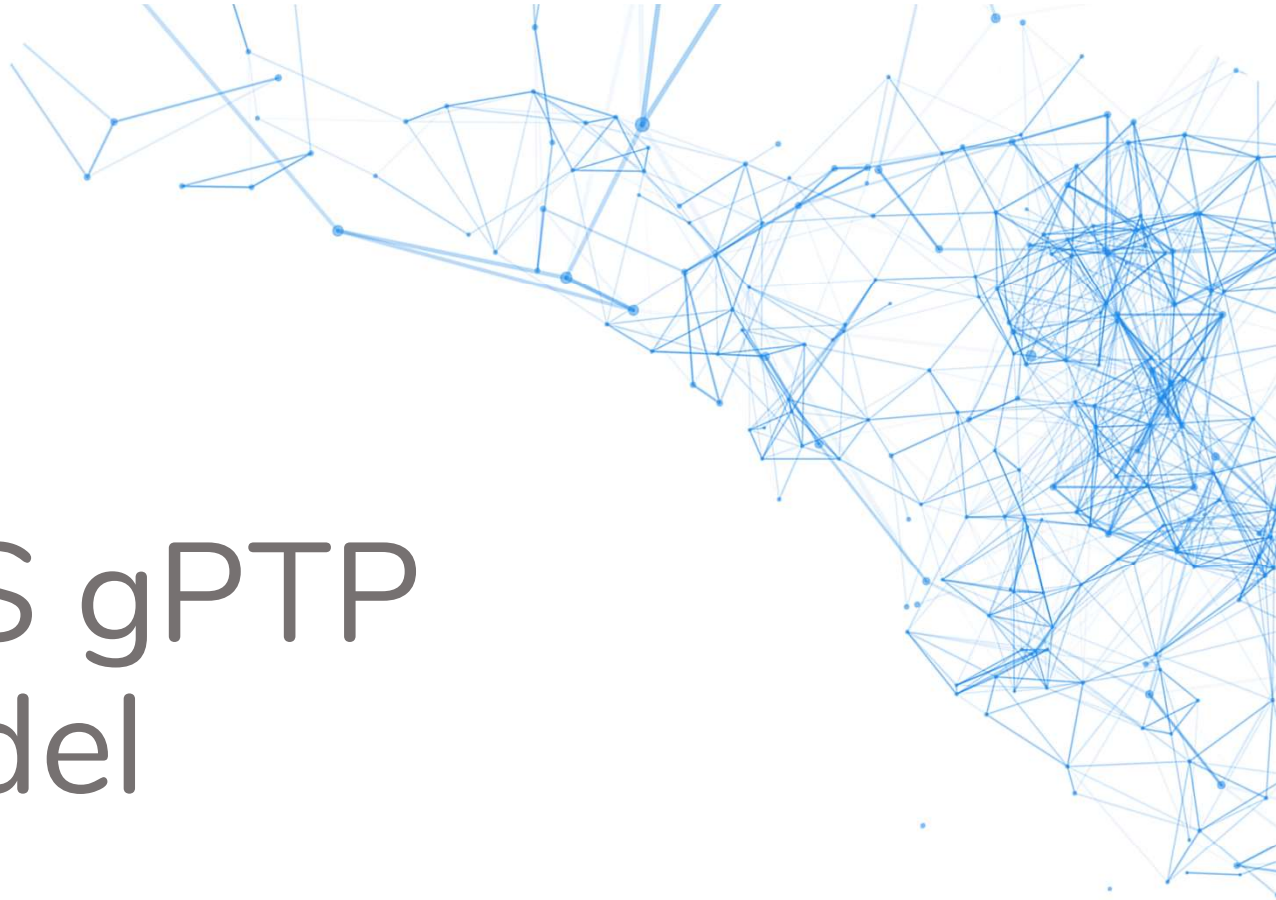
IEEE SA Ethernet & IP @ Automotive Technology Day 2020

