Security on the Fast Lane

How quick can MKA get in IVNs

Friedrich Wiemer (Bosch), Lara Hallaczek,
Nils Heitmann (NXP)

2025 Ethernet & IP @ Automotive Technology Day,
15-16 October 2025

Öffentlich C-SC0

Agenda

MACsec, MKA and Automotive MKA

1st Eval: Hypothesis

2nd Eval: Simulation

3rd Eval: Demonstrator

Conclusion

Öffentlich C-SC0

MACsec
Media Access Control Security

Integrity

Authenticity

Confidentiality

IEEE SA
STANDARDS ASSOCIATION

IEEE Standard for
Local and Metropoli

Port-Based Networ

IEEE Computer Society

Developed by the
LAN/MAN Standards Committee

IEEE Std 802.1X™-2020
(Revision of IEEE Std 802.1X-2010
Incorporating IEEE Std 802.1Xbx™-2014
and IEEE Std 802.1Xck™-2018)

IEEE

Authorized licensed use limited to: ROBERT BOSCH.

IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 802.1AE™-2018
(Revision of IEEE Std 802.1AE-2006)

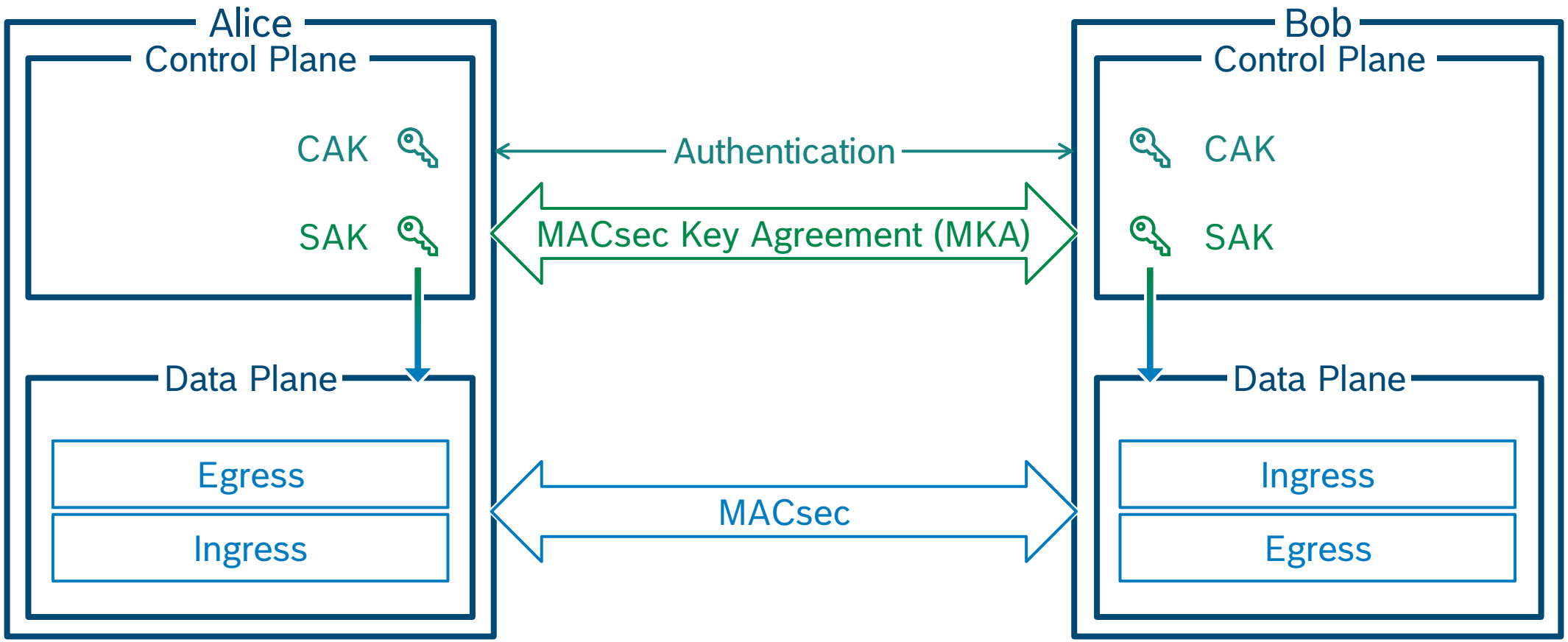
Authorized licensed use limited to: ROBERT BOSCH. Downloaded on July 05,2024 at 16:50:24 UTC from IEEE Xplore. Restrictions apply.

Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

MACsec
Connectivity Association

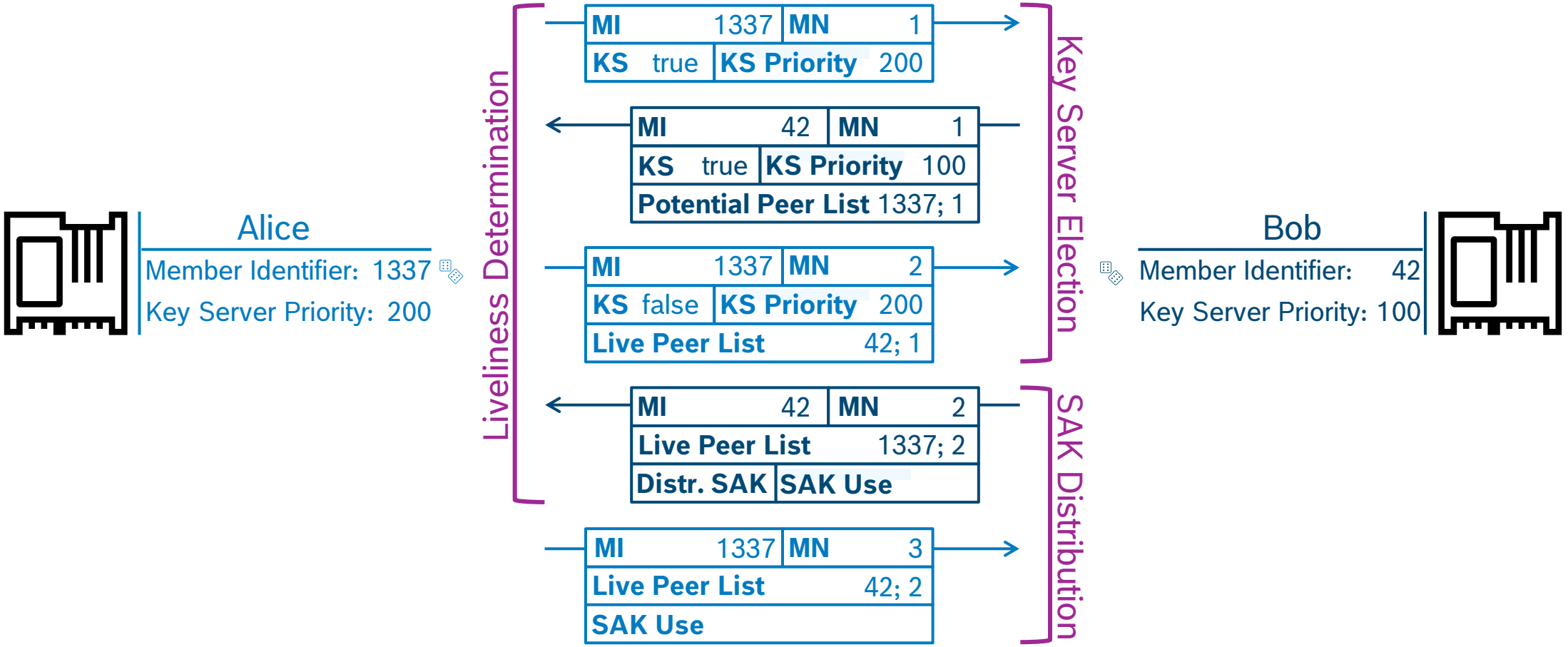
CAK Connectivity Association Key
SAK Secure Association Key



Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

MACsec Key Agreement (MKA)
Key Agreement Sequence



Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Automotive MKA
Optimizations

Pre-Selected Key Server

Immediate Responses and Reset Detection

Hello Time Ramp Up

Automotive MKA Specification

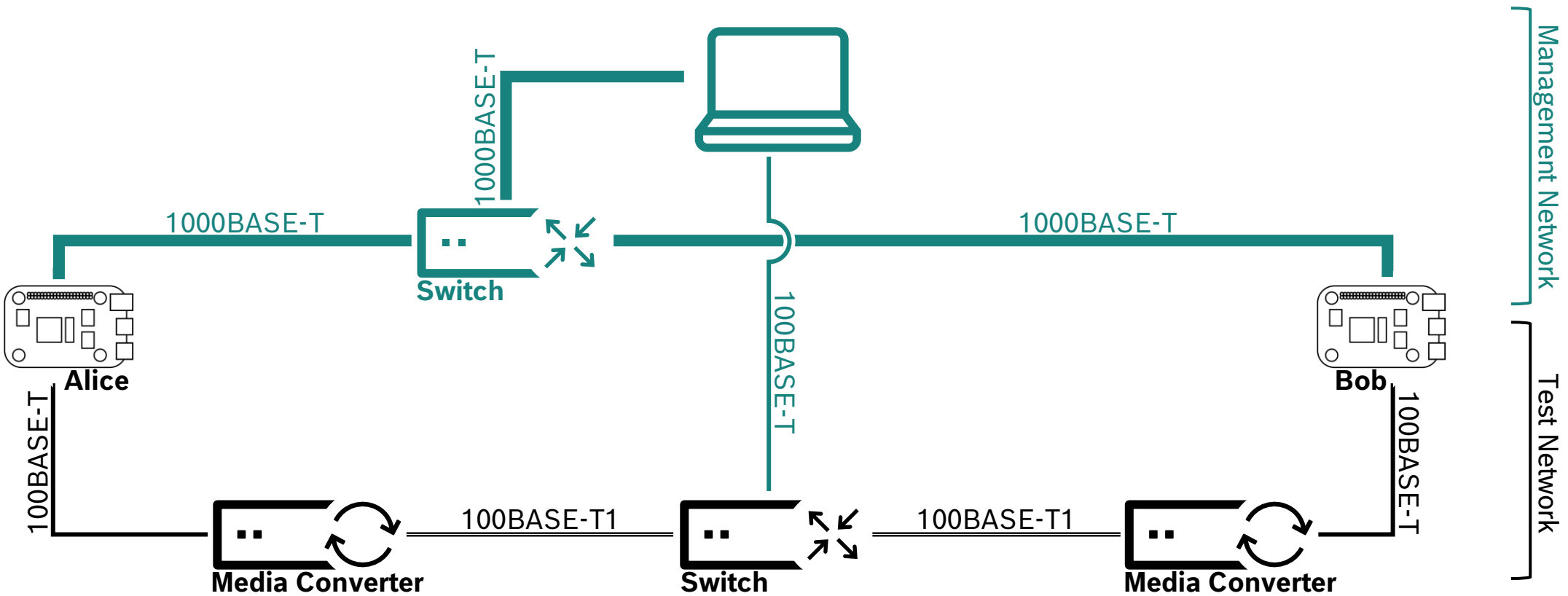
Automotive MKA Specification for Automotive Ethernet and MACsec

Version	1.0
Date	26.02.2025
Status	Final
Restriction Level	Public

Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Timing Evaluation
Raspberry Pi Demonstrator

