IN-VEHICLE NETWORK SECURITY – MACSEC, THE GAME CHANGER.

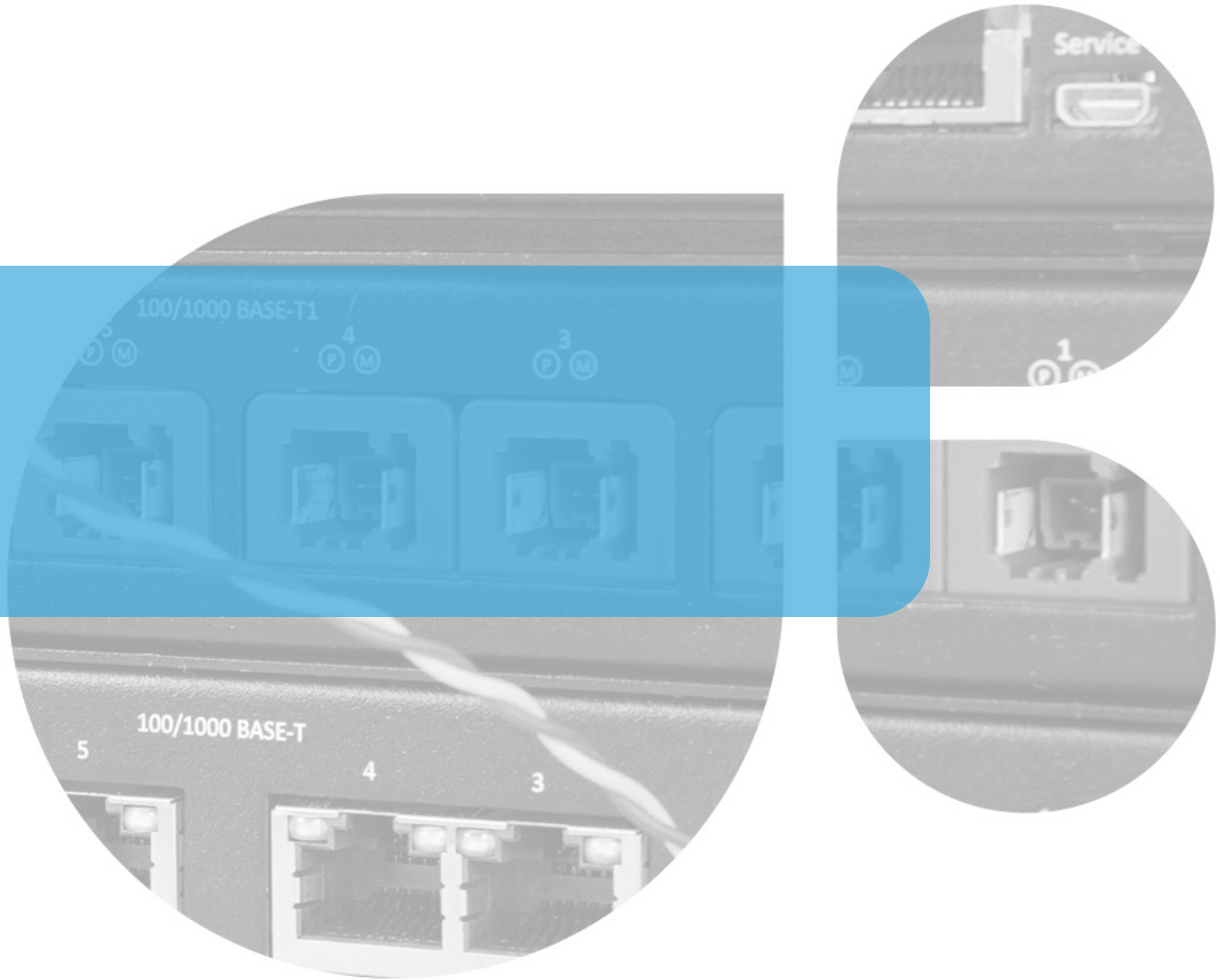
Dr. Lars Völker, Thomas Königseder | Technica Engineering GmbH

2022-11-15/16

MACSEC, THE GAME CHANGER.