Max Turner

ETHERNOVIA

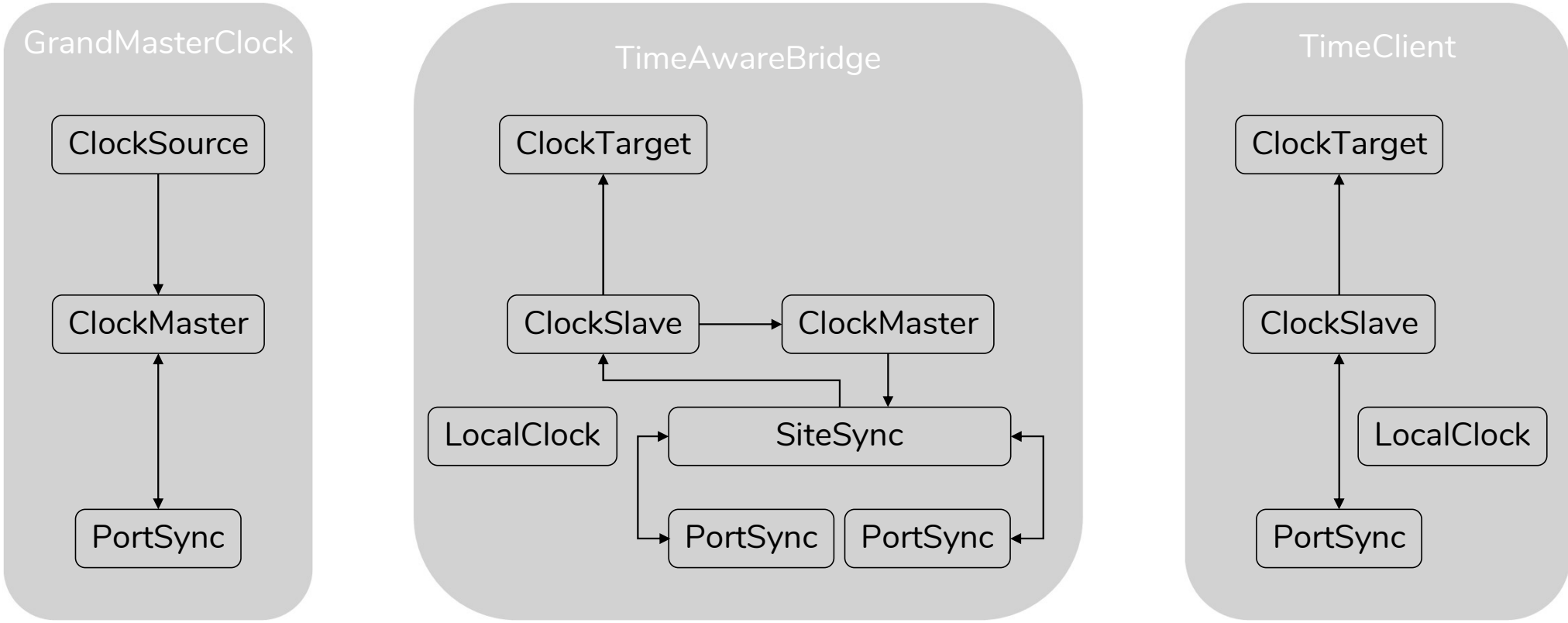
TRANSFORMING HOW CARS OF THE FUTURE ARE BUILT

Max Turner



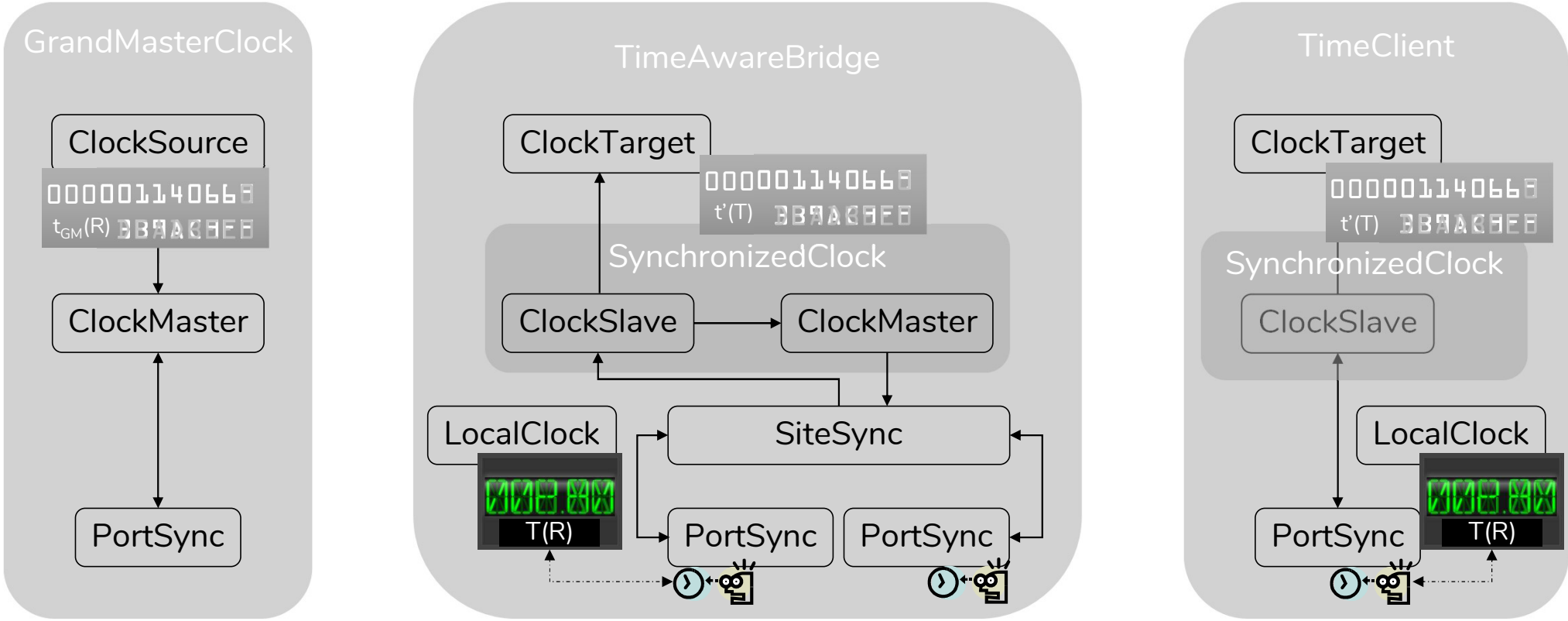
IEEE802.1AS gPTP Instance Model

IEEE802.1AS - gPTP Instance Models



ETHERNOVIA
TRANSFORMING HOW CARS OF THE FUTURE ARE BUILT

Symbols and Nomenclature

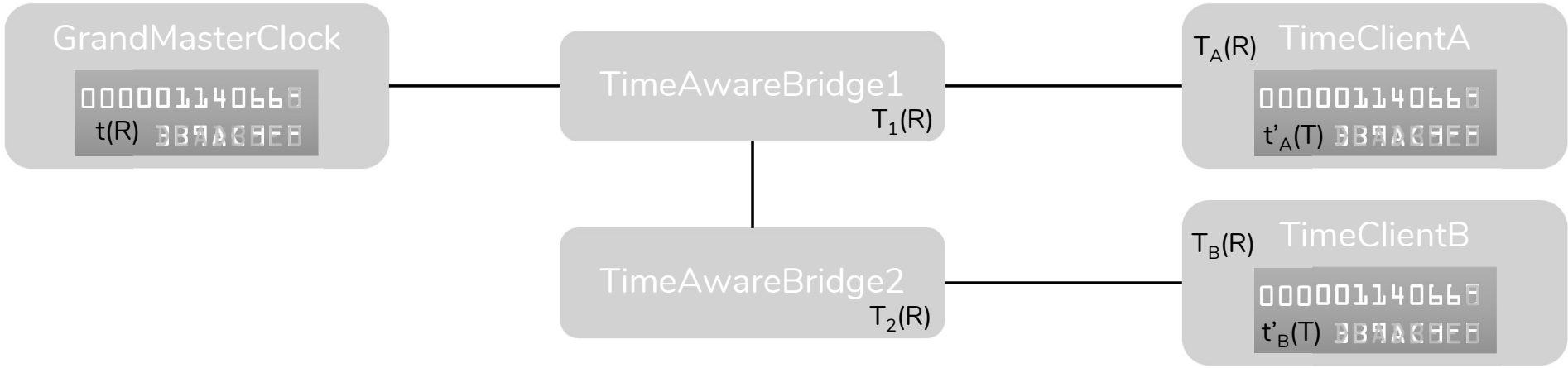


T … LocalClock (free running)

t' … SynchronizedClock (syntonous with GM)

