OPTIMALLY CONNECTING SENSORS INTO THE EE-ARCHITECTURE

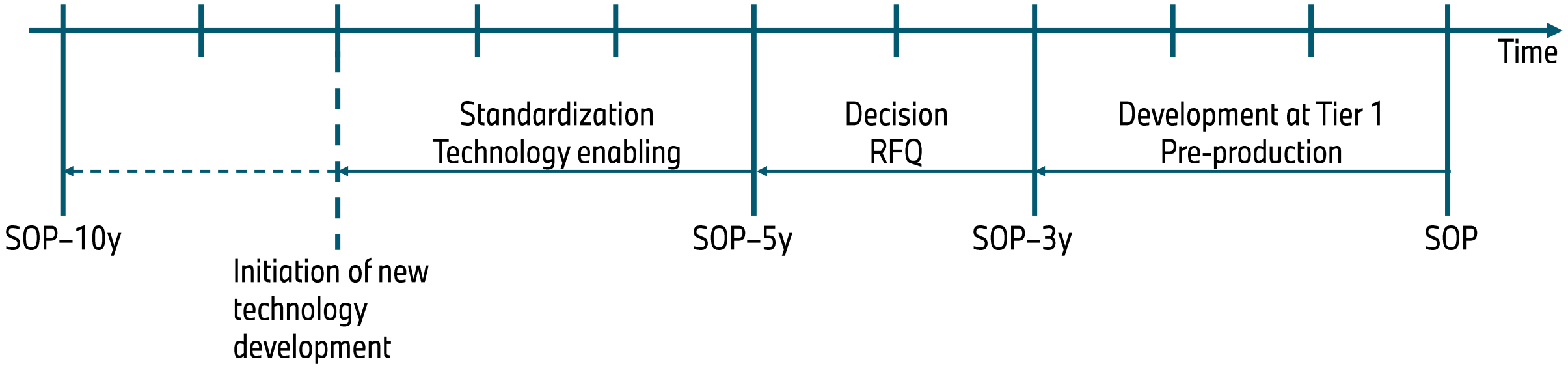
AUTOSENS, SEPTEMBER 13-14, 2022, BRUSSELS, BELGIUM

Dr. Kirsten Matheus, BMW

AGENDA

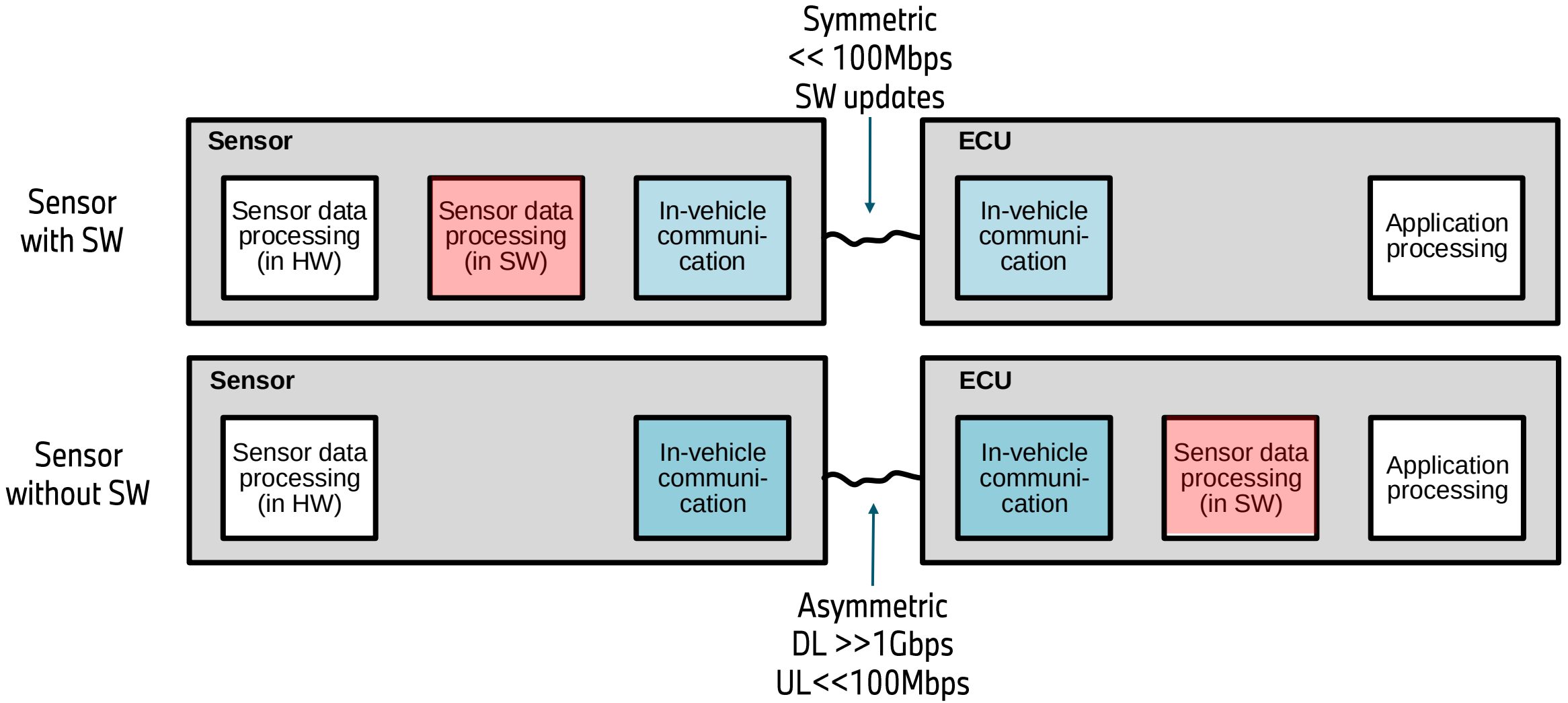
- Motivation
- Fundamental architectural decisions that impact the choice of communication technologies
  - Where to perform the processing of sensor data
  - How to integrate the sensor into the architecture
  - Link-based, protocol-based, or application-based security
- ASAML and IEEE 802.3ch
- Summary