TABLE OF CONTENT

#1 Motivation and Trends
#2 What do these Trends mean?
#3 What is MACsec?
#4 Interoperability
#5 Conclusion



MACSEC, THE GAME CHANGER.

#1 | MOTIVATION

MOTIVATION

SELECTED TRENDS IN VEHICLES

Trend: Software Defined Vehicle (SDV).

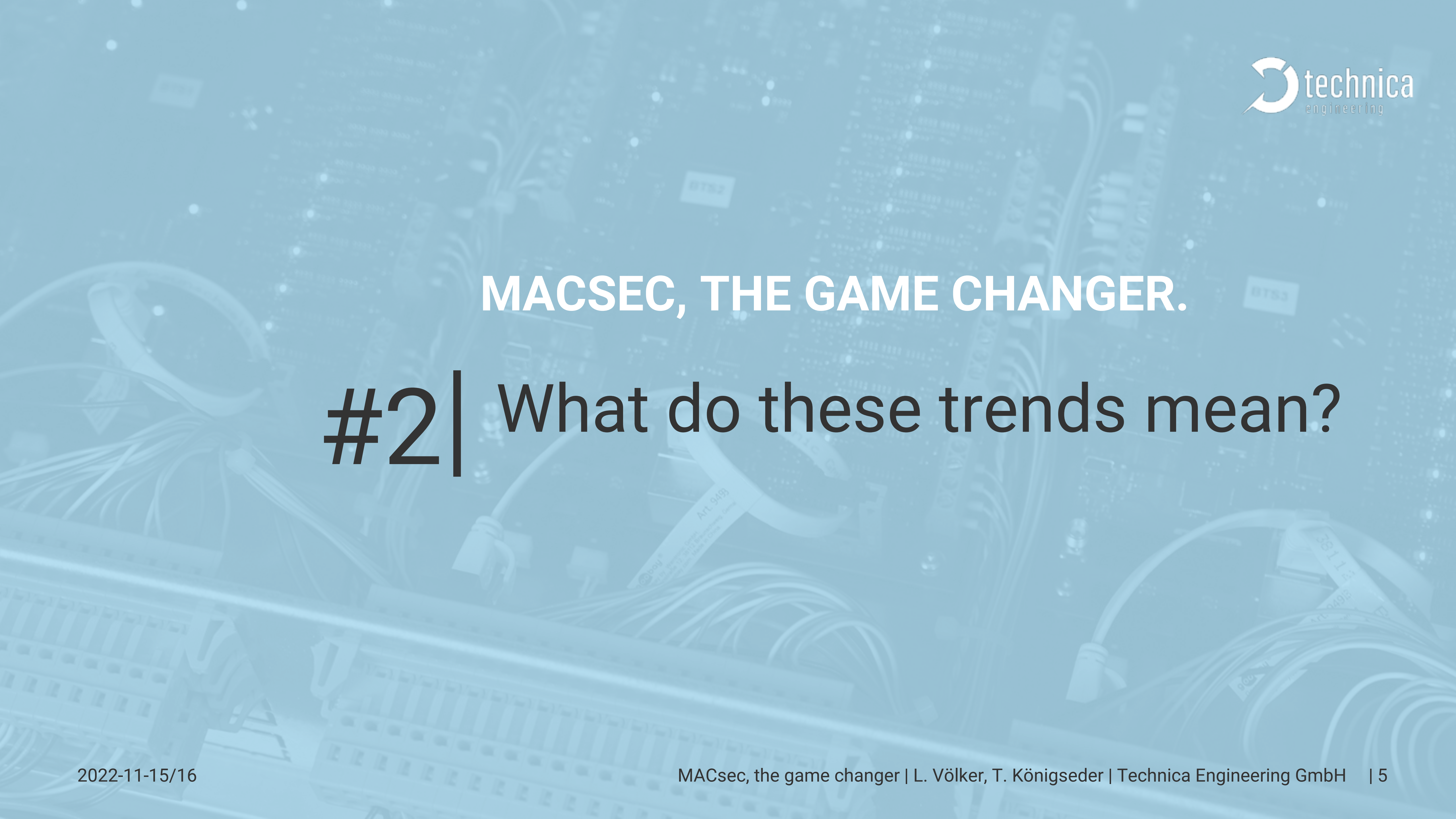
- Innovation mainly by software.
- Keeping products fresh by software update (“over the air”).

