THE CHALLENGES IN THE DEVELOPMENT OF A COMPLETE ETHERNET VEHICLE.

DR. KIRSTEN MATHEUS

OCTOBER 9, 2018, LONDON

8TH ETHERNET & IP @ AUTOMOTIVE TECHNOLOGY DAY

BMW GROUP

THE NEXT 100 YEARS

OBSTACLES WHEN MOVING TOWARDS AN ALL ETHERNET IVN.

- Using Ethernet only as yet another IVN technology e.g. for addressing higher data rates. This just adds to gateways, tools & methodologies, i.e. it increases the effort for maintaining all technologies.
- Using Ethernet just to replace legacy networks 1:1 instead of designing the system differently. This makes it more costly than necessary (even with 10Mbps Ethernet) a) because it does not fully exploit the functionalities Ethernet allows for b) because trying to rebuild e.g. CAN over Ethernet requires additional overhead.*)
- Need for risk minimization and step by step introduction. This means more radical (but efficient) changes cannot be made immediately. Instead the legacy networks run in parallel with additional costs and effort.
- Changing the mindset of a whole industry. An All Ethernet IVN can impact the way we develop and build cars. This might not only change the IVN but also product life cycles and value chains.

*) BTW, gateways today often need to recreate the functionality of Ethernet switches