Problem Description

Problem Description

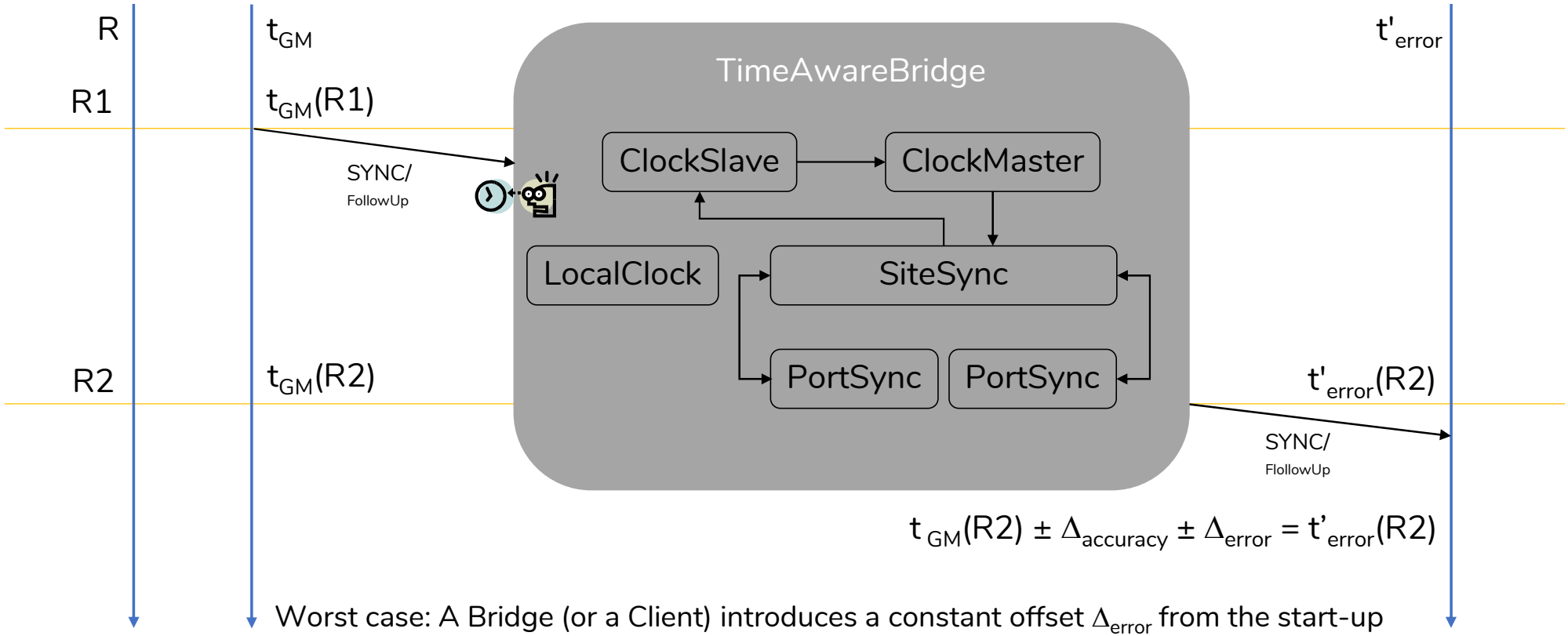


- gPTP-Sync-Messages (t') sent from GM to the Bridges/Clients
- pDelay-Messages based on Local-Clock (T) information
- How can we ensure – in safety terms – at any one point in Real-Time (R), the GM and all (relevant) clients have synchronized to the same clock-counter value, within an accepted accuracy?
  $t(R) \approx t'_A(R) \approx t'_B(R)$

Not Part of This Discussion

- For a sensor to measure a physical property over time, there must be an absolute reference to Real-Time (R), i.e. the clock must be syntonous to International Atomic Time (TAI)
  - This discussion will not cover ensuring the absolute accuracy of a clock with respect to TAI
- In order to check the validity of a security certificate a current Date and Time is required, i.e. the clock must be synchronous to Coordinated Universal Time (UTC)
  - This discussion will not cover a secure way to support current Date and Time with respect to UTC