THE DEVELOPMENT OF A NEW, STANDARDIZED IN-VEHICLE NETWORKING TECHNOLOGY HAS TO BE INITIATED 8-10 YEARS BEFORE INTENDED SOP.



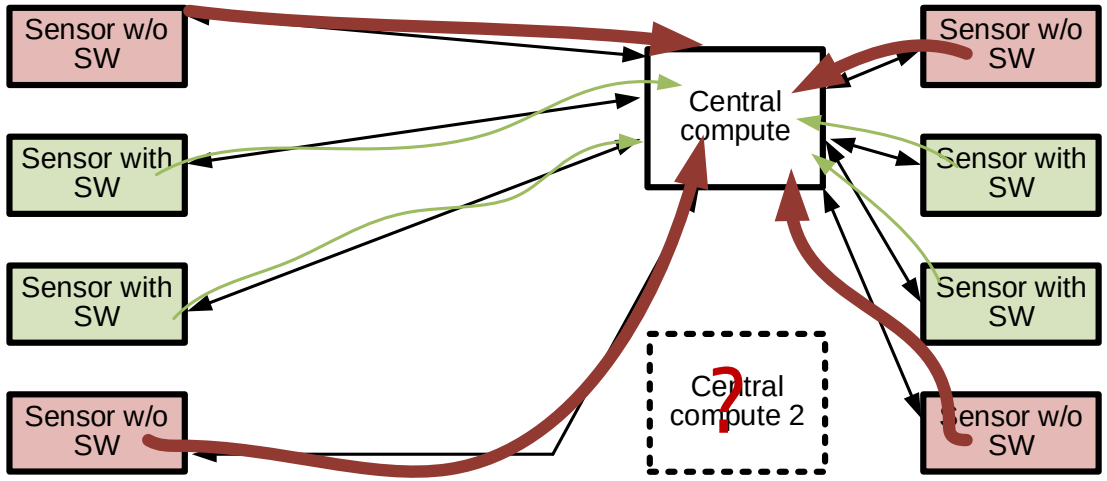
This early before SOP it is essential to enable options for important architectural decisions and not to unnecessarily restrict them.

ARCHITECTURAL OPTION 1:
LOCATION OF SOFTWARE (SW)-BASED SENSOR DATA PROCESSING.



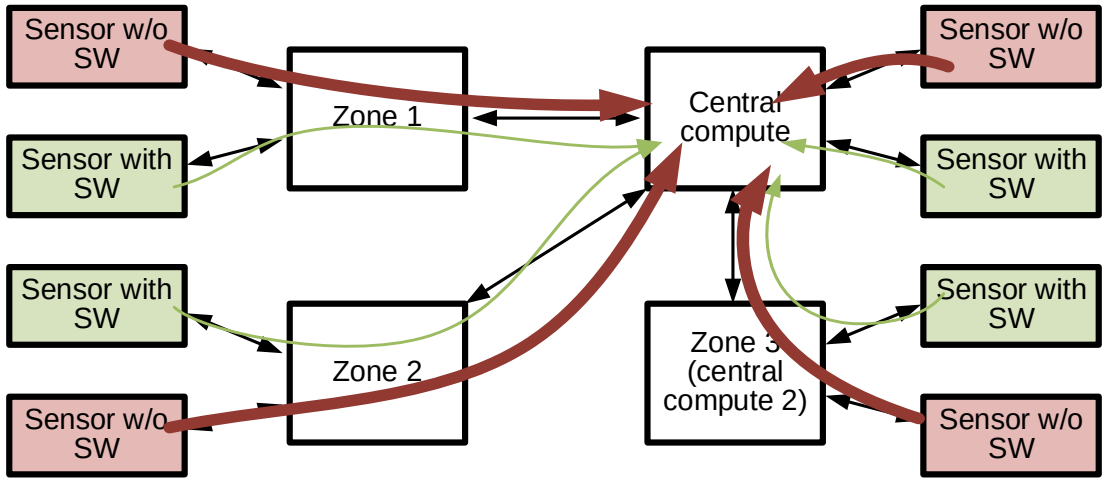
ARCHITECTURAL OPTION 2: PLACEMENT OF SENSORS IN EE-ARCHITECTURE.