THANK YOU FOR YOUR ATTENTION

Dr. Kirsten Matheus

BMW GROUP THE NEXT 100 YEARS

EXPANDED SINGLE PAIR RATES: EVOLVING 802.3 STANDARDS

G. Zimmerman
CME Consulting

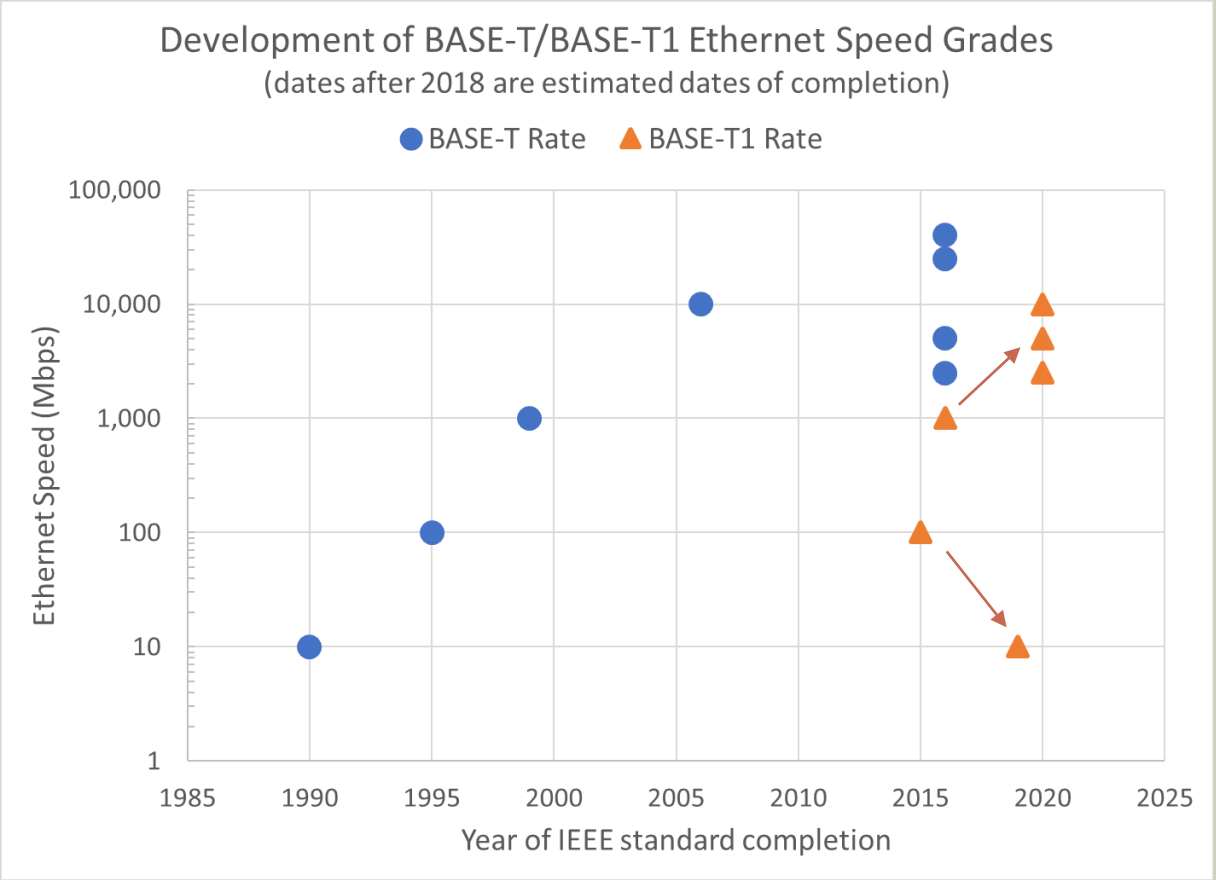
DISCLAIMERS

- Opinions expressed during this presentation are the views of the presenters, and should not be considered the views or positions of the Ethernet Alliance.

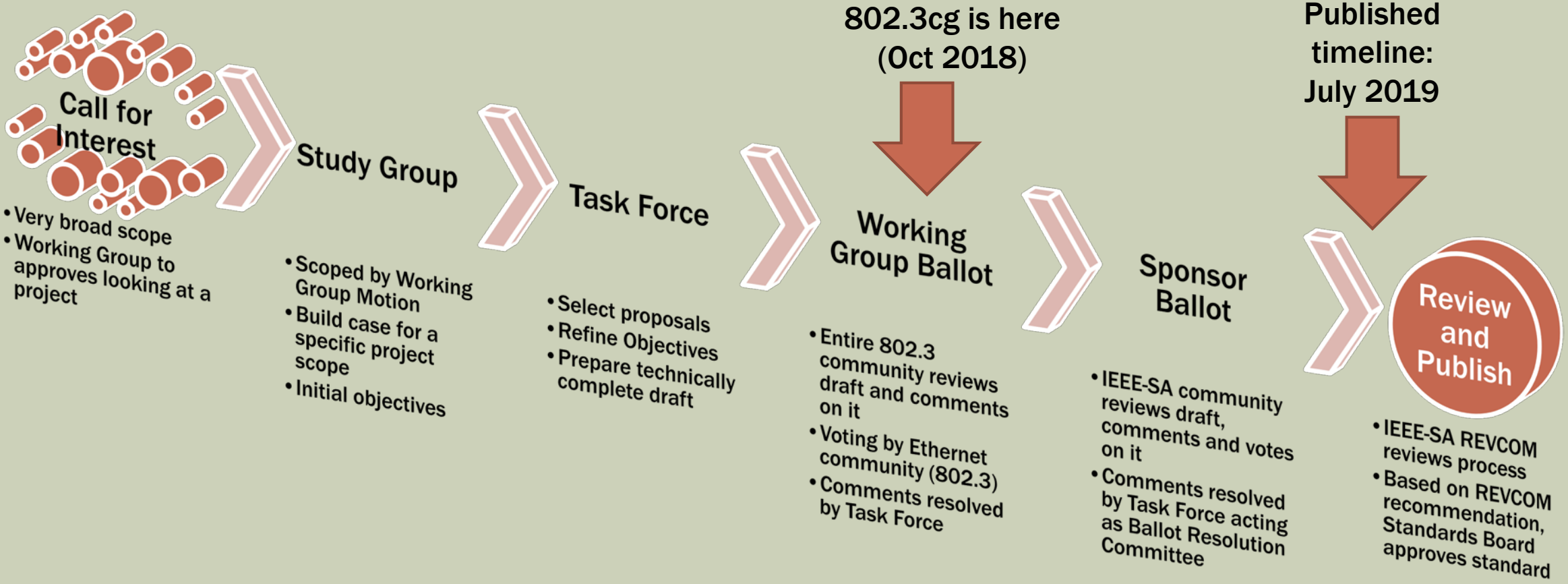
- Per IEEE-SA Standards Board Bylaws, Dec 2013
  - "At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE."

WHAT IS GOING ON WITH RATES?

