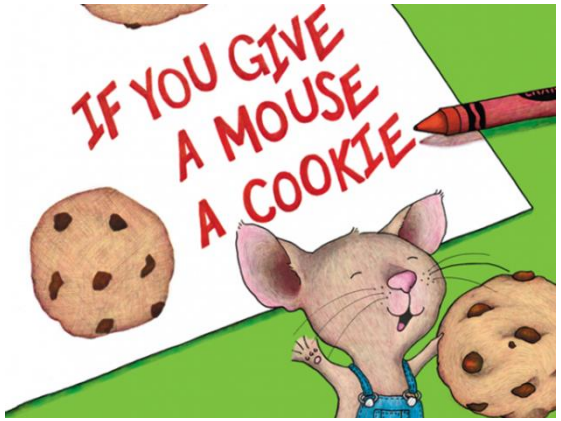
IEEE 802 Ethernet Networks for Automotive

Steven B. Carlson, János Farkas, Norm Finn,
Don Pannell, Mike Potts, Mick Seaman,
Natalie Wienckowski, George Zimmerman

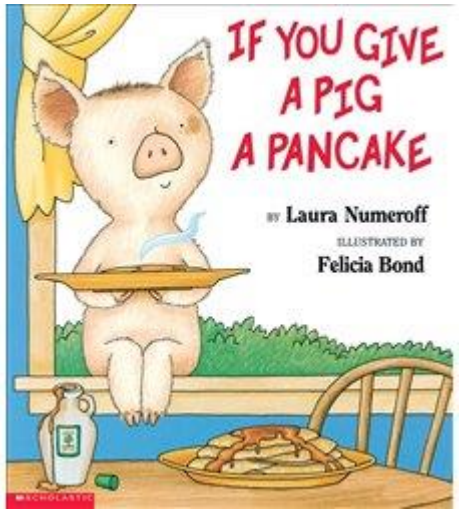
Outline

- Motivation
- PHY
- Time-Sensitive Networking (TSN)
  - reliability and timing
- Security
- Summary
- Q&A

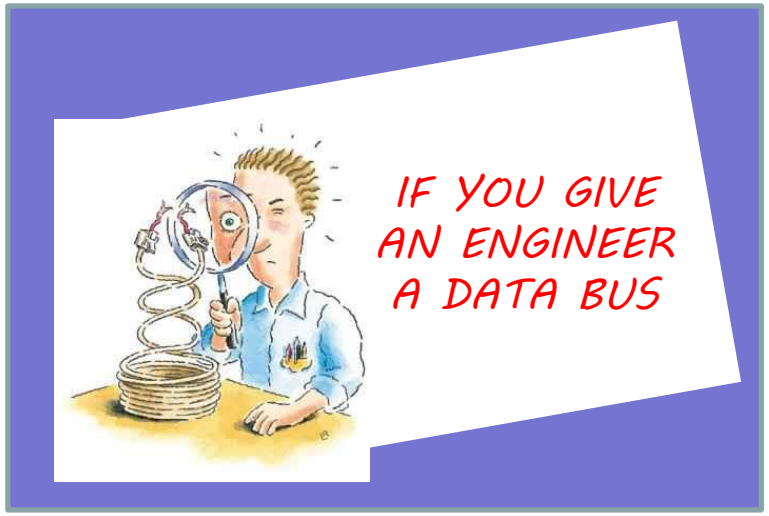
MOTIVATION



He's going to ask for a glass of milk.



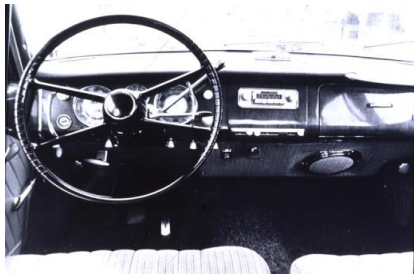
She'll ask for a bottle of syrup.



He'll ask for more bandwidth and faster speeds.

Innovation in Automotive Technology is both Hardware & Software

- **Increasing number of applications**
  - Increasing complexity over time
  - Higher bandwidth requirements
  - Need reliable networks



Electronic Injection
Check engine control
Cruise control
Central locking
…

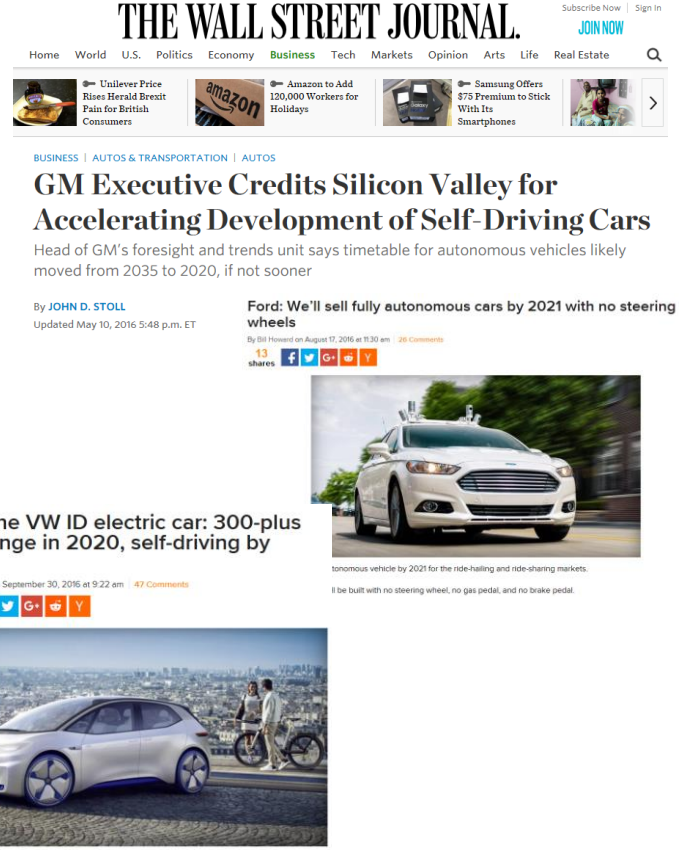
Gearbox control
Climate control
ASC Anti Slip Control
ABS Anti -lock Brake Sys.
Telephone
Seat heating control
Automatic mirrors