Trend: More data and data transmission.

- Entertainment, Internet, Apps, Audio/Video.
- Advanced Driver Assistance, Autonomous Driving.

Trend: Security is not optional but essential.

- Attacks becoming more common.
- Regulations concerning Security.

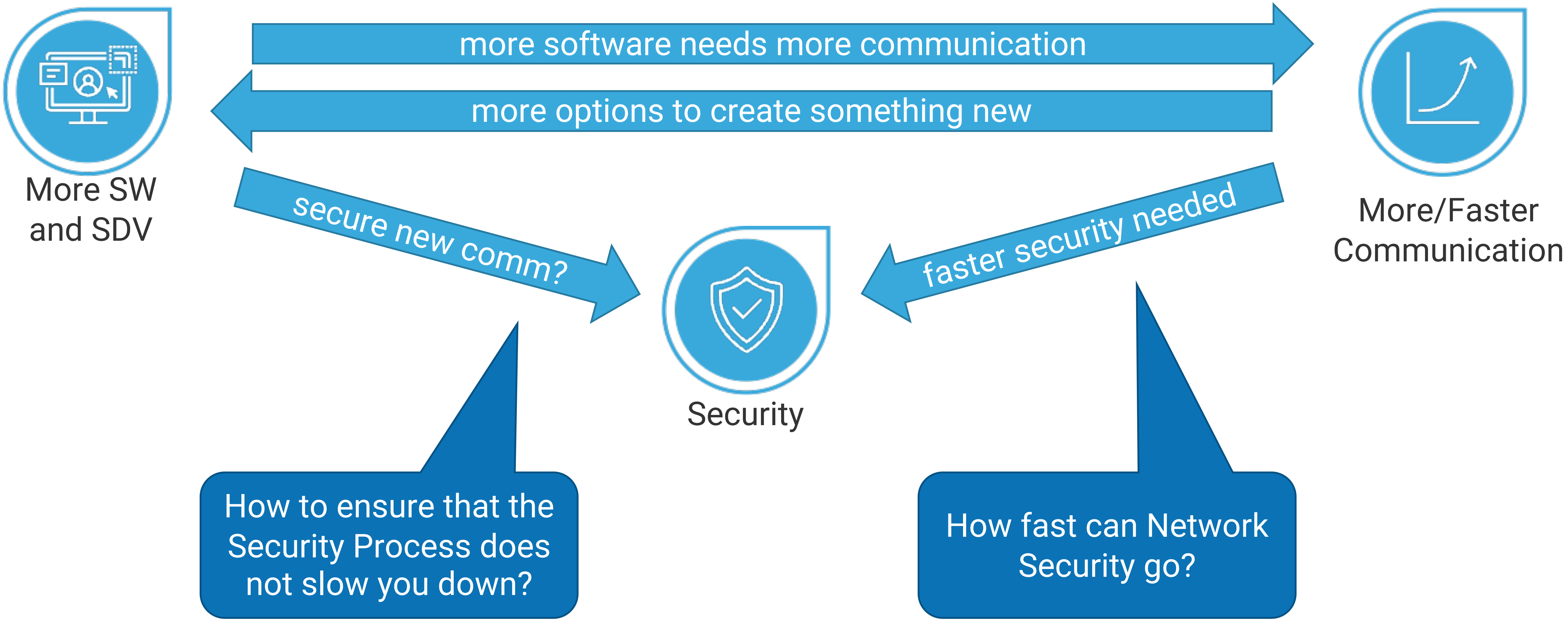


MACSEC, THE GAME CHANGER.

#2| What do these trends mean?

WHAT DO THESE TRENDS MEAN?