P2P connections only



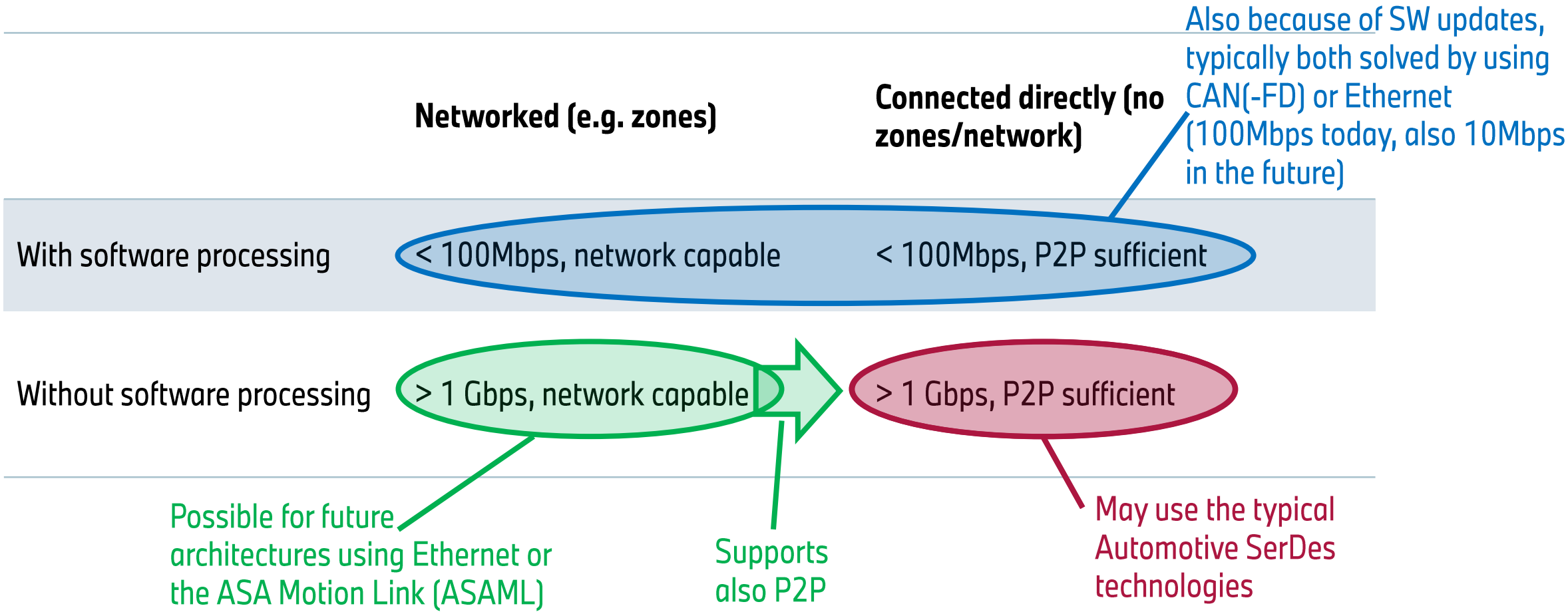
- P2P does not require addressing/networking in sensors
- Does not cause traffic in network
- Results in a large number of connectors at central ECU
- Destroys zonal approach (affects harness production)
- Multiprocessing requires additional solution (gateways?)