Navigation system
CD-changer
Active Cruise Control
Airbags
Dynamic Stability Control
Roll stabilization
Xenon lighting
Vehicle Assist
Voice input
Emergency call

ACC Stop&Go
Lane departure warning
Blind spot warning
Traffic sign recognition
Night vision
Active headlight system
Parking automation
Efficient dynamics
Hybrid engines
Internet access
Telematics
Online Services
Bluetooth integration
Local Hazard Warning
Personalization
SW Update
Smart Phone Apps

1970 1980 1990 > 2010

http://www.driverless-future.com/?page_id=384



Adapted from material provided by BMW

Motivation for Ethernet

- Data Needs
  - Raw camera data
  - Data logging (Government Regulations)
  - Map Data
  - Backbone aggregation
  - High resolution displays
  - In vehicle Wi-Fi hotspot (carrier link aggregation) – wired backhaul
- Latency Requirements
  - Minimum determined by Hardware
  - Maximum determined by Software
- Services
  - Precise Time Awareness
  - Redundancy / Fail over
  - Security

How is Automotive Different?

- Link Segment lengths are shorter
- Environment (EMC, Temperature, etc.) is harsher
- Qualification of Hardware is required
- Validation of Electronic Control Unit (ECU) Hardware and Software is required
- Reliability (higher MTBF)
- Start Up Time is shorter
- Latency is smaller
- Repeatability/Predictability is critical
- Safety/ASIL (ISO26262) compliance

Latency

- Real-time networks require **guaranteed not-to-exceed end-to-end latency** for critical data
- Two ways to accomplish this:
  1. ~~Throw away late packets~~
  2. **Provide zero congestion loss**
- Shapers and queueing define the time interval
- Worst-case latency
  a) Is guaranteed
  b) Grows linearly with the number of hops
- Average latency may be larger than simple priority

Keys to Success

- Reliability
- Predictability
- Flexibility
- Security

PHY

Automotive Networks

- **CAN (Controller Area Network) – since 1991**
  - Low-speed serial data bus: 1 – 1000 Kbps
  - Shared medium with CSMA/CR (Collision Resolution)
  - Dominant control bus in all automotive domains
  - Standardized in ISO 11898; Multi-vendor support

- **FlexRay (consortium of automotive companies) – since 2005**
  - 10 Mb/s serial data bus (single or dual channel)
  - Shared medium with TDMA
  - Control bus for high dynamic applications, chassis control, but also designed for future “X-by-Wire” applications
  - Standardized in ISO 10681; Multi-vendor support

Automotive Networks

- **MOST (Media Oriented Systems Transport) – since 2001**
  - Shared ring topology: 25 Mb/s (POF), 50 Mb/s (Cu), 150 Mb/s (POF)
  - Bus system for control and streaming Infotainment data
  - Proprietary solution

- **Ethernet (100BASE-TX) – since 2008**
  - Mainly diagnostics and firmware upgrades during vehicle servicing (typically not used while the car is operating due to EMC limits)
  - Standardized in ISO 13400-3:2011 Road Vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 3: Wired vehicle interface based on IEEE 802.3
  - 100BASE-T1 – since 2013

- **LVDS / CML – since 2001**
  - Point-to-point high-speed links (1-4 Gb/s) for cameras and displays
  - Multi-vendor support but typically incompatible with each other

Typical Wire Harness in a Car

Used with permission from Molex

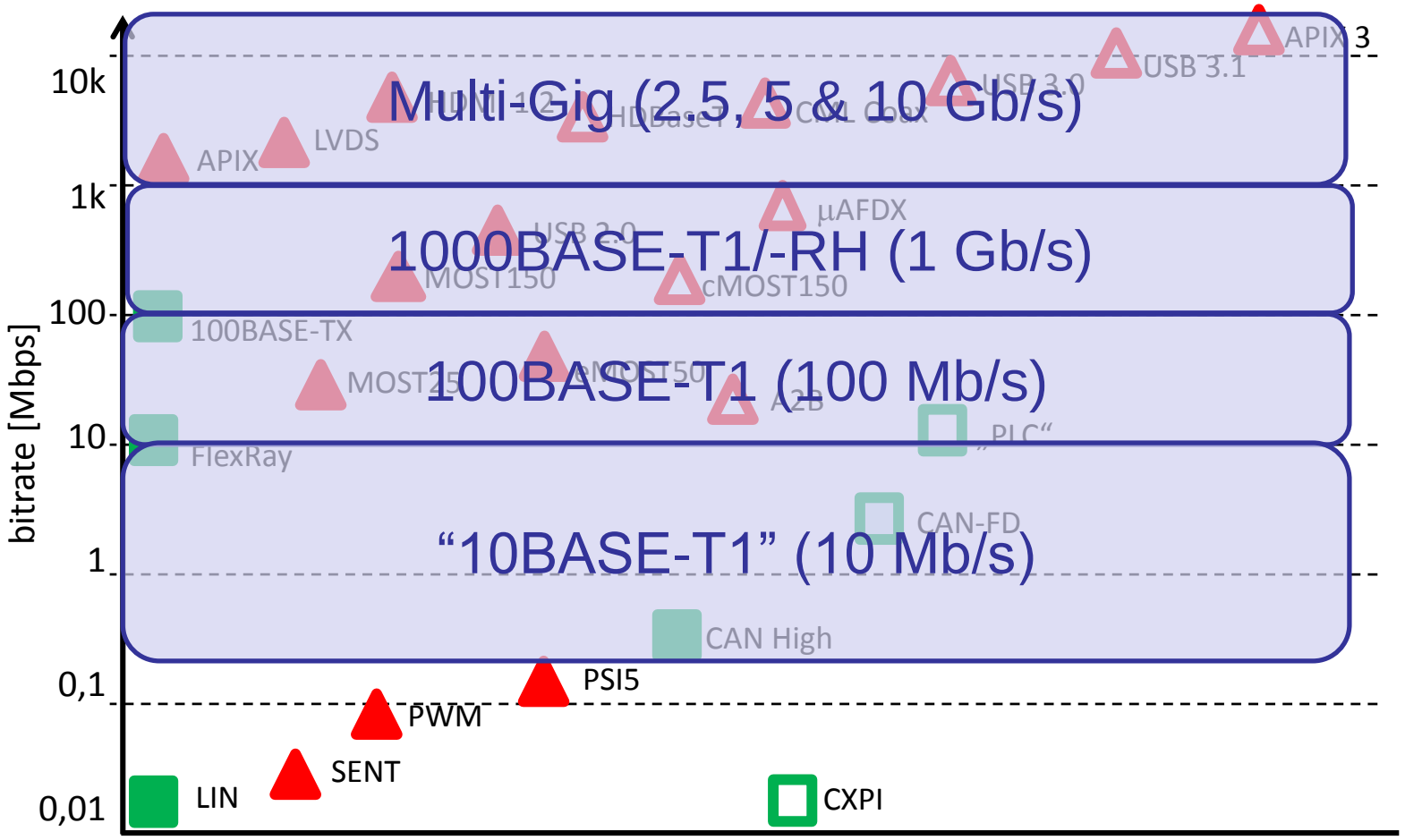
Cabling is the 3rd highest cost component in a car
- Engine (1st)
- Chassis (2nd)