INTERACTIONS


more software needs more communication
more options to create something new
More SW and SDV
More/Faster Communication
secure new comm?
faster security needed
Security
How to ensure that the Security Process does not slow you down?
How fast can Network Security go?

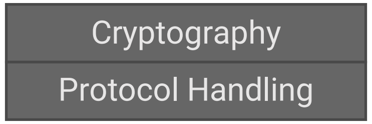
WHAT DO THESE TRENDS MEAN?

FASTER SECURITY NEEDED…

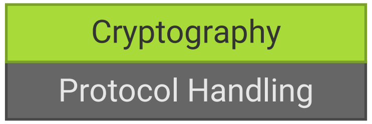
How fast can Network Security go?

Not all Security solutions scale the same…

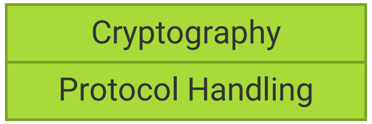
- 1st gen Network Security: “software-based”:
  - Easy to integrate but only good for slow speed (~ 1..10 Mbit/s).
  - E.g., Proprietary solutions, first gen SecOC.


Cryptography
Protocol Handling

- 2nd gen Network Security: “hardware accelerated crypto”:
  - Expensive crypto operation are offloaded to accelerator (~ 1..100 Mbit/s).
  - E.g., IPsec, (D)TLS, and SecOC.


Cryptography
Protocol Handling

- 3rd gen Network Security: “Full offload of data path”:
  - Hardware support allows for up to 10 Gbit/s and higher.
  - Impact on compute resources minimal.
  - E.g., MACsec.


Cryptography
Protocol Handling

WHAT DO THESE TRENDS MEAN?

SECURITY PROCESS TOO SLOW?

How to ensure that the Security Process does not slow you down?

Traditional approach “tailored security” is slow:

1. Design feature and its communication.
2. Run Threat Analysis and create Security Concept.
3. Add or adapt (security) mechanisms.

Better approach “security frontloading”:

- Create strong security platform for SDV that allows to add later.
- Security Analysis validates whether “present security is adequate”.

Which security solutions supports frontloading?

WHAT DO THESE TRENDS MEAN?

FRONTLOADING NETWORK SECURITY?

How to ensure that the Security Process does not slow you down?

	Startup Delay	Processing Overhead CPU
SecOC	(depends)	Per message/PDU
TLS/DTLS	Per Connection	Per packet
IPsec	Per Peer	Per packet
MACsec	Per Ethernet port	None

- MACsec is best for frontloading (due to superior hardware offloading):
  - Startup Delay stays constant, when adding more traffic streams (even to new peers).
  - CPU impact stays constant, when incrementing amount of traffic.
  - Can reach full Ethernet line-speed.

- Use MACsec for Software Defined Vehicles.

MACSEC, THE GAME CHANGER.

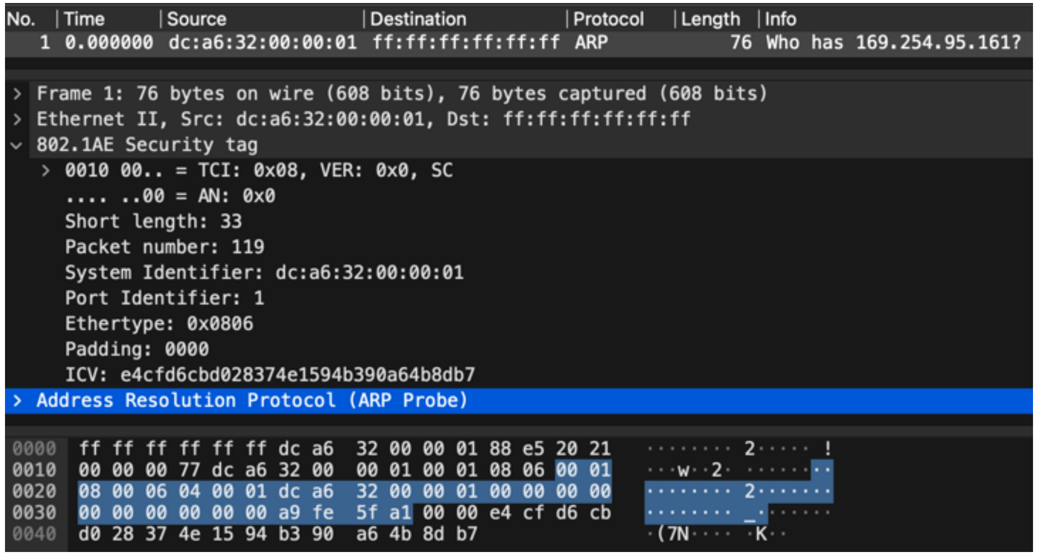
#3 | What is MACsec?