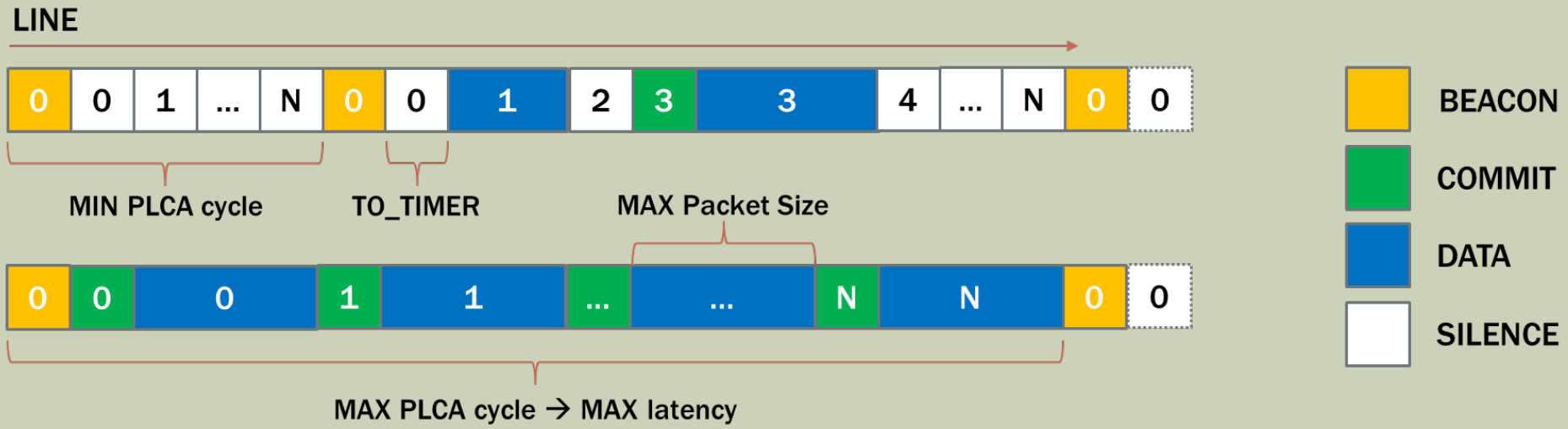
- 802.3cg – 10 Mbps Single Pair
  - Return to 10Mbps half-duplex
  - Point-to-point 15m operation
    - Optional full duplex
  - Return to CSMA/CD shared-medium networking (optional as half-duplex)
    - 25m, single twisted pair, no repeaters
    - Performance enhancments to avoid collisions on the medium (PLCA)
- 802.3ch – Multigig Single pair
  - Point-to-point, extension of rates beyond gigabit