Harnesses are built **ONE** at a time with 50% of cost in labor

Cabling is the 3rd heaviest component in a car
- Chassis (1st)
- Engine (2nd)

Reducing cable weight has a direct impact on fuel economy!

Automotive Ethernet



- There are no standard communication links for system usage above 1000 Mbps
- There are many proprietary communication links above 1000 Mbps
- Standard links are needed for this space
- There are no standard communication links for system usage between 100 Mbps and 1000 Mbps
- There are few standard communication links for system usage between 10 Mbps and 100 Mbps
- There are many standard communication links for system usage below 10 Mbps
- However, adding Ethernet in this space reduces the need for Gateways between various networks

Specific use

System use

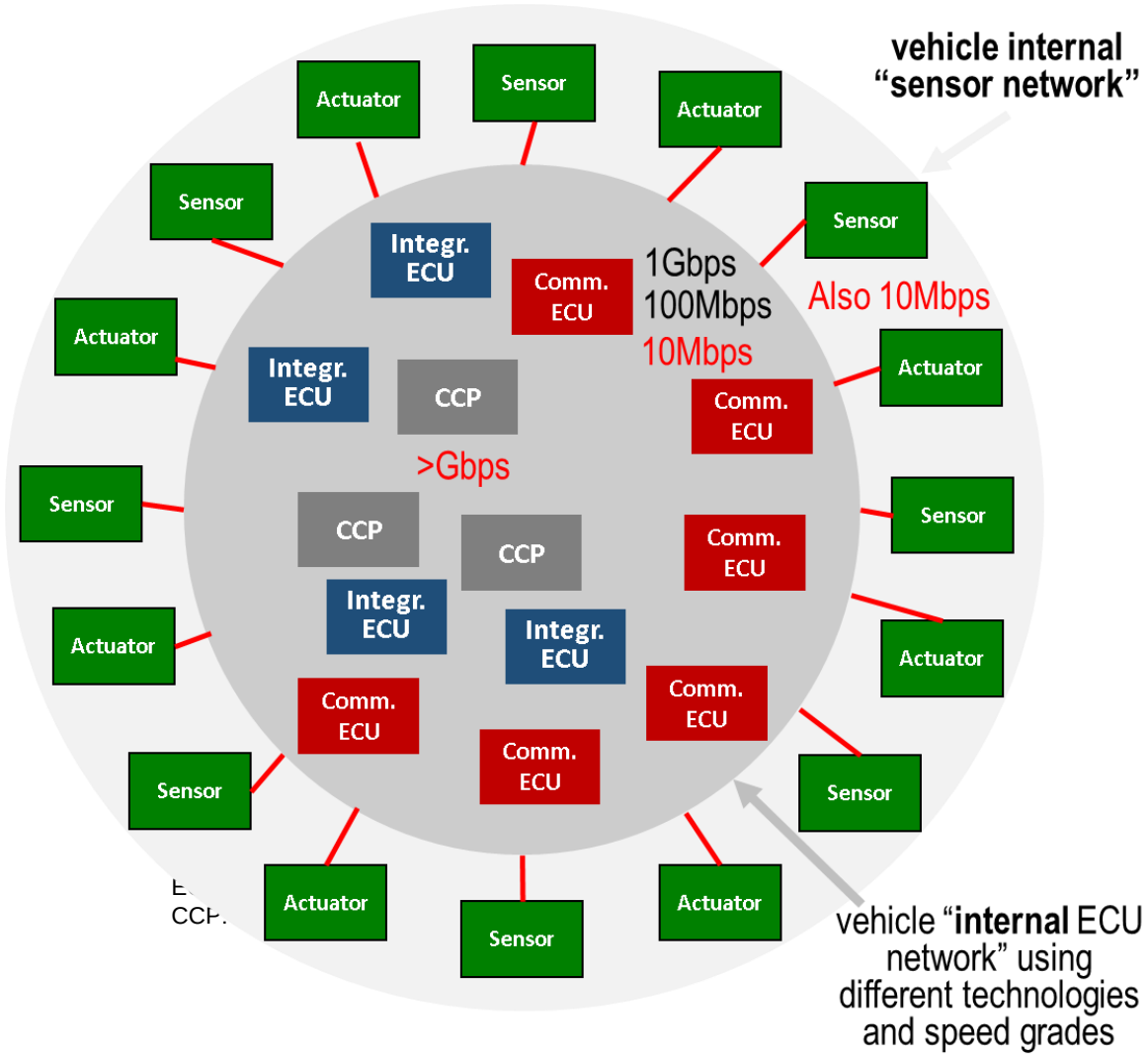
Proposed technologies

Specific use

System use

Technologies in series development

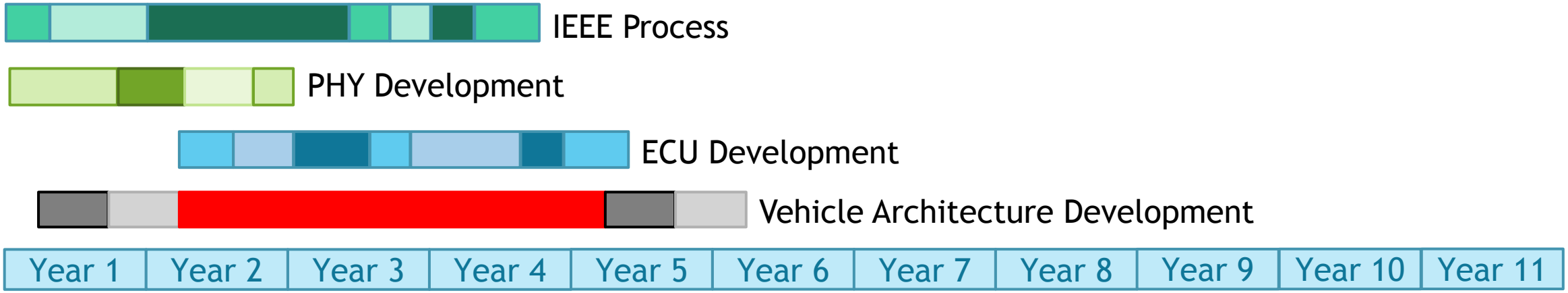
Automotive Architecture Trends



- The transition to Ethernet is underway.
  - 802.3bp, 802.3bw
- There is a desire to converge towards **one** network type (“Ubiquitous IP”).
  - Independence of physical and logical network.