WHAT IS MACSEC?

OVERVIEW

IEEE Standard MACsec.

- “Authentication only” or “Encryption + Authentication”.
- Hop-by-hop mode supported for link-based protection.
- Security Tag including Integrity Check Value (ICV).
- Based on Secure Association Key (SAK).
- Typically: GCM-AES-128 or GCM-AES-256.
- Optional: Extended Packet Number (XPN).



```
No.  |Time      |Source           |Destination       |Protocol |Length |Info
   1 0.000000  dc:a6:32:00:00:01  ff:ff:ff:ff:ff:ff  ARP            76  Who has 169.254.95.161?

> Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Ethernet II, Src: dc:a6:32:00:00:01, Dst: ff:ff:ff:ff:ff:ff
v 802.1AE Security tag
  > 0010 00.. = TCI: 0x08, VER: 0x0, SC
    .... ..00 = AN: 0x0
    Short length: 33
    Packet number: 119
    System Identifier: dc:a6:32:00:00:01
    Port Identifier: 1
    Ethertype: 0x0806
    Padding: 0000
    ICV: e4cfd6cbd028374e1594b390a64b8db7
> Address Resolution Protocol (ARP Probe)

0000  ff ff ff ff ff ff dc a6  32 00 00 01 88 e5 20 21   ········ 2····· !
0010  00 00 00 77 dc a6 32 00  00 01 00 01 08 06 00 01   ···w··2· ········
0020  08 00 06 04 00 01 dc a6  32 00 00 01 00 00 00 00   ········ 2·······
0030  00 00 00 00 00 00 a9 fe  5f a1 00 00 e4 cf d6 cb   ········ _·······
0040  d0 28 37 4e 15 94 b3 90  a6 4b 8d b7               ·(7N···· ·K··
```

But where to get the SAK from?

WHAT IS MACSEC?

KEY EXCHANGE

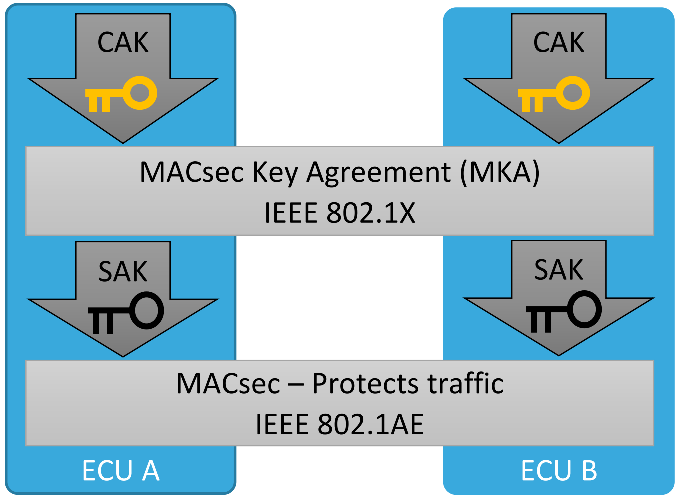
MACsec Key Agreement (MKA).

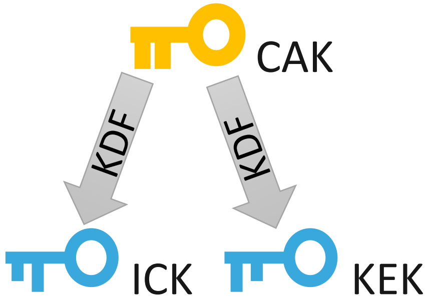
- MKA allows to generate fresh SAKs for MACsec:
  a) based on pre-shared Connectivity Association Key (CAK).
  b) based on EAP generated CAK (e.g., based on EAP-TLS).
- Key Server is elected, and Key Server distributes encrypted SAK.