Integration in zones/network



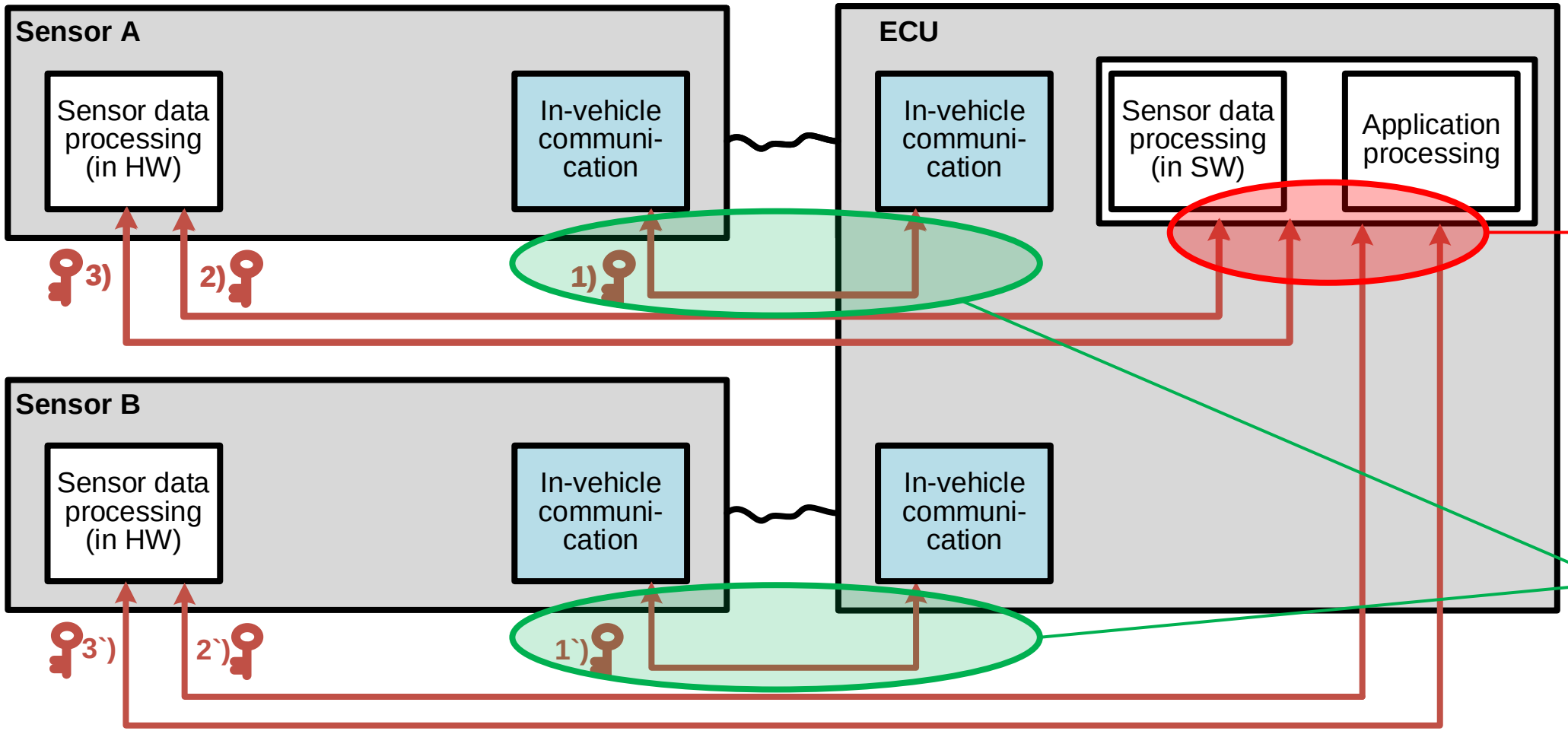
- Requires addressing/networking in sensors
- Sensors w/o SW load network with asymmetric traffic
- Optimized harness production/support of zones
- Inherently supports multiprocessing solutions

THE BASIC COMMUNICATION REQUIREMENTS DEPEND ON RESPECTIVE CHOICES. NETWORKED SOLUTIONS COVER P2P, BUT NOT THE OTHER WAY AROUND.



ARCHITECTURAL OPTION 3: LINK LAYER [1], PROTOCOL LAYER [2], OR APPLICATION LAYER [3] SECURITY. (1)