  - Reduction in number of In-Vehicle Network (IVN) technologies. (MOST / FlexRay / …)
  - Reduction of multiple gateways.

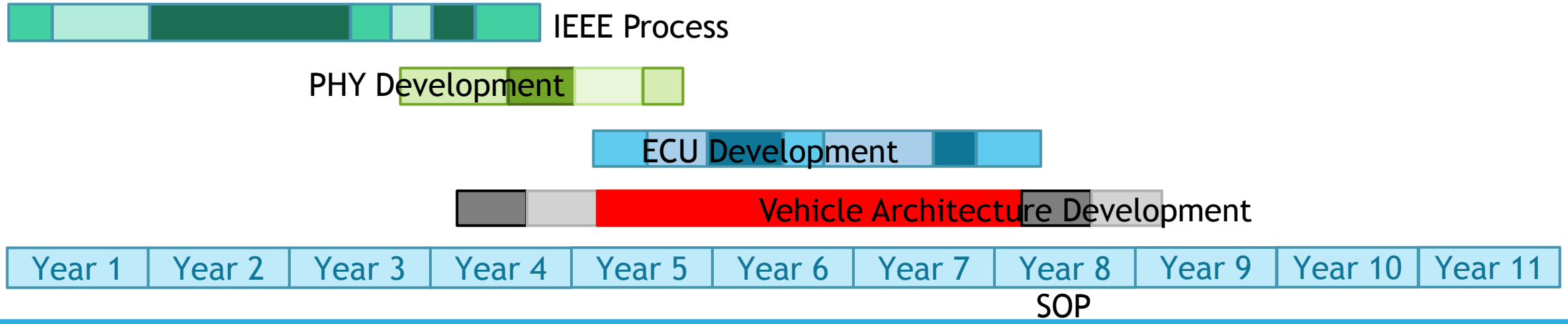
Total Automotive Ethernet PHY Development from Concept to Production

- Vehicle Architecture Development takes about 1 year and is done every 4 to 6 years.
- ECU Development takes about 3.5 years from RFQ to SOP.
- ECU Development starts after Vehicle Architecture Development.
- PHY Development takes about 2 years from the time all requirements are known and silicon is available for qualification.
- PHY samples must be available before end of Vehicle Architecture Development in order to be considered for the Architecture.
- The IEEE Process takes about 4 years.
- PHY sample development can start about 3 years into this process.



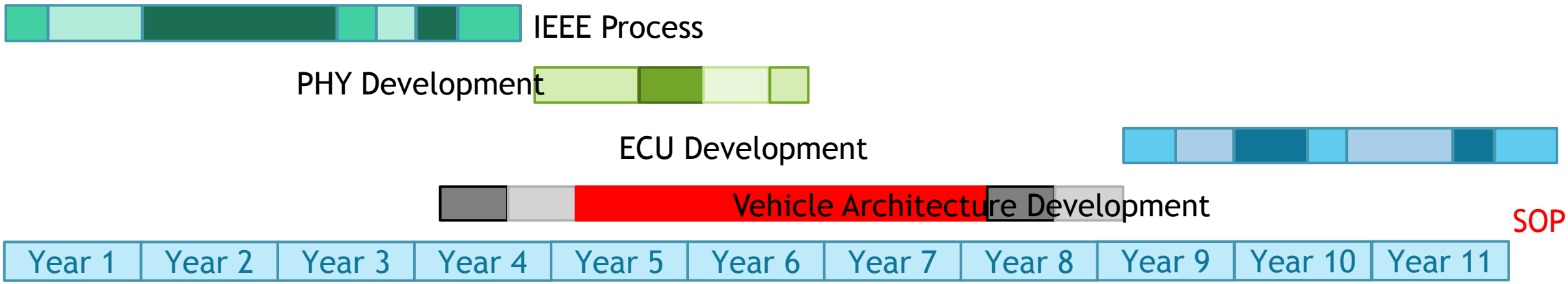
Total Automotive Ethernet PHY Development from Concept to Production

- The IEEE Process takes about 4 years.
- PHY sample development can start about 3 years into this process.
- If this lines up with the Vehicle Architecture Development, SOP is 8 years after the start of the IEEE Process.