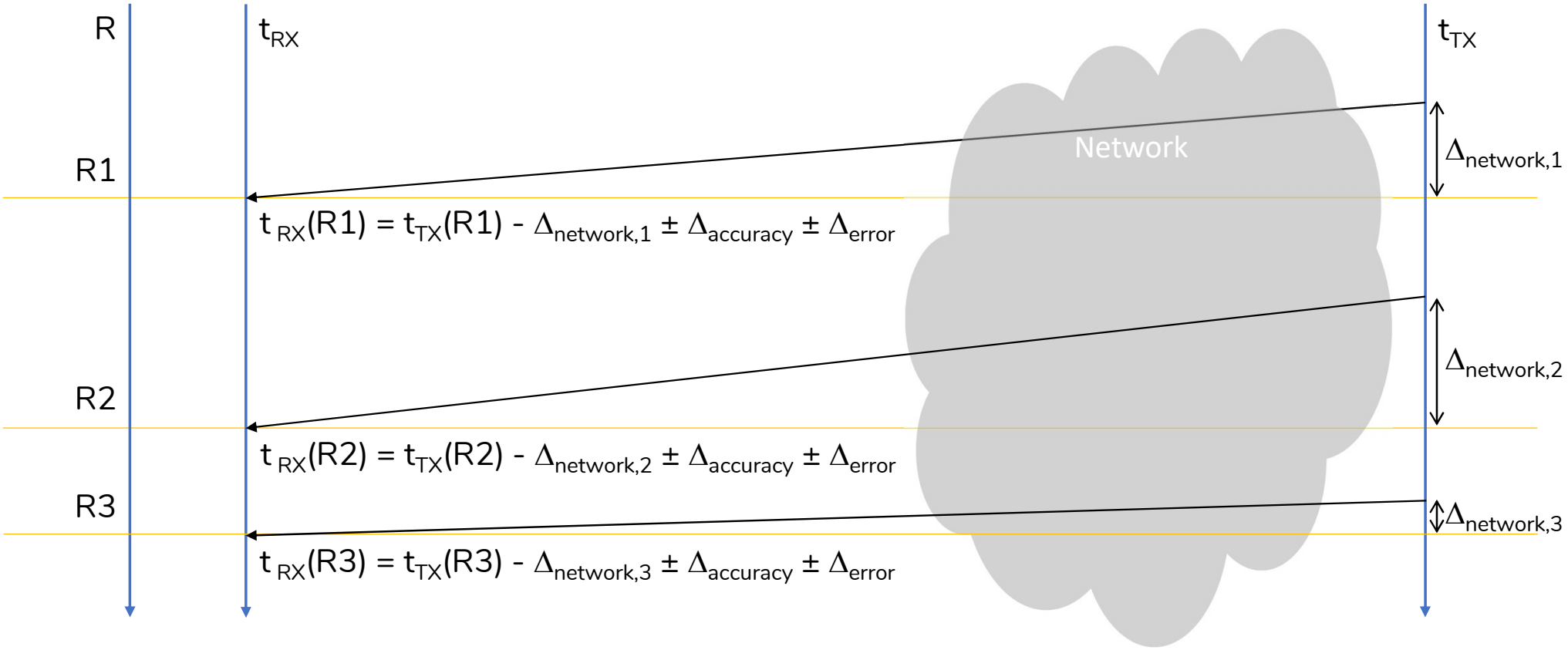
The “Byzantine” Bridge Error



Worst case: A Bridge (or a Client) introduces a constant offset Δ_{error} from the start-up (not a transient change)