IEEE 802.3 PROCESS IN BRIEF

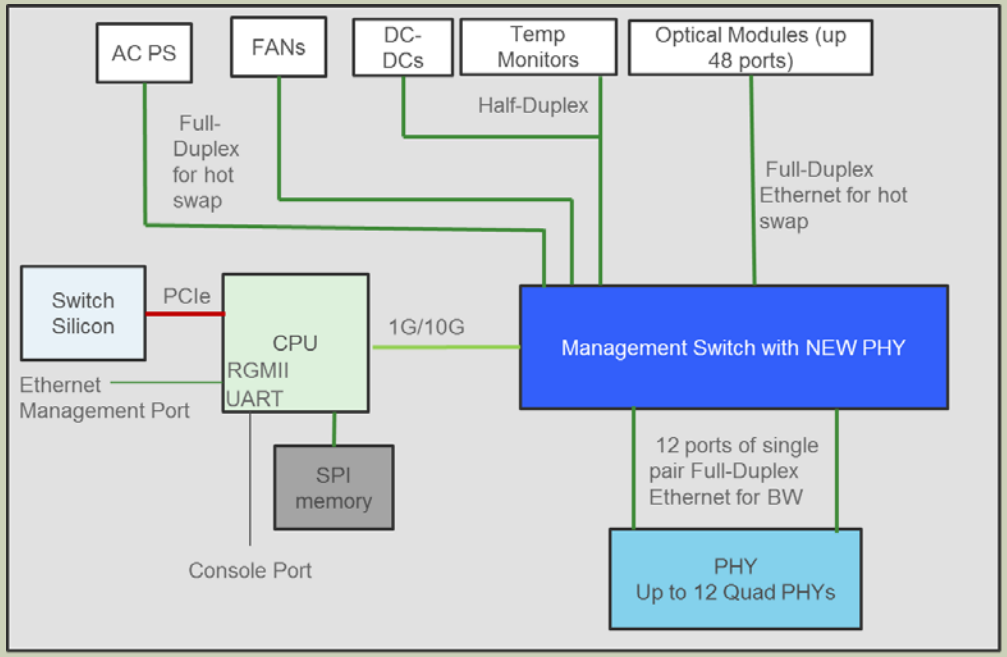


PLCA IN A NUTSHELL

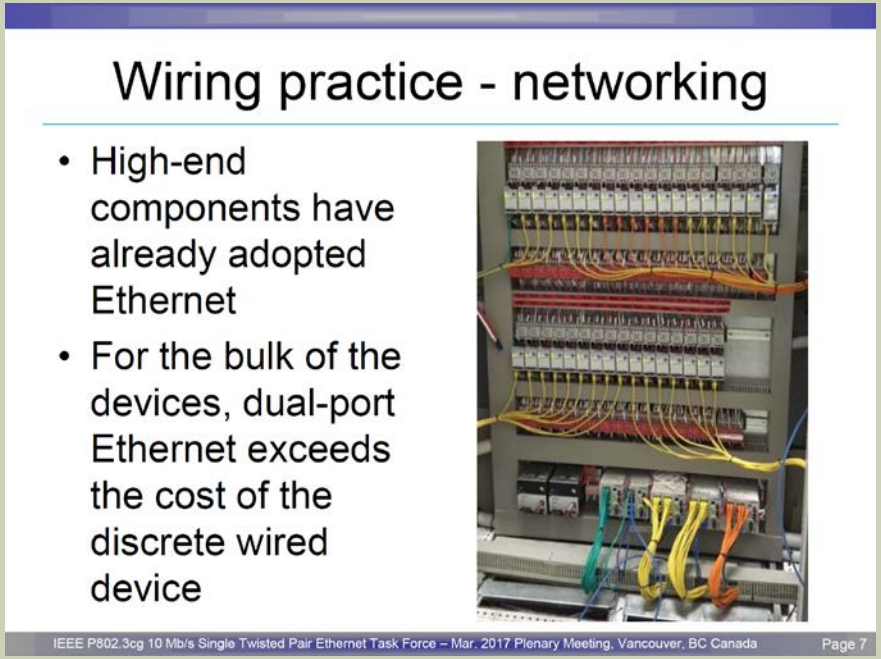


- Max latency is guaranteed to always be less than one PLCA cycle
- Round-robin scheduling provides fairness of opportunity
  - Amendments in progress to allow multiple TOs for nodes to be configured
- A PLCA cycle consists of one BEACON and N+1 transmit opportunities, allowing up to N+1 variable size packets to be sent
  - PHYs can start a transmission only during the transmit opportunity which number matches their own node ID
  - A new transmit opportunity starts if nothing is transmitted within TO_TIMER or at the end of any packet transmission