Total Automotive Ethernet PHY Development from Concept to Production

- PHY Development may not start until the IEEE Process completes.
- If this does not line up with the Vehicle Architecture Development, SOP may be 11 (or more) years after the start of the IEEE Process.



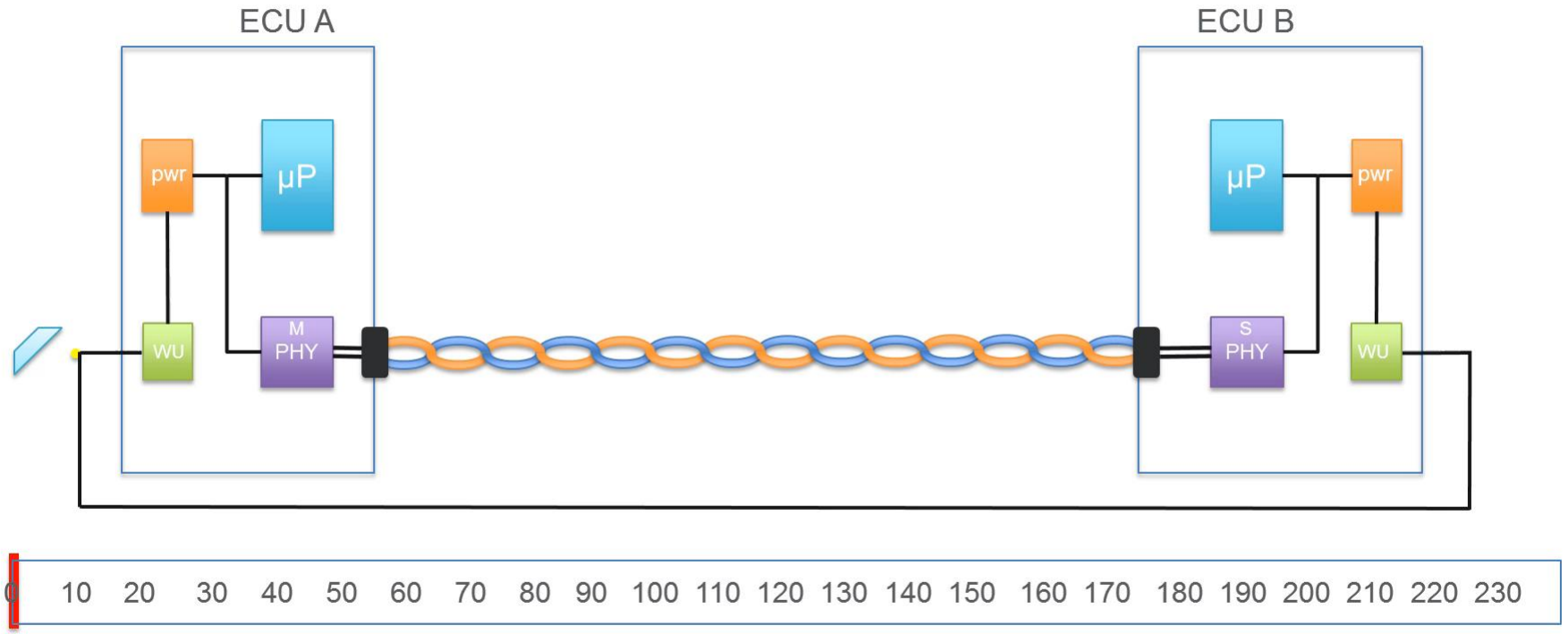
Automotive Conditions

- **Harsh Environmental Conditions**
  - Operating temperatures:
    - Body & cabin: -40°C to 85°C
    - Chassis & powertrain: -40°C to 125°C or even 150°C
  - Mechanical accelerations:
    - Body & cabin: up to 4 G
  - Dirt, water, salt, dust, ice, snow, mud, oil, grease, transmission fluid, brake fluid, engine coolant, hydraulic fluid, fuel, etc. (i.e., this is not a data center)
- **Automotive EMC requirements are stringent!**
  - Tighter requirements than Class A/Class B EMI specs for consumer products
  - Automotive EMC test specs exist, e.g., CISPR25 & ISO11452-2 & -4
  - ESD, owners don't wear ESD straps

For additional information see:

- http://www.ieee802.org/3/bw/public/buntz_tazebay_3bw_01_0914.pdf
- http://www.ieee802.org/3/bw/public/Wienchowski_3bw_02_0914.pdf