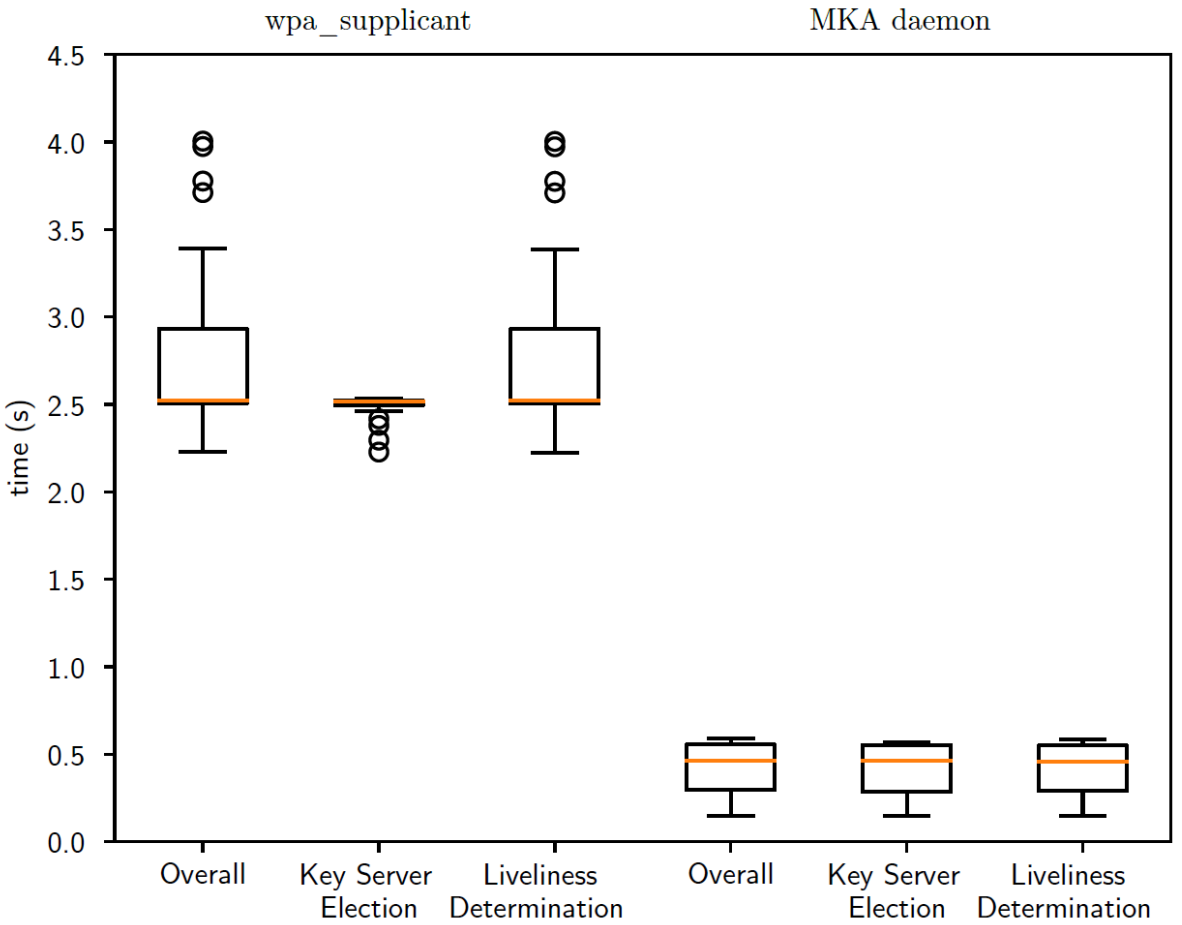


Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

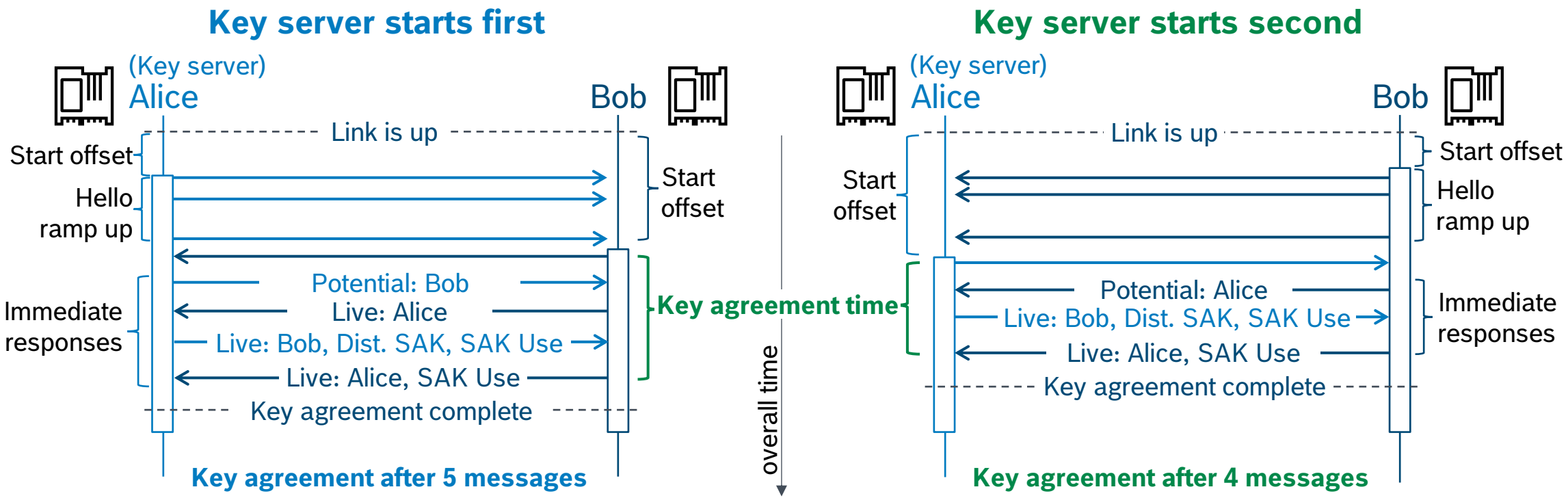
Timing Evaluation
Raspberry Pi Demonstrator: First measurements

- Running time of MKA („time to key agreement) measured
  - from first message of last node
  - to final SAK Use of client
- wpa_supplicant showed some outliers (o)
- Lower and higher quartile indicated by box
- Median indicated by orange bar



Öffentlich C-SC0
2025 Ethernet & IP @ Automotive Technology Day
© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Timing Evaluation
Raspberry Pi Demonstrator: Observations



Hypothesis: time to key agreement differs, depending on the starting offset.