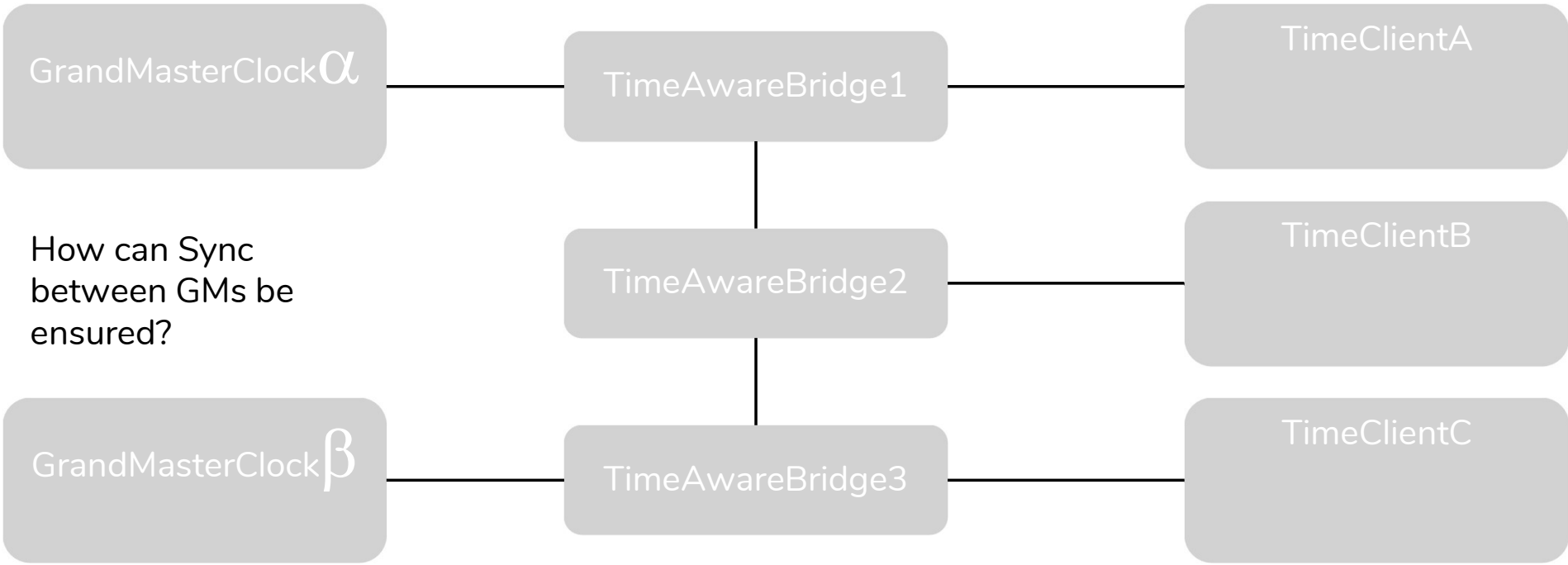
Potential Solutions

Statistical Approach



Changes in the network delay may influence detectability of constant offset

Redundant GM



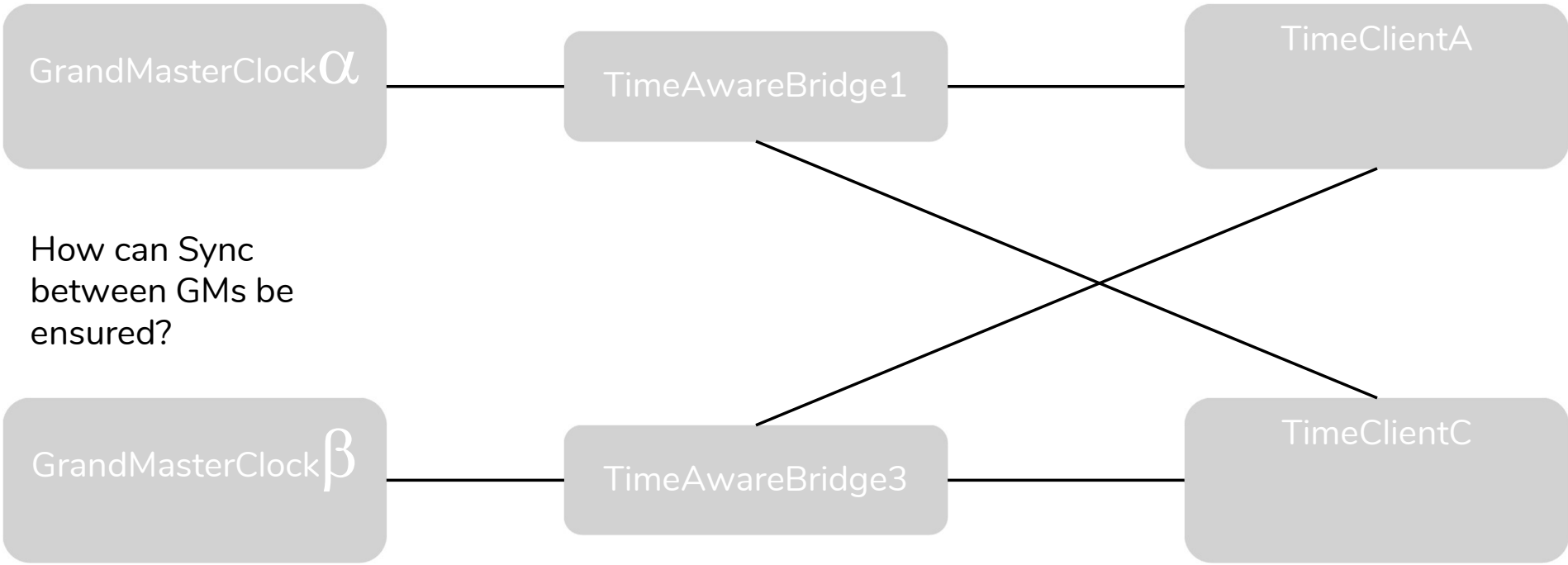
Added element may reduce availability and introduce new error scenarios

Bridges can still introduce constant offset to both domains

Clients can compare domains but must avoid common cause failures
Client status not available to monitor

ETHERNOVIA
TRANSFORMING HOW CARS OF THE FUTURE ARE BUILT

Redundant Client Connections



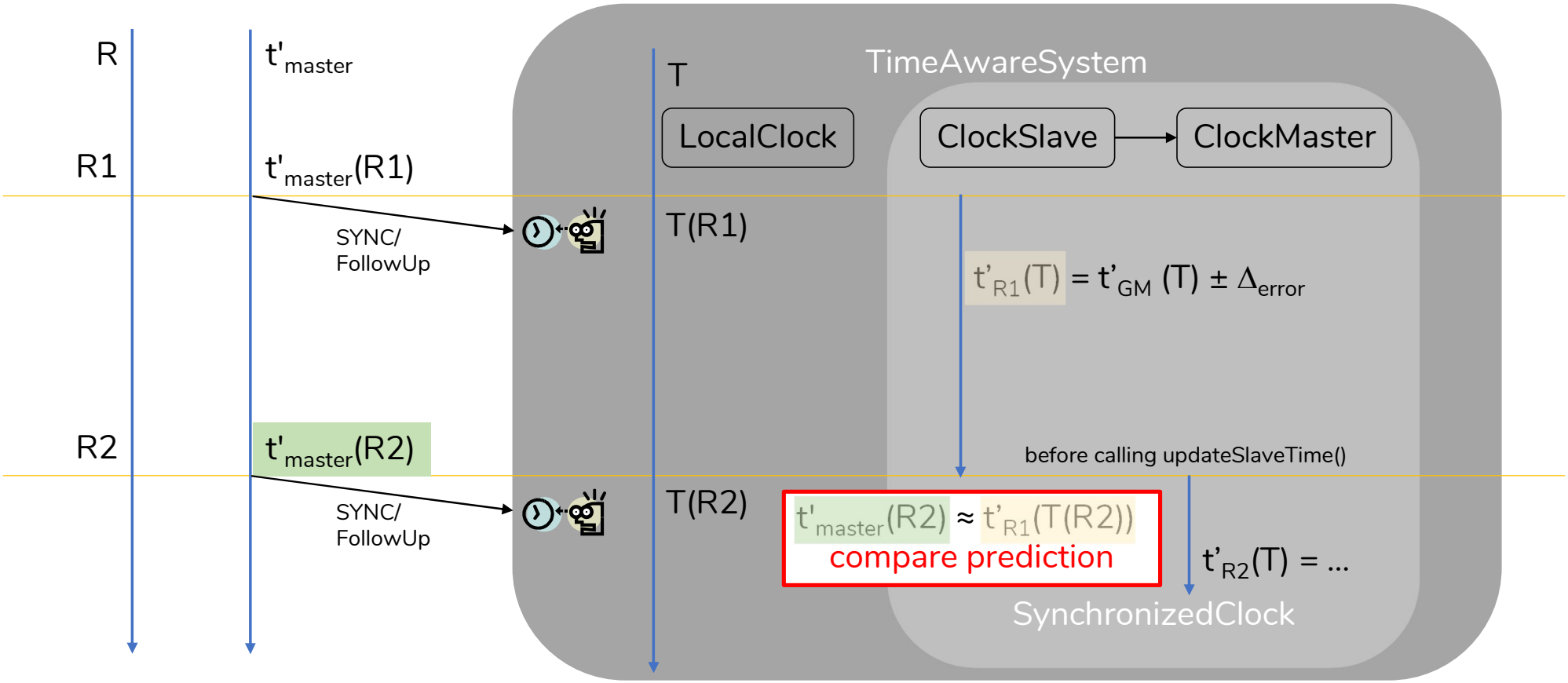
Added elements may reduce availability and introduce new error scenarios