ECU START-UP EXAMPLE 1
PHY MASTER/SLAVE PRE-CONFIGURED

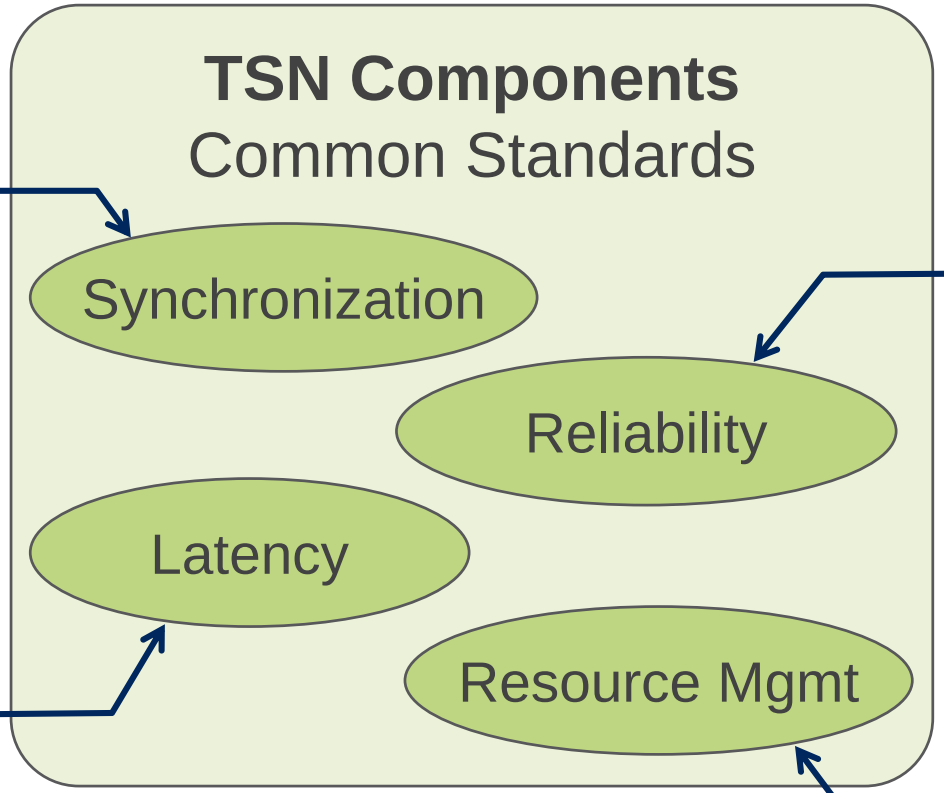


GENERAL MOTORS

1

TIME-SENSITIVE NETWORKING
RELIABILITY AND TIMING

Time-Sensitive Networking (TSN)



Time synchronization:
Timing and Synchronization

Ultra reliability:
Frame Replication and Elimination
Path Control and Reservation
Per-Stream Filtering and Policing
Reliability for time synchronization

Bounded low latency:
Credit Based Shaper
Frame preemption
Scheduled Traffic
Cyclic Queuing and Forwarding
Asynchronous Traffic Shaping

Dedicated resources & API
Stream Reservation Protocol
TSN configuration
YANG
Link-local Registration Protocol

Zero congestion loss

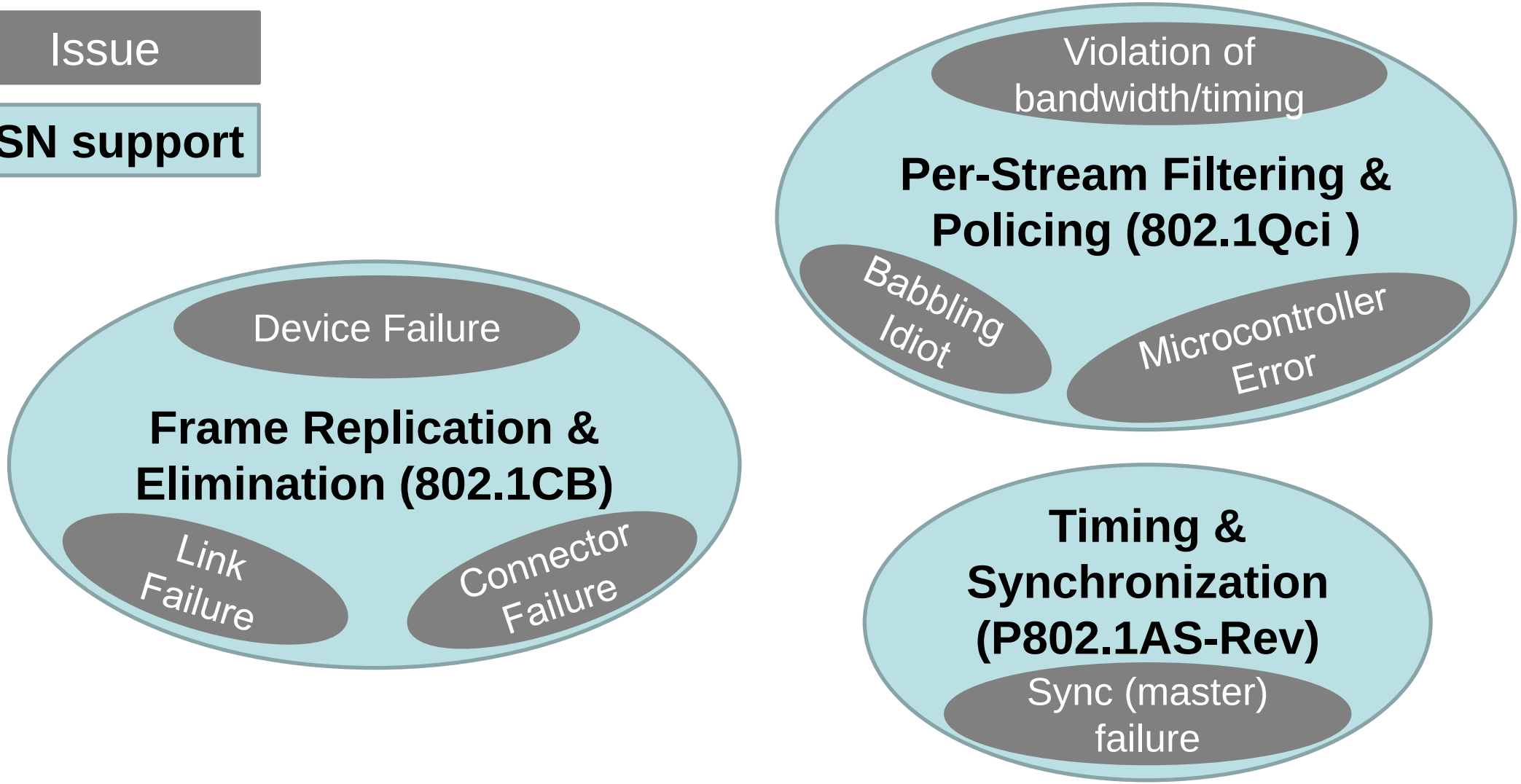
Guaranteed data transport with bounded low latency, low delay variation, and extremely low loss

Audio Video Bridging (AVB) → Time-Sensitive Networking (TSN)