MULTIDROP 10BASE-T1S ISN'T JUST AUTOMOTIVE



10BASE-T1S for control plane in Ethernet switches

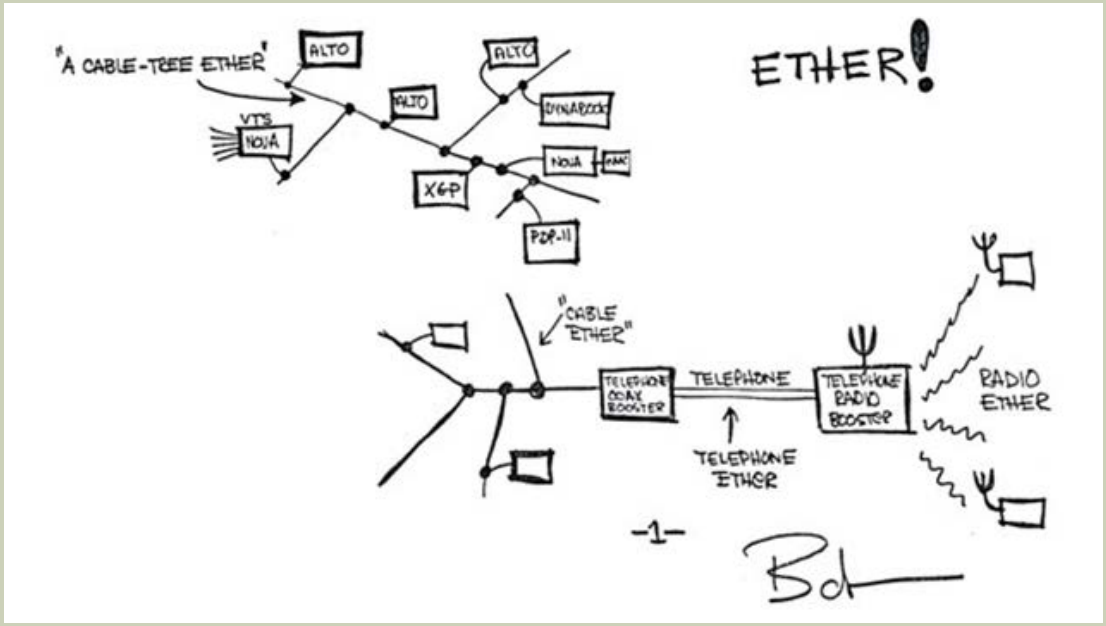


10BASE-T1S for industrial backplanes

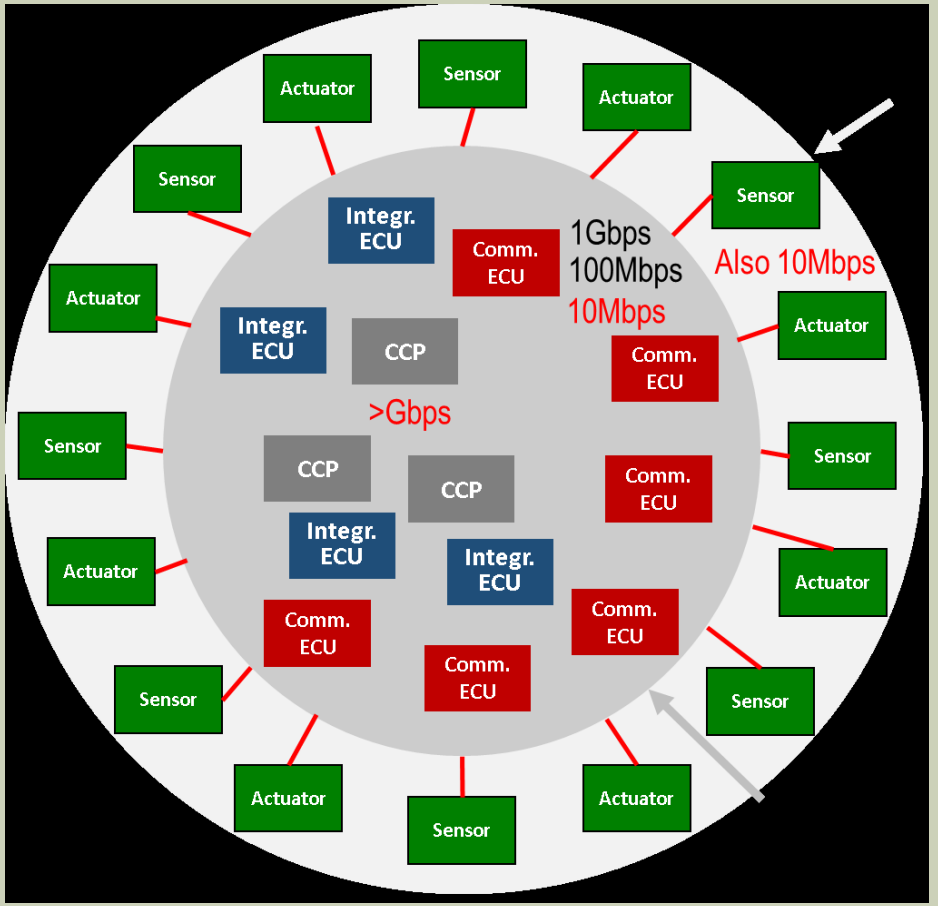
Wide usage of Single Pair Ethernet components builds the skill base as well as component volume

SPEEDS ENABLE A WHOLE AUTOMOTIVE ETHERNET NETWORK

THEN....



NOW....



The Challenges in the Development of a Complete Ethernet Vehicle

Don Pannell

Fellow
Automotive Ethernet Networking

Oct 2018 | IP Tech Day - London

SECURE CONNECTIONS FOR A SMARTER WORLD

Challenges of a Complete Ethernet Vehicle

- Ethernet in Automotive is what is referred to as a Brownfield market, meaning solutions already exist for the connection needs in a car. Some solutions have existed for many decades (CAN released in 1986). A “Complete Ethernet Vehicle” would imply a displacement of all existing connection methods.
  - Maybe its better to focus on a “Complete Ethernet Backbone in a Vehicle” first

- The driving force is clear. Higher speeds, redundancy & security, not to mention the benefits of the portability of Application Software.
  - Since 1980 Ethernet has consistently gotten cheaper, better and faster without needing the Application Software to be changed to take advantage of this

Challenges of a Complete Ethernet Backbone in a Vehicle

- Cost Effective Solutions, Education & Tools
  - Ethernet's 38 year history shows that the cost of Ethernet solutions go down
  - Education is the industry's job & your attendance at Conferences like this helps!
- Why Education?
  - Automotive Network developers need to understand what Time Sensitive Network (TSN) solutions can and cannot do. TSN removes "classic" Ethernet's deficiencies.
- Why Tools?
  - Due to TSN's many solutions, picking the right mechanism for a stream's needed determinist latency with reliability &/or security can be difficult
  - Tools like this exist today and I predict more and improved versions in the future
  - Future Backbone networks will likely be able to do this dynamically on-the-fly

Mixed Traffic over Ethernet

Norman Finn

HUAWEI TECHNOLOGIES CO., LTD.