Bridges can still introduce constant offset to one domain

Clients can compare domains locally but cannot compare each other

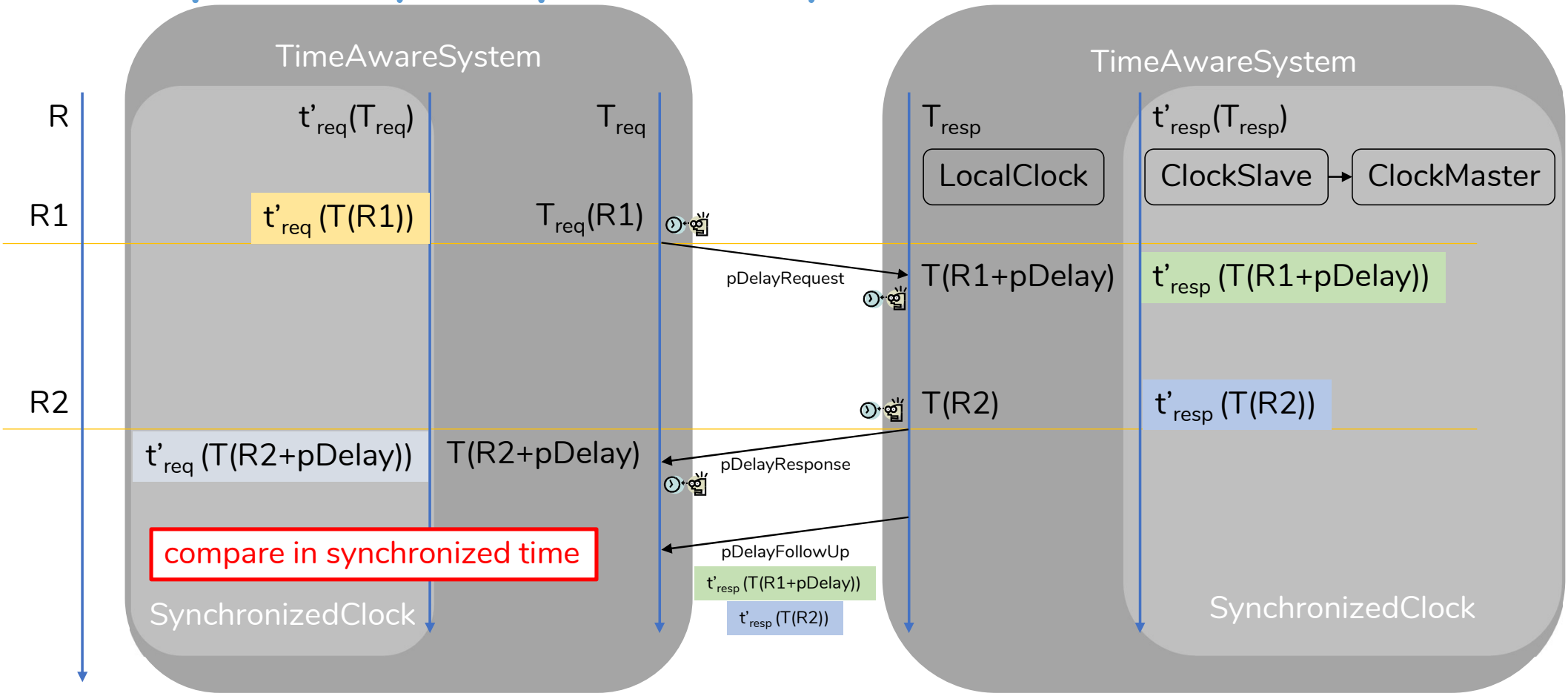
Central Validator Approach

Predict next originTimestamp



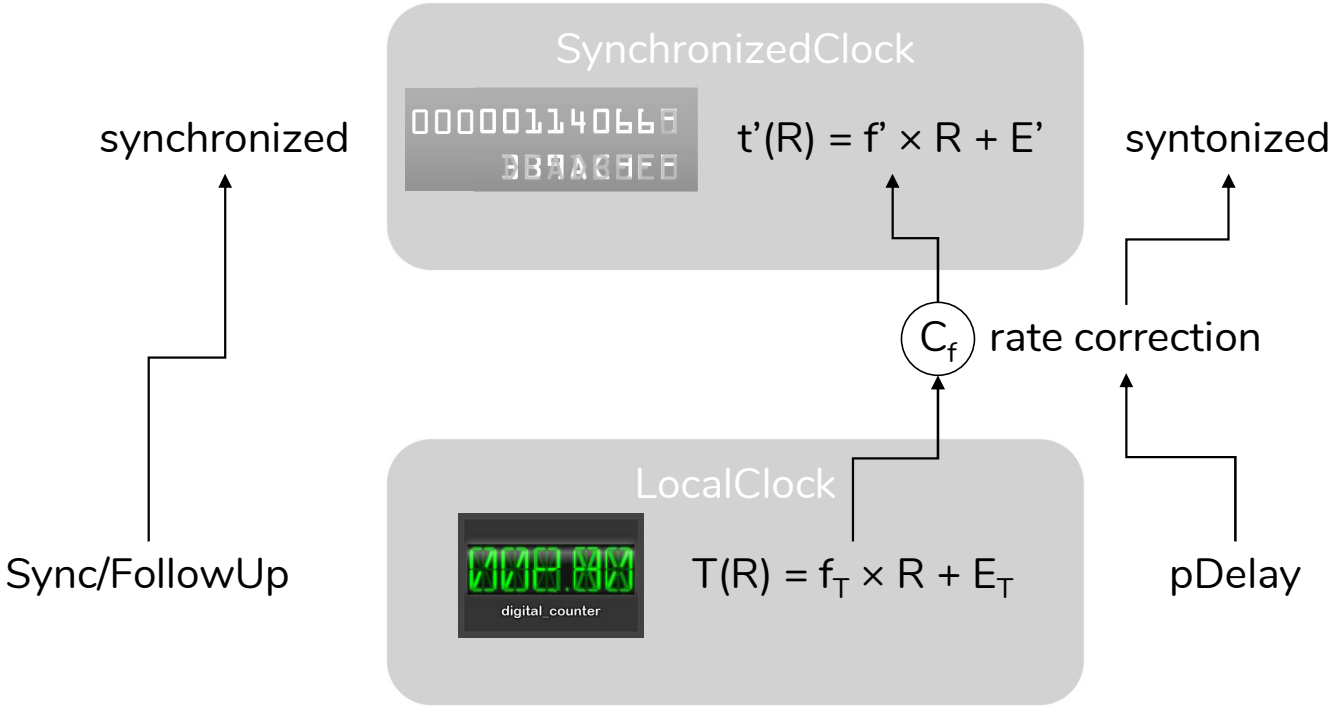
pDelay neglected

Use pDelay to probe SynchronizedClock



ETHERNOVIA
TRANSFORMING HOW CARS OF THE FUTURE ARE BUILT

Why neighbourRateRatio from pDelay?



Improved Start-Up time:

- Can start on each link after link-up
- pDelay and neighbourRateRatio are already known when first Sync-Message arrives

Boundary Clock: create new OriginTimeStamp for transmitted Sync-Message
Transparent Clock: keep incoming OriginTimeStamp, add CorrectionField in Local-Time to transmitted Sync-Message