Reliability

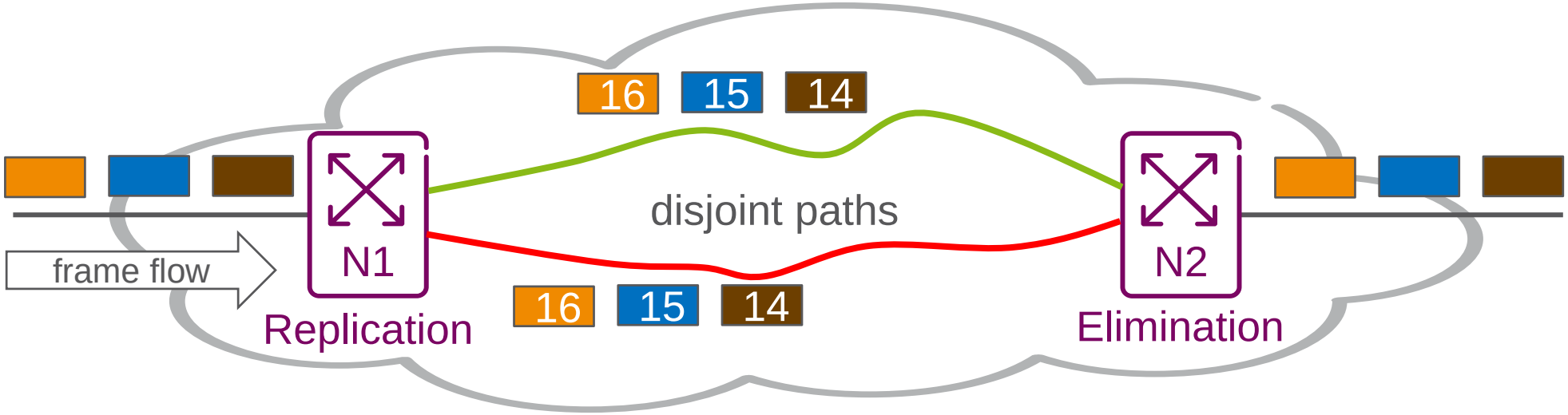
Issue

TSN support

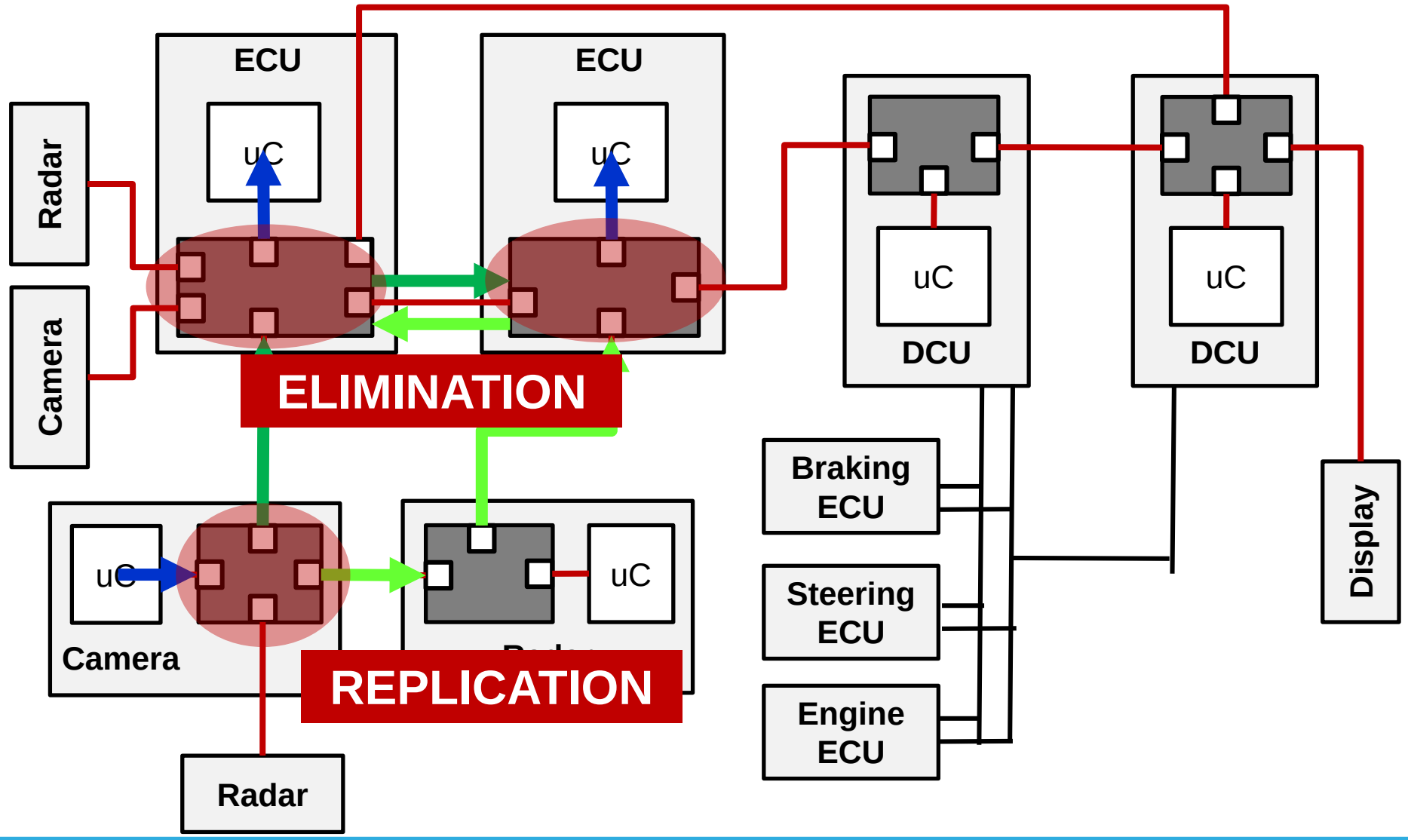


Frame Replication and Elimination

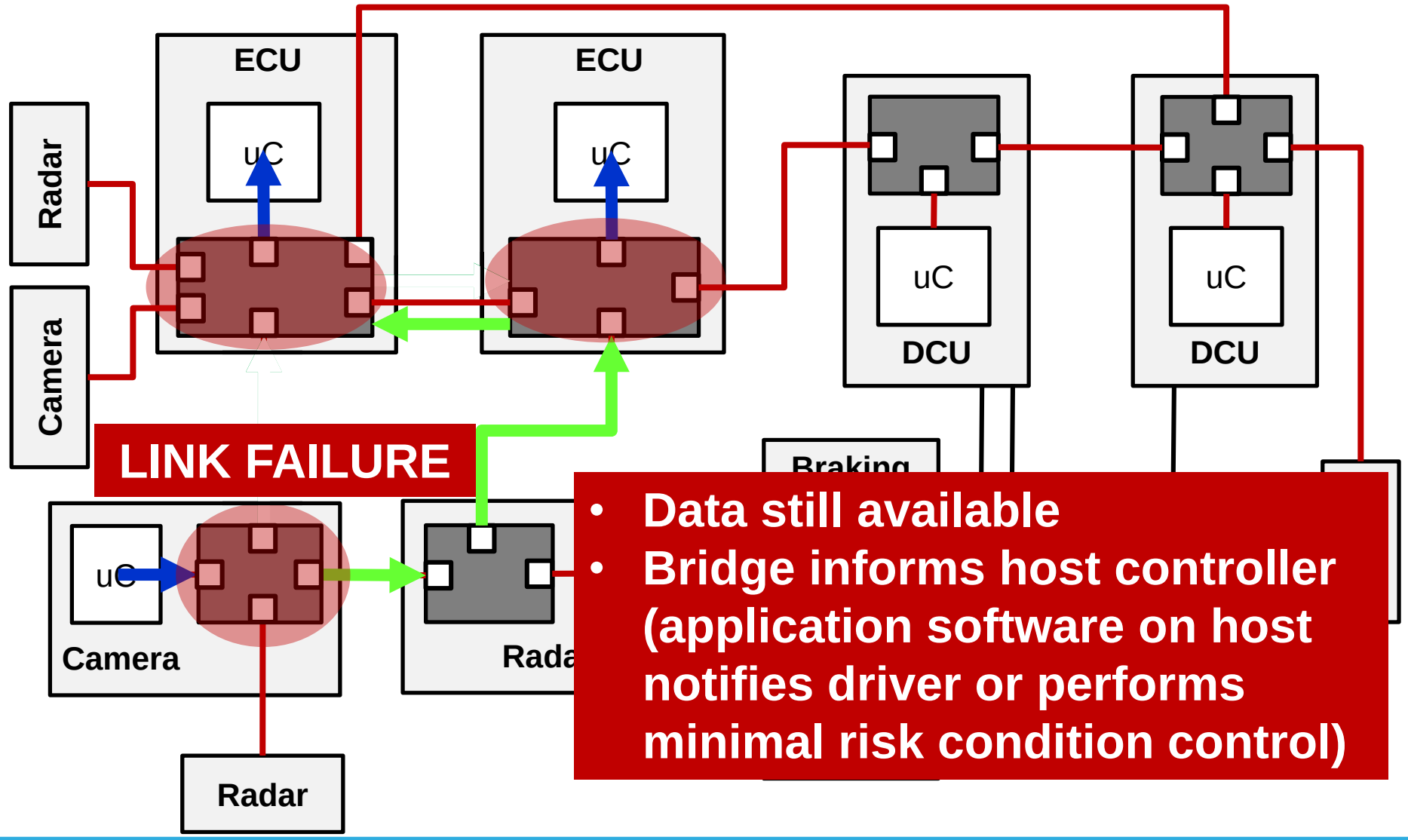
- Avoid frame loss due to equipment failure (802.1CB)
- Per-frame 1+1 redundancy