1. Link layer security offloads the processor in ECU

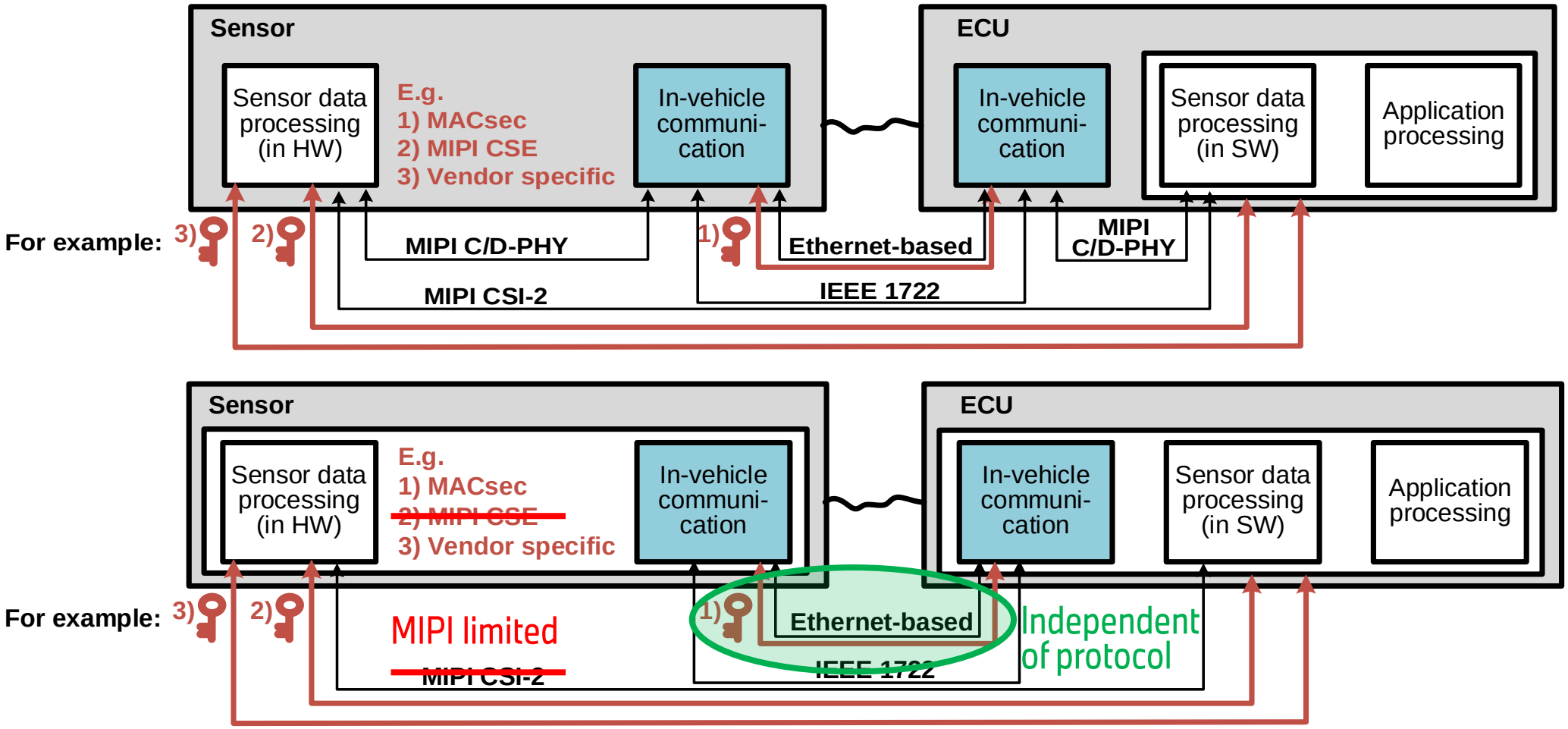


Might be a number of different protocol or application layer security mechanisms

Independent of use case, terminated in communication chip

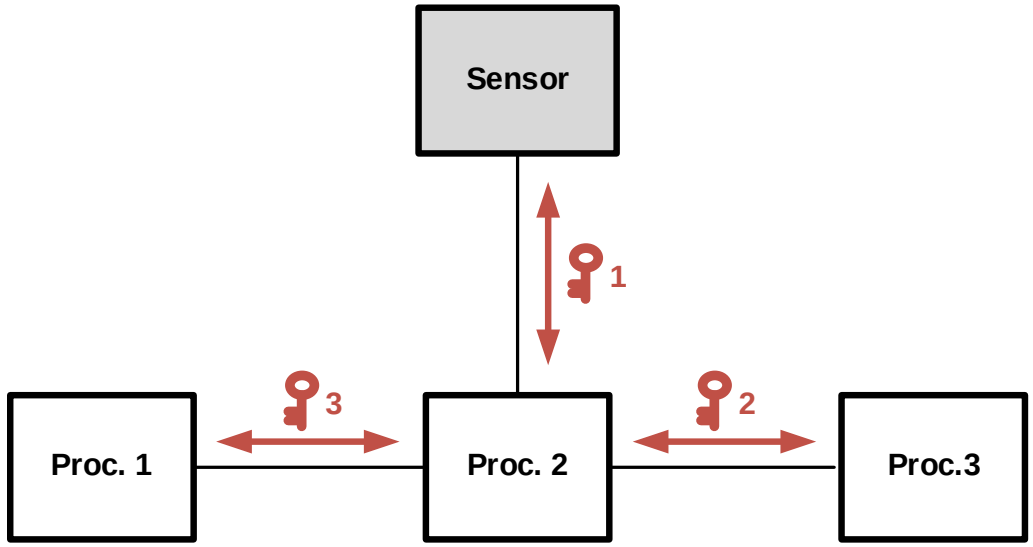
ARCHITECTURAL OPTION 3: LINK LAYER [1], PROTOCOL LAYER [2], OR APPLICATION LAYER [3] SECURITY. (1)