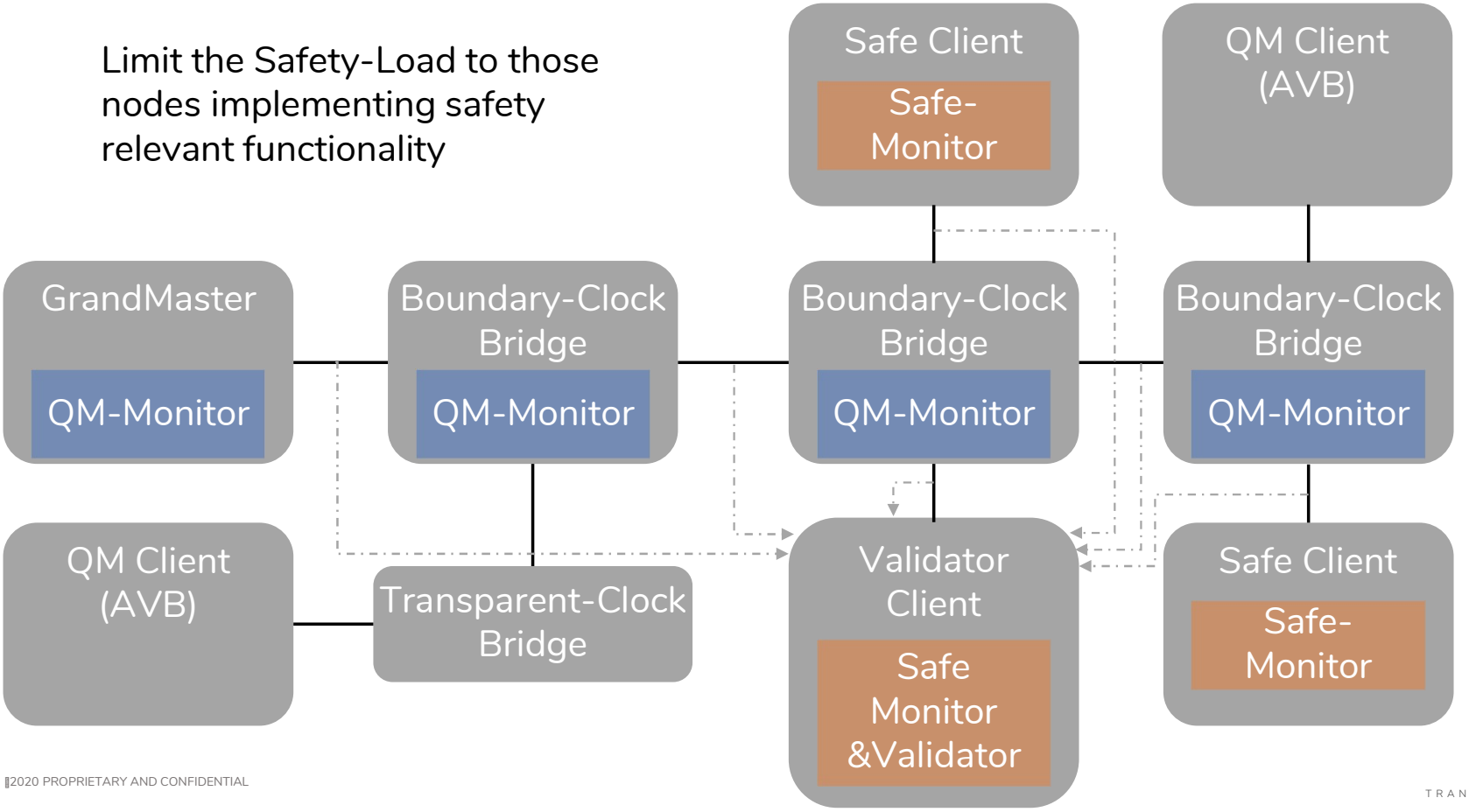
List of Data-Points per Link

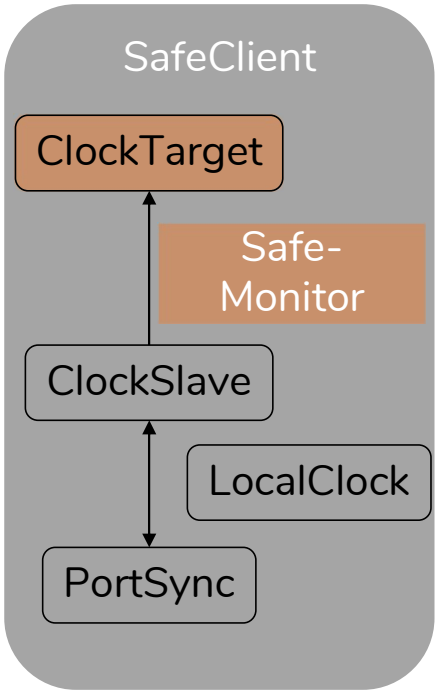
Event Message	Transmit time-stamp	Receive time-stamp
Sync-Message	$T_{master}(R_{sync})$ $t'_{master}(T(R_{sync}))$ [also in FollowUp-Msg]	$T_{client}(R_{sync}+pDelay)$ $t'_{client}(T(R_{sync}+pDelay))$
pDelayRequest-Message	$T_{req}(R_{req})$ $t'_{req}(T(R_{req}))$	$T_{resp}(R_{req}+pDelay)$ [also in pDelayFollowUp-Msg] $t'_{resp}(T(R_{req}+pDelay))$
pDelayResponse-Message	$T_{resp}(R_{resp})$ [also in pDelayFollowUp-Msg] $t'_{resp}(T(R_{resp}+pDelay))$	$T_{req}(R_{resp}+pDelay)$ $t'_{req}(T(R_{resp}+pDelay))$

Autosar has added interfaces to record these time-tuples, should IEEE802.1AS and IEEE1588 follow?
The knowledge of Synchronized Time at each port requires Boundary Clocks

Mixed System Overview

Limit the Safety-Load to those nodes implementing safety relevant functionality





ETHERNOVIA
TRANSFORMING HOW CARS OF THE FUTURE ARE BUILT