Öffentlich C-SC0

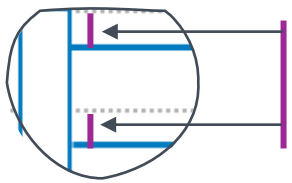
© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Timing Evaluation

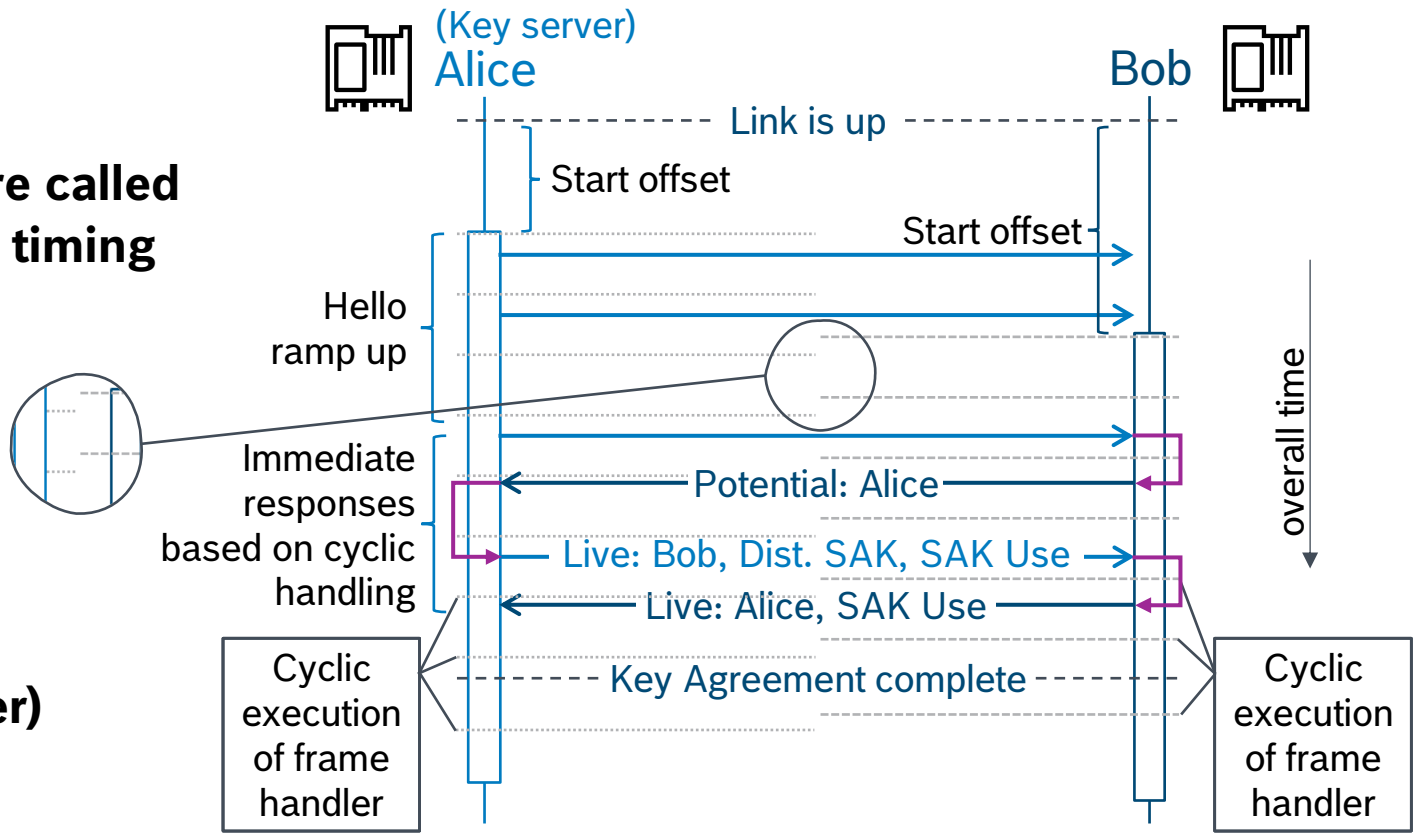
Expected key agreement time differences with Autosar SW Arch

Message handlers are called cyclically w/ specific timing

Execution points in time differ between multiple nodes



Processing time of messages differ (jitter)



Cyclic processing of messages in Autosar

Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Simulation
MKA Plugin Parameters

PEGaSE

- Frame processing time: ~1ms
- Key Install Delay: ~400µs
- Start Offset: 0 to 100ms
- Sample Size: 1000 runs

Network Size
2 Nodes
(hop-to-hop configuration of MACsec)