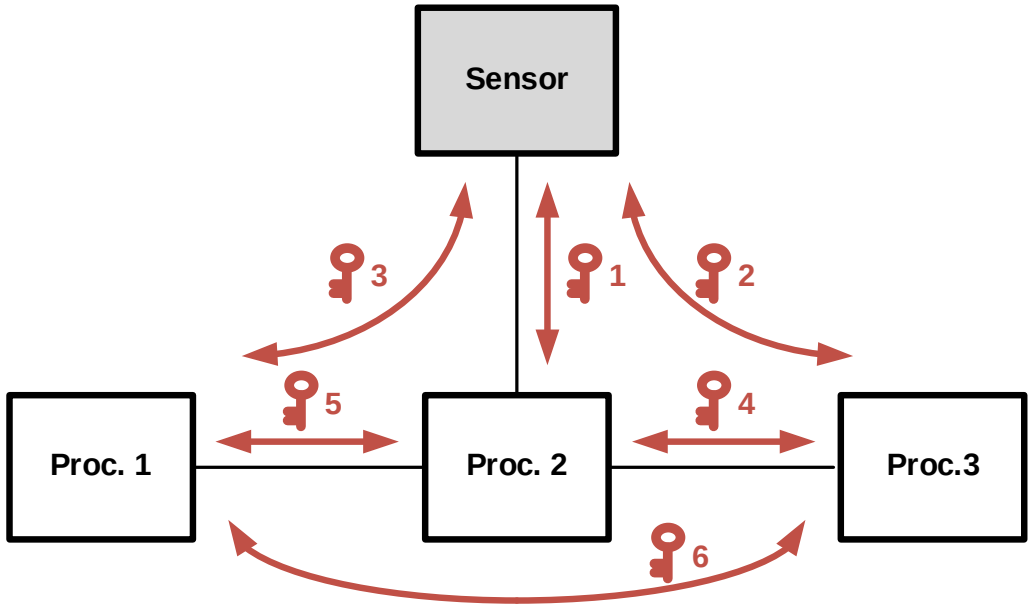
2. Link layer security avoids protocol usage dependencies



ARCHITECTURAL OPTION 3: LINK LAYER [1], PROTOCOL LAYER [2], OR APPLICATION LAYER [3] SECURITY. (1)

3. Link layer security reduces the number of en/decryption relationships





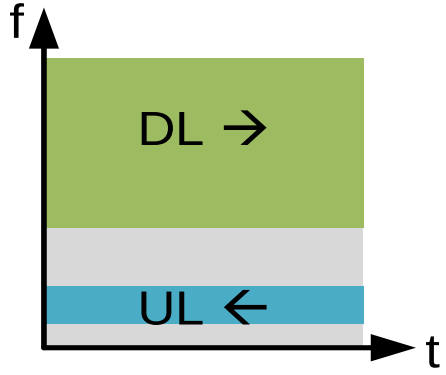
BOTH, MGBASE-T1 ETHERNET AND THE ASA MOTION LINK CAN BE USED FOR "SERDES" AS WELL AS A NETWORKING TECHNOLOGY.

	Ethernet IEEE 802.3ch	ASAML (ASA Motion Link)
Standardized at	IEEE 802.3	Automotive SerDes Alliance (ASA)
Companies participating	Automotive players very similar to ASA	Automotive players very similar to IEEE (>100)
User data rate	2.5, 5, 10 Gbps, symmetric (DL=UL)	1.86, 3.73, 6.7, 10.1, 13.4 (2.5, 5, 10) Gbps DL, 30, 100 Mbps UL, asymmetric/symmetric
Integrates into Ethernet network	Original purpose	Respective product definition always possible but optimized with v 2.0
May be used as SerDes-bridge	Matter of product definition	Original purpose
Link-based security	MACsec	ASAsec (based on MACsec plus key exchange)
Power saving	EEE	Light sleep mode

Power and effort optimized for asymmetric high-speed communication

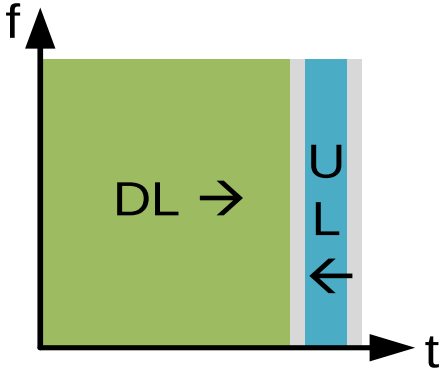
USING TDD SCHEME OPTIMIZES THE PMA/PMD COMPLEXITY FOR SINGLE PAIR, ASYMMETRIC COMMUNICATION AS USED WITH THE ASAML.