Many kinds of data traffic

- **Mission critical** – ABS, engine control, displays
- High volume – camera video
- Infotainment – Audio, video distribution
- Vehicle to Vehicle, Vehicle to Infrastructure
- Data collection – fleet owner, manufacturer
- Software/firmware download
- Logging and diagnostics
- And on and on …

Bridging/Routing/TSN/DetNet can!

- Today, one enterprise network can carry a mixture of secure, insecure, high-volume, low-volume, local, long-distance, time-sensitive, bulk, … data flows. And, the **applications don't know about the network**.
- TSN/DetNet adds the capability to carry mission-critical flows, along with all the other data flows, over **one physical Ethernet network**.
- The designer can **change** the trade-offs made between development cost / production cost / flexibility / utility / reliability … **without redesigning the applications**.

Thank you

www.huawei.com

escrypt
SECURITY. TRUST. SUCCESS.

Security of next generation EE-Architecture

IEEE SA Ethernet & IP @ Automotive Technology Day

Siddharth Shukla

escrypt
SECURITY. TRUST. SUCCESS.

Apply defense in depth approach for security:

1. Network segregation
   - Limit number of external communication interfaces
   - Establish/preserve different communication domains (similar to CAN) based on VLANs for different critical networks
2. Threat detection (central vs distributed)
   - Firewall (whitelist/blacklist) as first level of defense using combination of:
     - Stateless Packet Inspection
     - Stateful Packet Inspection
     - Deep Packet Instection
   - Intrusion Detection System (IDS) to detect potential attacks in field
3. Consider secure onboard communication
   - MACSec (with possible modifications),
   - IPSec
   - (D) TLS
   - SecOC
4. Intrusion Prevention System (IPS) to prevent attacks
5. FOTA to update firmware in field

Recommendations:

1. Use hardware assisted firewall/IDS solutions to achieve performance requirements (possibly in switch)
2. Consider state-of-art security requirement for switch hardware (secure boot, upgrade and downgrade etc.)
3. Cover complete Ethernet stack for protection

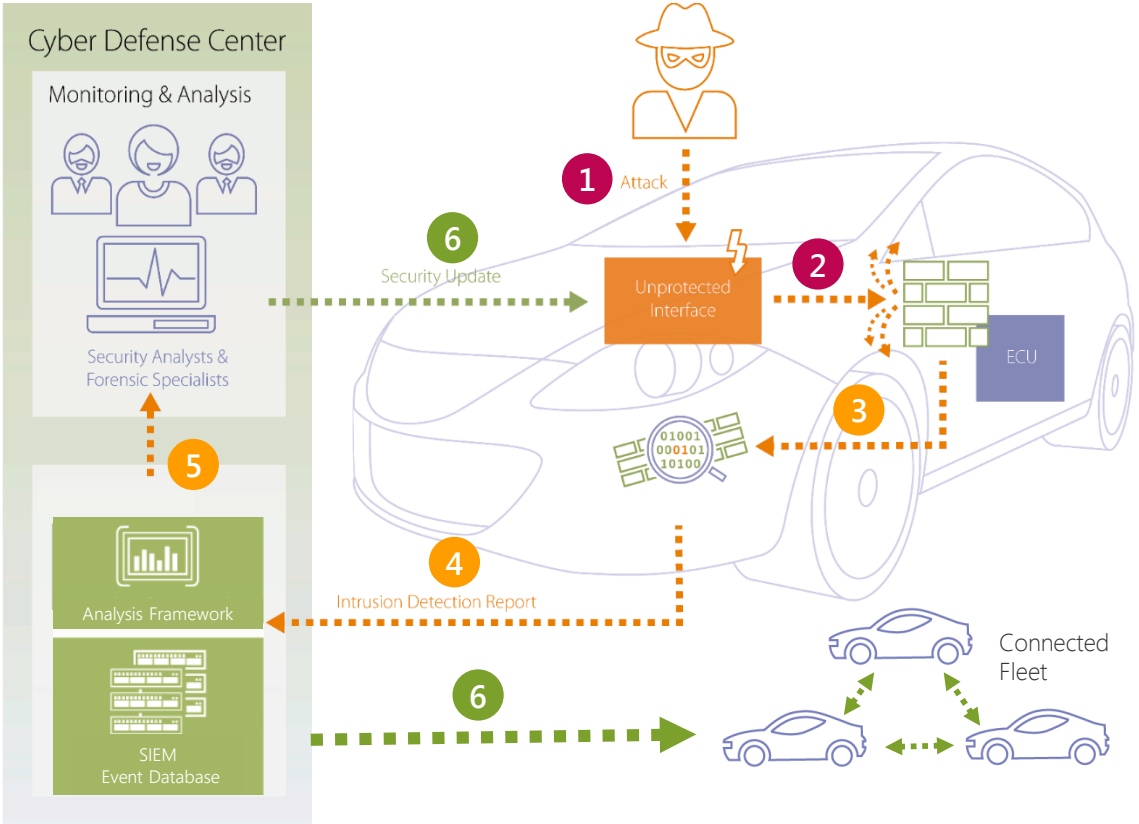
Challenges:

1. MAC address translation
2. MAC address Pre learning or during runtime?
3. PNAC or local CPU based MAC authentication?
4. Security in TSN?
5. Achieving configurable hardware/software co-design?

In-Vehicle network protection

Continuous protection over entire vehicle life cycle

escrypt
SECURITY. TRUST. SUCCESS.



1. **Attack:** Misuse of 0-day exploit in web browser
2. **Security is not absolute:** The OEM's secure flashing implementation was vulnerable and the attacker was able to flash and run arbitrary code, e.g., in order to send malicious signals.
3. **Firewall:** The filtering mechanisms blocks illegitimate signals, e.g, from an invalid source, and informs the IDS. The attacker is not able to control other ECUs.
4. **Intrusion Detection:** When attacker performs advanced attacks, the in-vehicle IDPS solution detects the anomaly (i.e., potential attack) on the in-vehicle network, it creates and sends an Intrusion Detection Report
5. **Monitoring & Analysis:** The IDPS backend collects all anomaly reports from the vehicle fleet and enables security analysts and forensic specialist to analyze the attack and identify the vulnerability
6. **Intrusion Prevention:** A security update to remedy the vulnerability will be deployed to the entire vehicle fleet

ESCRYPT GmbH
Headquarters
Wittener Straße 45
44879 Bochum
Germany

Phone: +49 234 43870-200
Fax: +49 234 43870-211

info@escrypt.com
www.escrypt.com

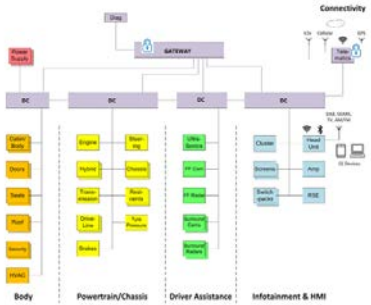
PANEL SESSION

THE CHALLENGES IN THE DEVELOPMENT OF A COMPLETE ETHERNET VEHICLE

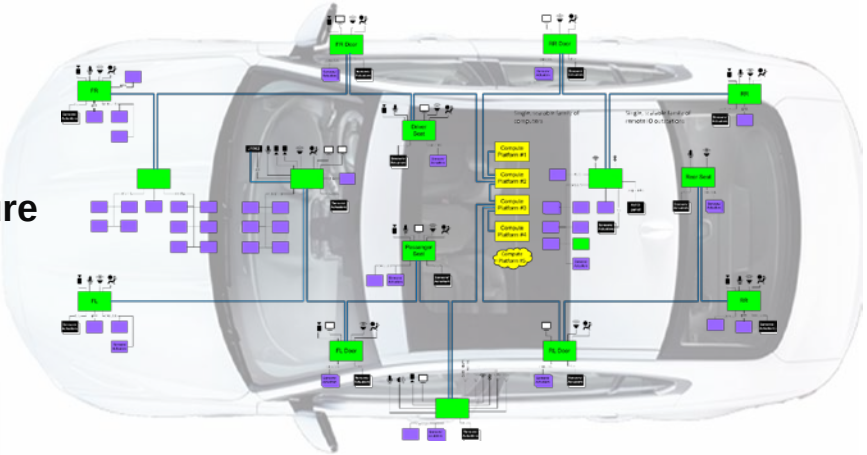
Moderator: Syreeta Bath
Panellists: Kirsten Matheus, George Zimmerman, Don Pannell, Norman Finn, Siddharth Shukla
9th October 2018, Olympia London