Message Processing Cycle
1ms to 10ms

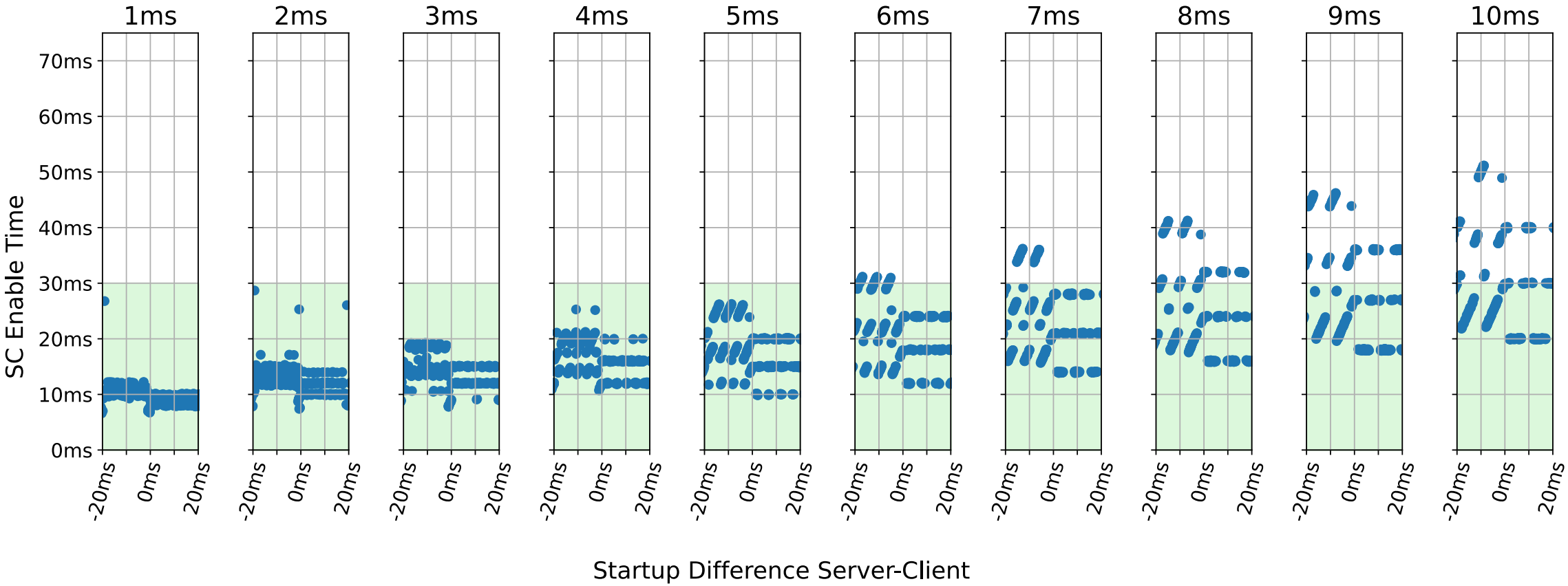
Hello Time Ramp Up Start Value
20ms

Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Simulation

Time until SC is enabled for different cycle time

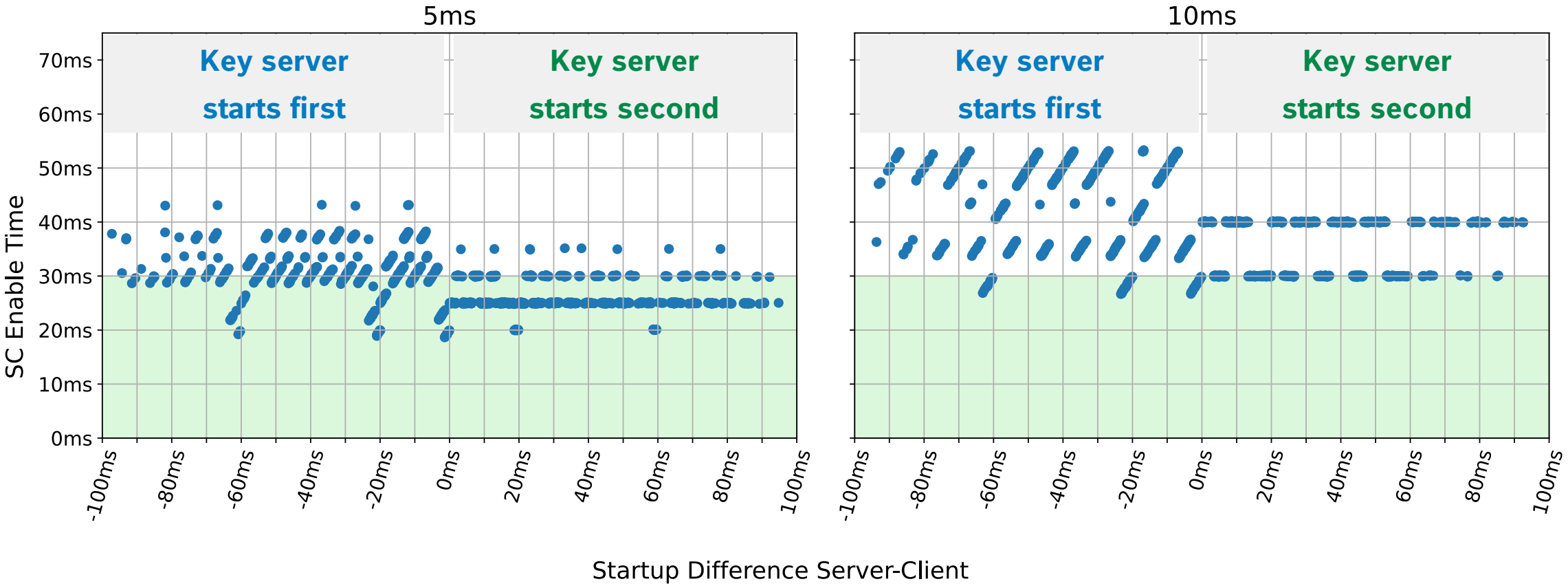


Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Simulation

Time until SC is enabled for 5ms and 10ms cycle time