MKA generates additional keys out of CAK:

- ICV Key (ICK): MKA message integrity protection.
- Key Encryption Key (KEK): encryption of keys in MKA messages.

Recommendation: Use pre-shared CAKs for fastest startup.





CAK: Connectivity Association Key (symmetric long-term secret)

SAK: Secure Association Key (symmetric session key)

WHAT IS MACSEC?

AUTOMOTIVE MACSEC

How to adapt MACsec for vehicles?

- Improved startup from 3-6s to 14ms and faster. See [1], [4]. ☑
- Integration into ECU architectures understood. See [2]. ☑
- Complementary technologies identified. See [2], [3]. ☑
- Automotive semiconductor availability. See various press releases. ☑
- ECO System ready. First tools for development and testing ready. ☑
- AUTOSAR standard. Finalization for next release done. ☑
- Interoperability?

[1] Dr. L. Völker: "**Starting up MACsec for Automotive Ethernet**", Jun. 2021 / 7th International VDI Conference - Cyber Security for Vehicles.
[2] Dr. O. Creighton (BMW), Dr. Lars Völker: "**Automotive MACsec Architecture**", Nov. 2021 / Ethernet & IP @ Automotive Technology Hybrid Event Week.
[3] Dr. L. Völker: "**MACsec und Automotive Security**", Apr. 2022 / CAST Automotive Security Workshop.
[4] Dr. L. Völker: "**Automotive MACsec (Demo)",** May 2022 / Technica Demo on YouTube.

MACSEC, THE GAME CHANGER.