ARCHITECTURES AND NETWORK TYPES

Domain Based Architecture



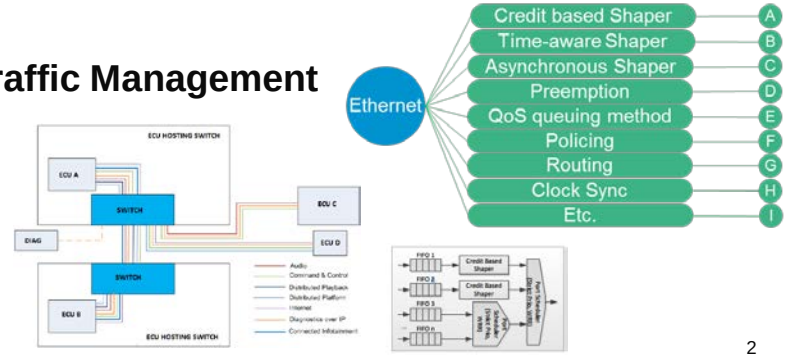
Zonal Architecture



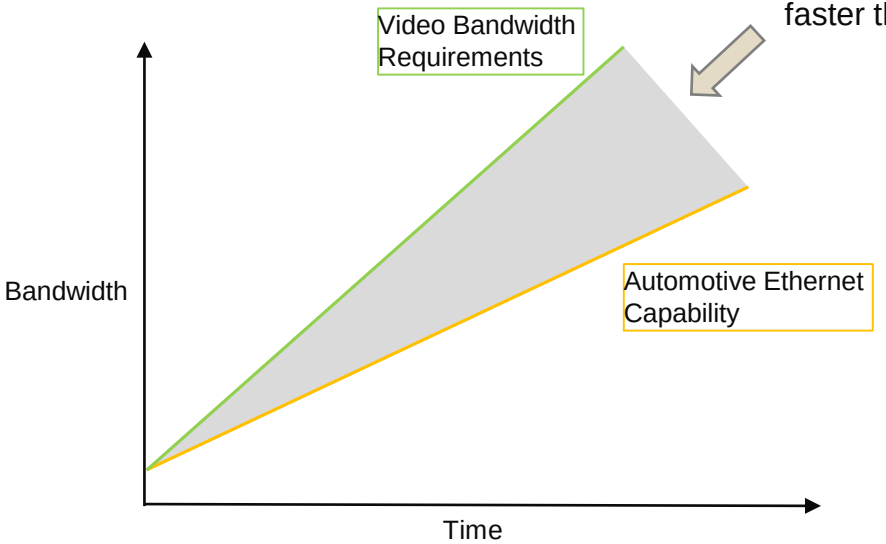
Protocols

Layer		Diagnostics	Services & Discovery	Address Config	Video	Audio	Time Sync	Support Protocols
7 6 5	**Application Presentation Session**	DoIP/ TFTP SecOc	SOME/IP & SD	DHCP	RTP	IEEE 1722 (AVTP)	IEEE 802.1AS (gPTP)	ICMP, ARP
4	**Transport**	TLS	TCP/ UDP					
3	**Network**	IPSec	IPv4/ IPv6					
2	**Data Link**	MacSec	Ethernet MAC & VLAN (802.1Q)					
1	**Physical**	Ethernet Physical Layer						

Traffic Management

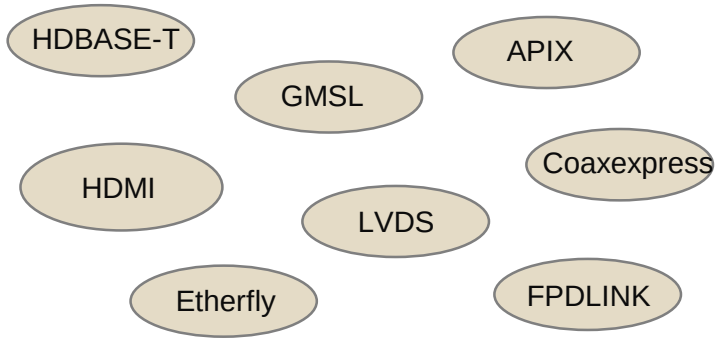


VIDEO ARCHITECTURES
(TYPICAL USE CASE FOR HIGHER BANDWIDTH)



Bandwidth requirements for video use cases seems to be increasing faster than Automotive Ethernet Speed grade increases

What fills the gap…..
Consumer or Proprietary technologies



PANEL CONCLUSION

How would you envision your vehicle in 2030 and beyond? How much of the vehicle will be IP based, will we still have a mix of other IVN technologies to support some of the use cases discussed today?