Summary

Central Time Validation Concept

- Boundary-Clock Bridges required
- Additional interfaces required
- Additional communication channel
- Frequency of validation messages determines time to detection
- Definition of limits is TBD
- Interop with multiple time-domains is TBD
- Monitoring done in QM
- Safety load applied only where needed
- Can be adopted to other busses (FR, CAN, …)
- Can check local and synchronized clocks
- Can detect “Byzantine” fault
- Works with AVnu hold-over Bridges

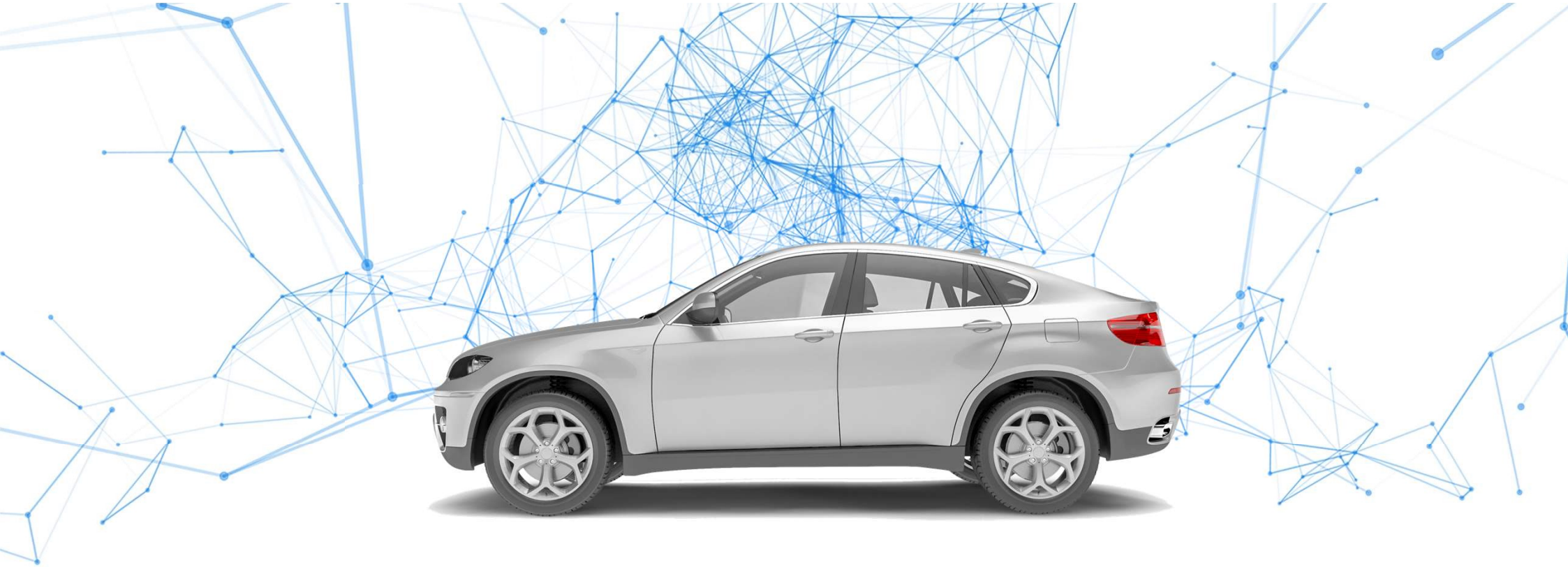
Thanks

Special thanks go to:

- Karl Budweiser, BMW
- Florian Bogenberger, Exida
- Emily Hudoletnjak, Exida

For patiently discussing, simulating and thinking up improvements!

Further reading: “A Method for Validation of Time Synchronization in Automotive Ethernet Networks” by Valentin Haider, Deggendorf Institute of Technology, Feb. 2020



THANK YOU

ETHERNOVIA | max.turner@ethernovia.com