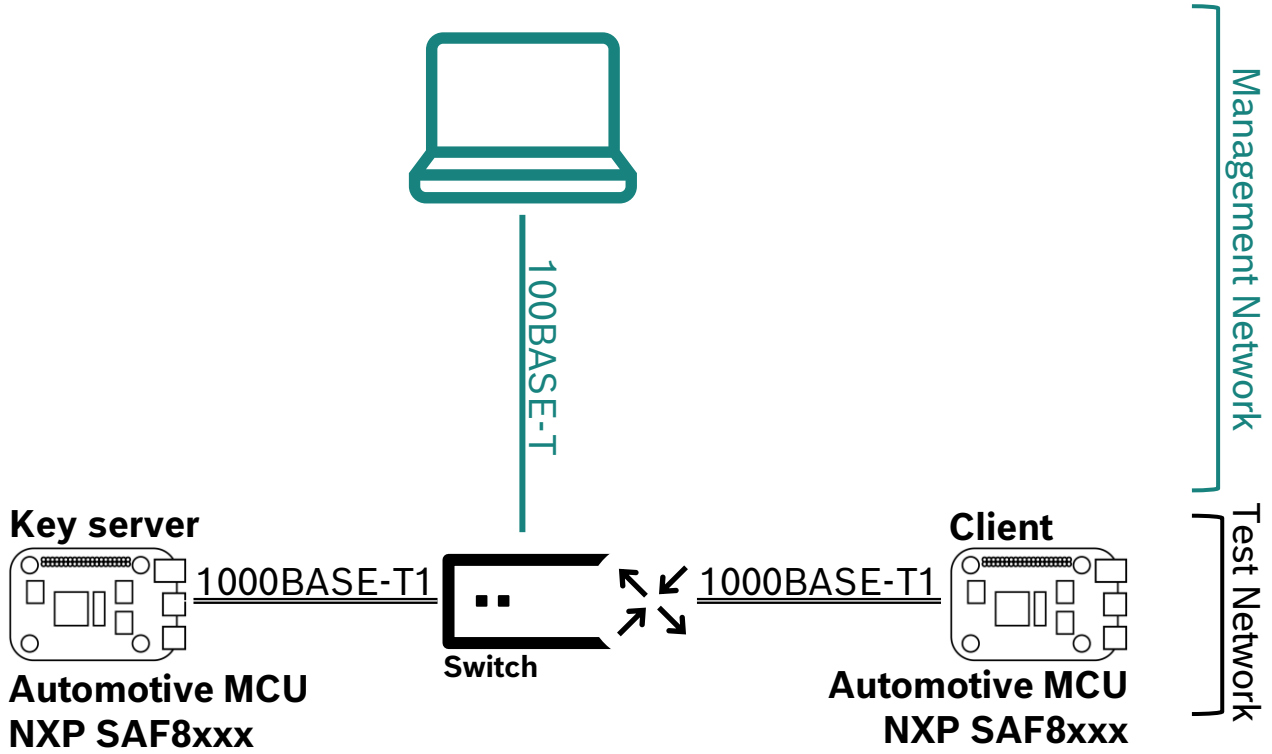


Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Experimental Setup
Test Environment

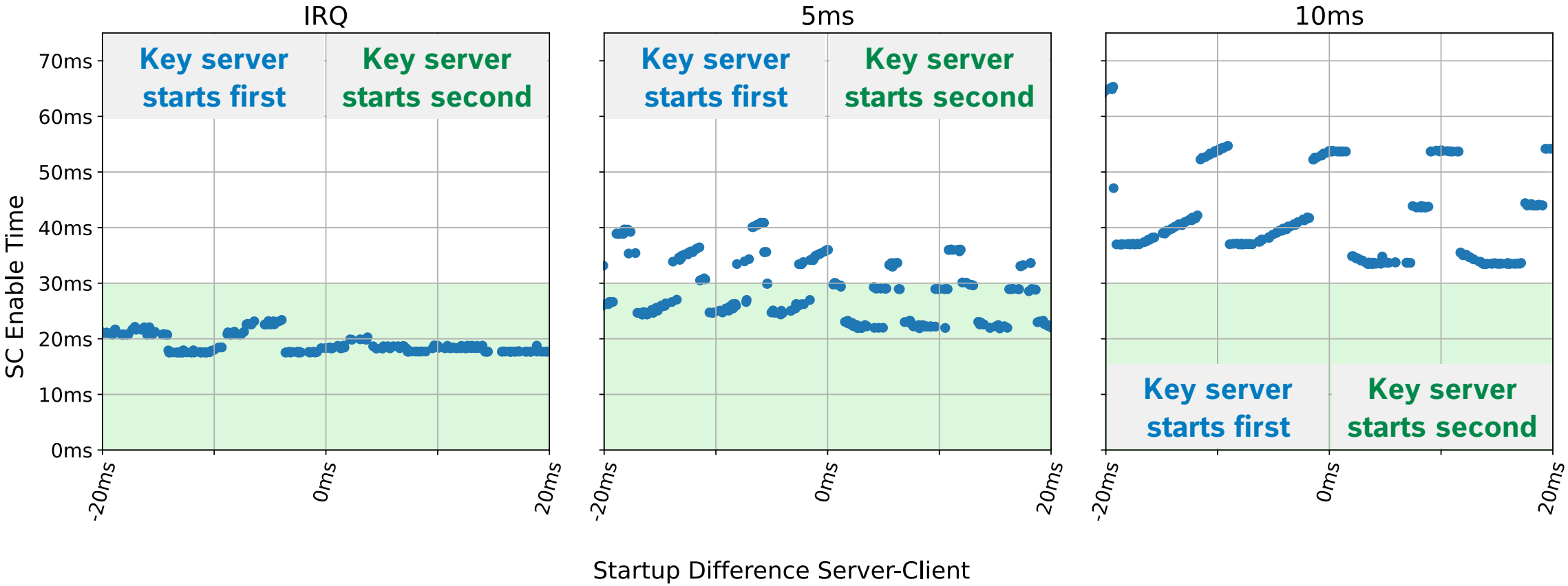
- Start: laptop sends sync frame w/ 2 offsets
- Stop: key server sends time of SC enablement
- SW: own impl. of MKA w/ TC17 profile and HSM support
- Cyclic message processing



Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

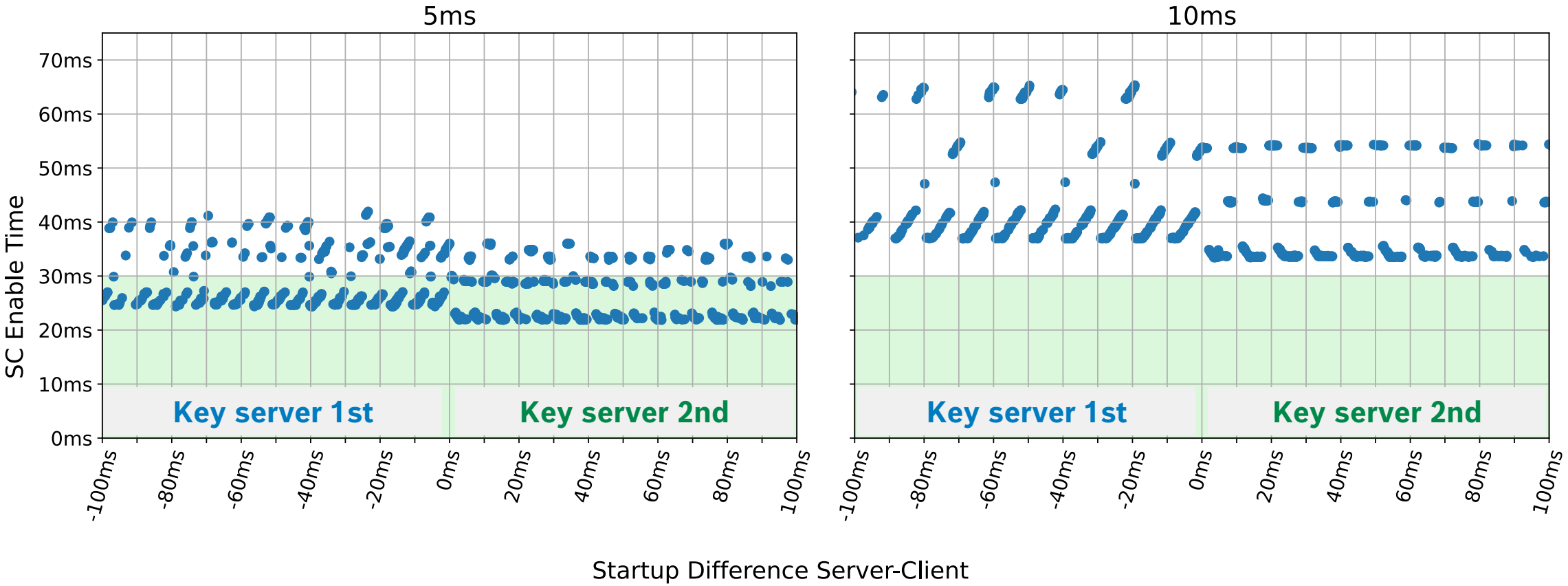
Experimental Setup
Overview



Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

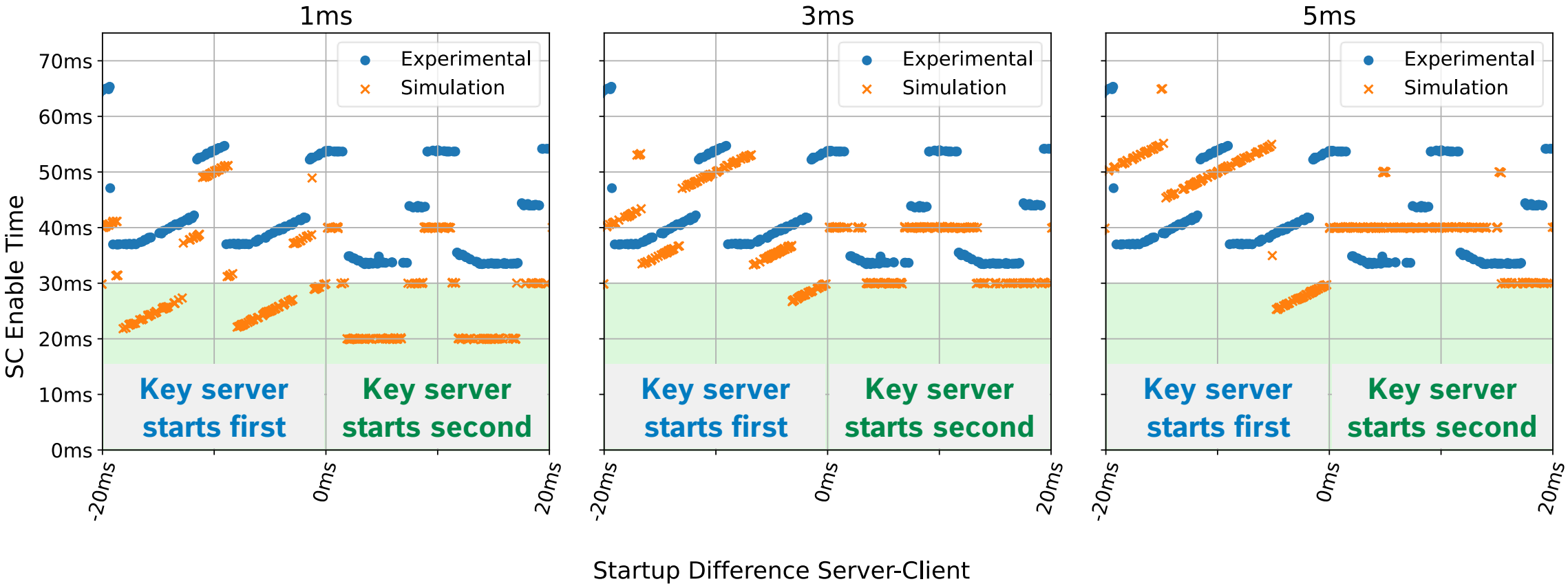
Experimental Setup
5ms and 10ms cycle



Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

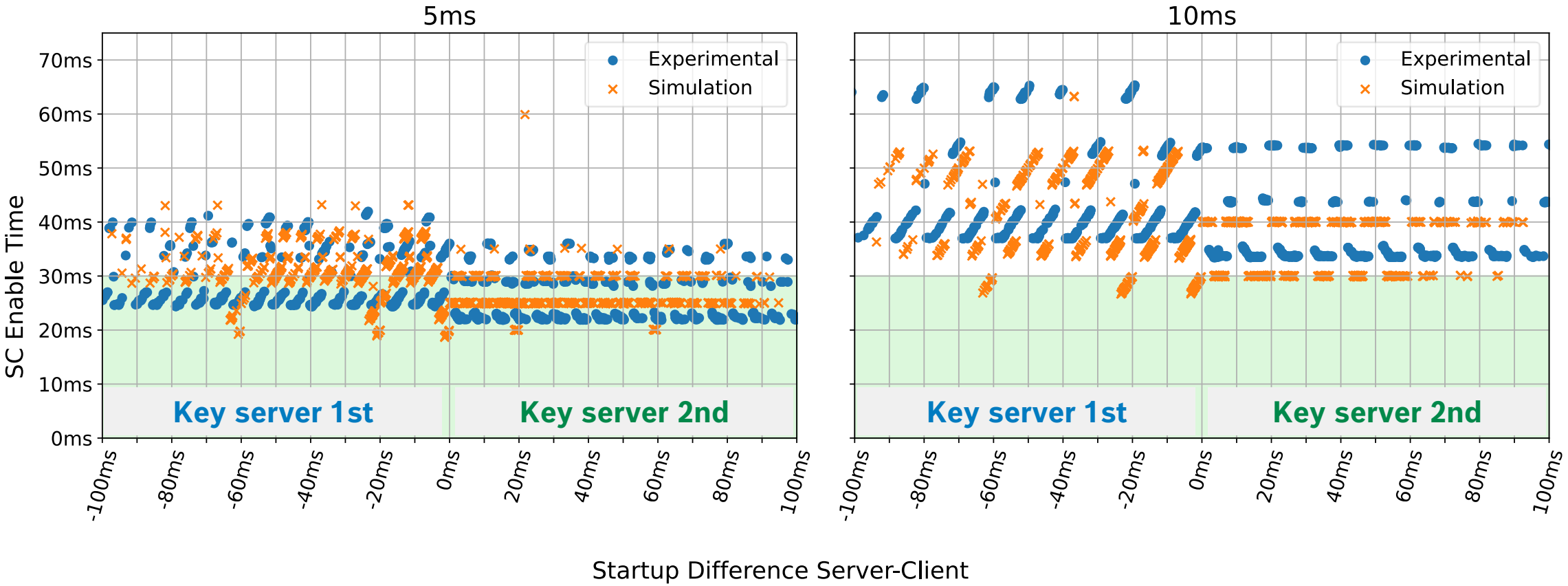
Comparison – Simulation vs Experimental
10ms Cycle, Differing Processing Time



Öffentlich C-SC0
2025 Ethernet & IP @ Automotive Technology Day
© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Comparison – Simulation vs Experimental

3ms Processing Time

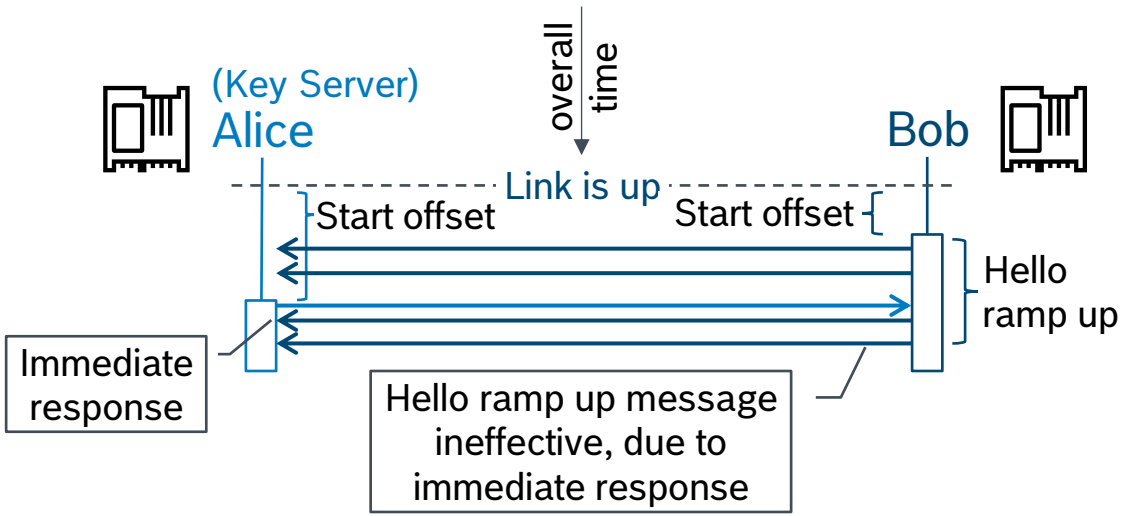


Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Summary
Conclusion

- Reaching 30ms in general difficult to achieve
- Fastest key agreement time happens, when key server starts late
  - Unintuitively
- Hello time does not matter in default cases
- Small variance in start up offset can significantly influence time to key agreement
- Cycle times need to be very small or IRQ-based
  - >5ms not reliably fast enough
- Processing time important as well



Should we look into no-rekeying solutions from 10BASE-T1S for switched Ethernet as well?

Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.

Thank you for your attention!
Questions?



“Secure, or not secure, that is the question”

—freely adapted from Hamlet

Öffentlich C-SC0

© Robert Bosch GmbH 2025. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.