#4| Interoperability

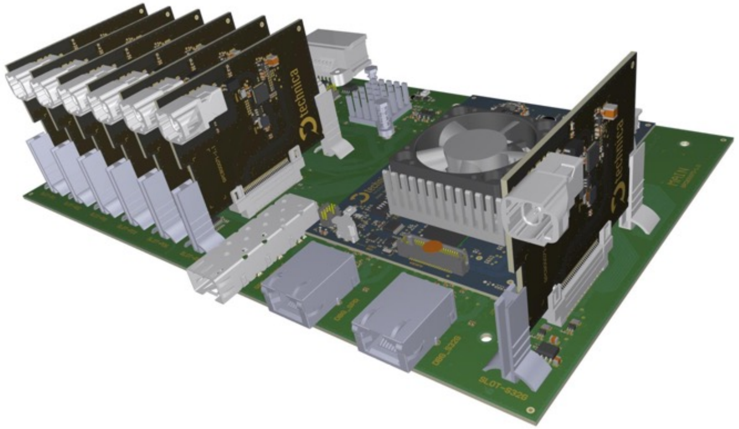
INTEROPERABILITY

OVERVIEW AND OUTLOOK

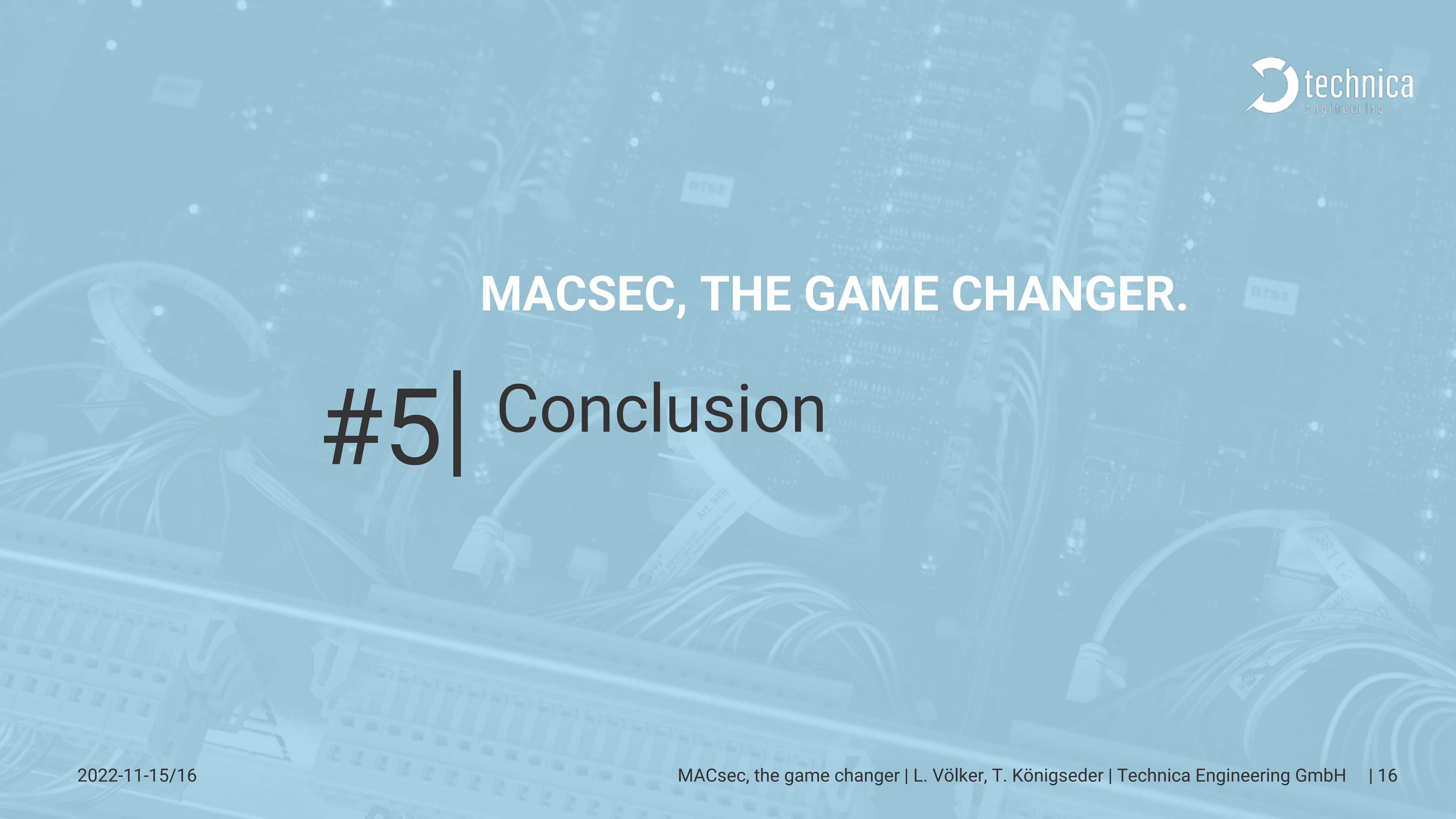
Interoperability is the key to a healthy eco system.

- MACsec interoperability needs to be tested:
  - We showed “interop” on the first two chips available 2021.
  - We are working with chip vendors and others on this topic.

- How to get MKA interoperability?
  - We have created a test suite for conformance.
  - Our MKA implementation is available as ”golden device”.



Technica MACsec Interop Platform



MACSEC, THE GAME CHANGER.

#5| Conclusion

MACSEC, THE GAME CHANGER

CONCLUSION

MACsec is the Game Changer for Network Security:

- MACsec is an open standard conceived by the IT industry.
- MACsec scales to 10 Gbit/s and beyond.
- Security Frontloading is essential for SDVs and MACsec enables this.
- MACsec leaves the expensive compute resources to applications.

MACsec is on the way:

- First OEM publicly stated SOP in 2025.
- Standards, Tools, Implementations, Interoperability in progress.

When will you bring MACsec to series production?

Technica Engineering GmbH

Leopoldstraße 236
80807 Munich, Germany

DR. LARS VÖLKER
Technical Fellow

lars.voelker@technica-engineering.de
+49 175 11 40 982