FDD



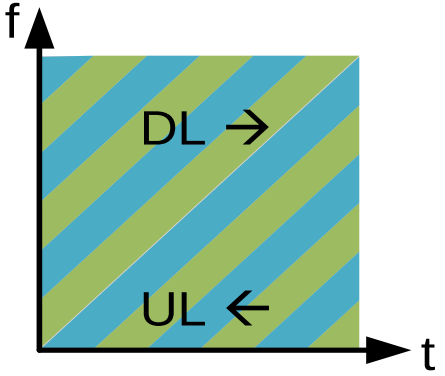
- Used in (proprietary) SerDes bridges inside cars today.
- Results in different IC at both ends of the communication.
- More symmetry only possible with added wires or added echo cancellation.
- Higher complexity for power-over.

TDD



- Used for ASAML.
- In principle, same IC at both ends of the communication.
- Symmetry can easily be achieved by changing timing.
- Attention needs to be paid to delay on UL.
- Efficient power-over.

Full-duplex



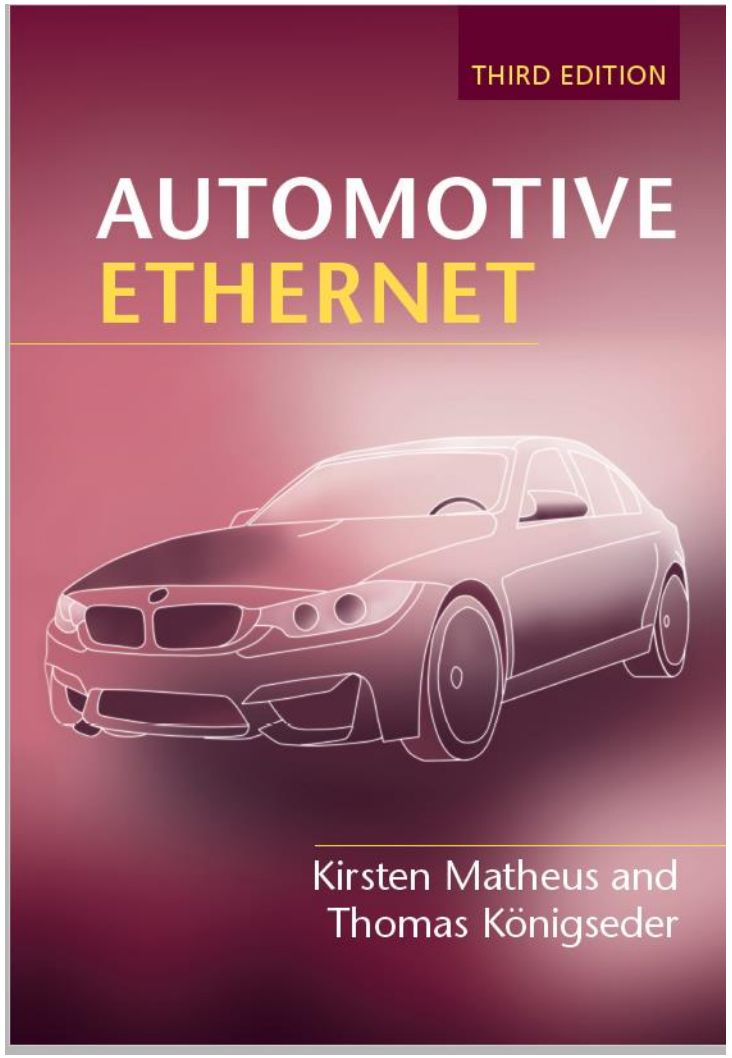
- Used for IEEE 802.3ch.
- Same IC at both ends (symmetric).
- Always requires echo cancellation and high resolution ADC/DAC.

SUMMARY AND CONCLUSION.

- The trend towards autonomous driving increases the number of sensors in cars and the importance to communicate with them safely and securely.
- The respective communication infrastructure needs to be initiated well ahead of time and should support all architectural options.
- The choice to integrate sensors directly and efficiently into the in-vehicle Ethernet network can only be fulfilled by technologies that support Ethernet communication.
- Ethernet-based communication can also be used P2P (however, P2P destroys the zonal approach).
- Link-based security is preferred over protocol or application based security, as it offloads the application processor and makes security independent of any protocols or application used. If needed, protocol or application-based security may be used additionally.
- Both, IEEE 802.ch and the ASAML fulfill the requirements for asymmetric and networked high-speed communication, with the ASAML being very competitive in terms of complexity due to the used TDD scheme.

THANK YOU FOR YOUR ATTENTION

FOR MORE DETAILS ON AUTOMOTIVE ETHERNET SEE ALSO:

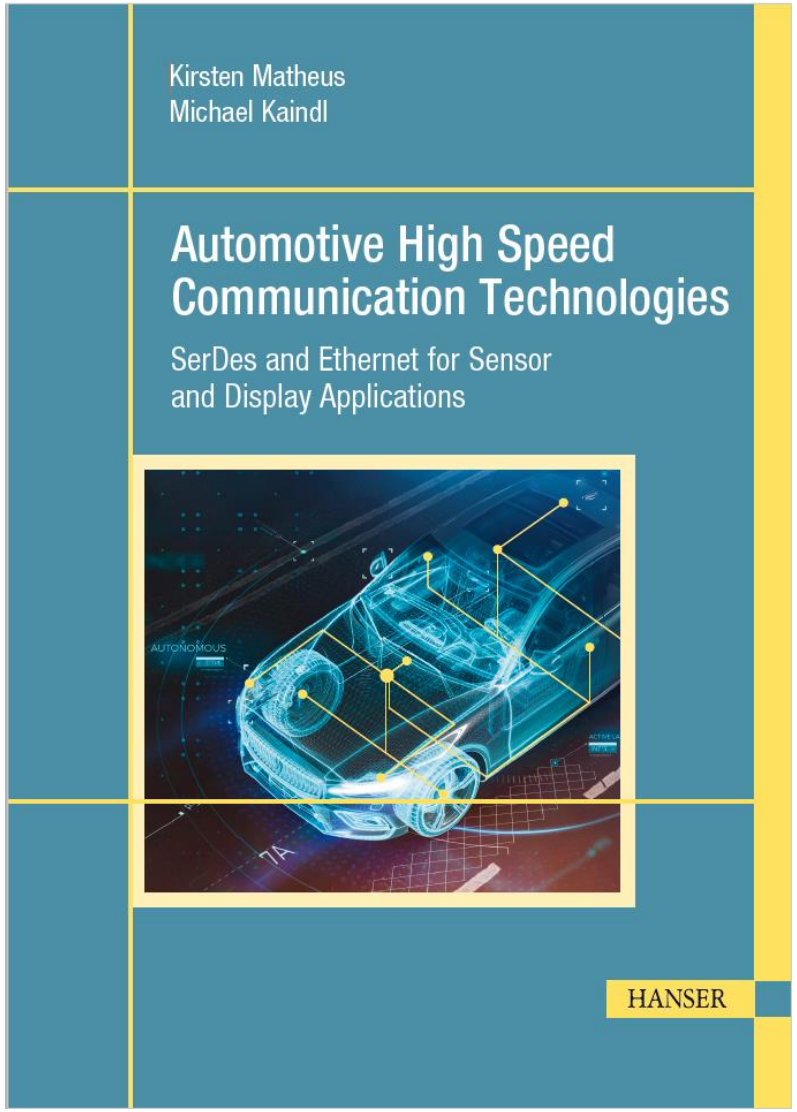


Added third edition content includes:

- Detailed explanations of how the 10BASE-T1 PHY technology works including the new multidrop mode.
- Detailed explanation of how the MultiGBASE-T1 PHY technologies work.
- Extended information on the new TSN standards.
- A layer by layer description for security in Automotive Ethernet.
- Lessons learned with Automotive Ethernet.
- Updated content throughout the complete book.

- Start of sale: April 2021

FOR MORE DETAILS ON AUTOMOTIVE SENSOR AND DISPLAY COMMUNICATION SEE:



Comprises the following Chapters:

1. Introduction and Background
2. The Automotive Use Cases (Displays, Cameras, other Sensors)
3. The Automotive Environment
4. The Electromagnetic Environment in Cars
5. The Automotive Communication Channel
6. Power
7. Automotive SerDes Technologies
8. High Speed Automotive Ethernet
9. Related Standards and Protocols
10. Test and Qualification

- Start of sale: Autumn 2022

FOR MORE INFORMATION ON THE AUTOMOTIVE SERDES ALLIANCE SEE: AUTO-SERDES.ORG

Founded in May 2019, to standardize Automotive SerDes. 100+ members in September 2022.

Main features of ASAML V 1.01 (Dec. 2020)

- User data rates >1.8, 3.6, 6.4, 9.7, 13Gbps
- One backwards compatible technology
- Light/deep sleep modes, effective power over
- Advanced diagnostics, time synch
- Encapsulates video, I2C, Ethernet
- 2-level security as integral part of the technology

Main features of ASAML V 1.1 (tbc. in 2022)

- User data rates >52Gbps (link aggregation)
- Encapsulates I2S, eDP, HDMI, SPI

Main features of ASAML V 2.0 (tbc. early 2023)

- Optimized Ethernet DLL