  - NO failure detection / switchover
- Serialize frames, send on two maximally disjoint paths, then combine and delete extras



Frame Replication and Elimination in a Car

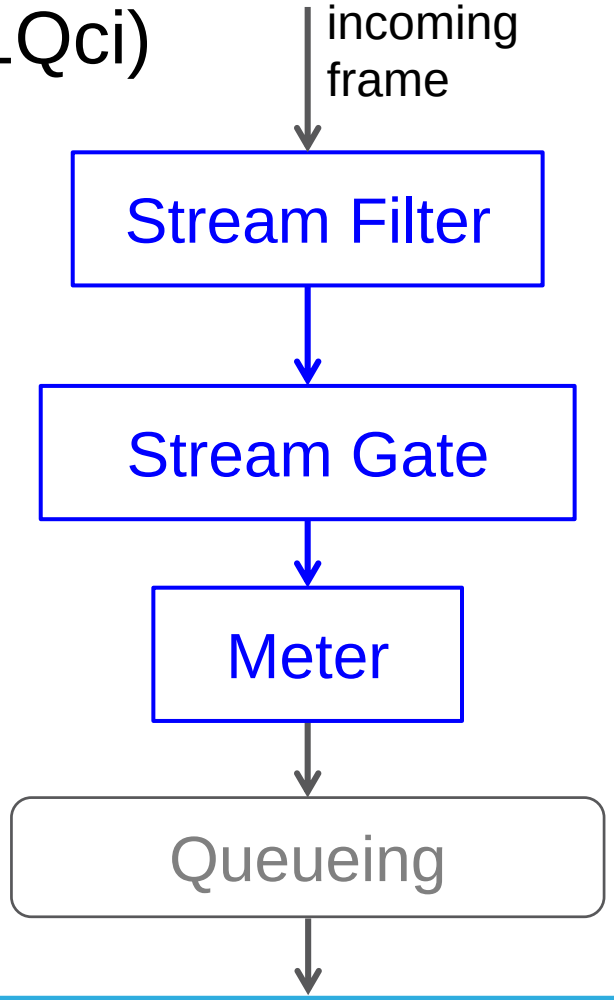


Frame Replication and Elimination in a Car

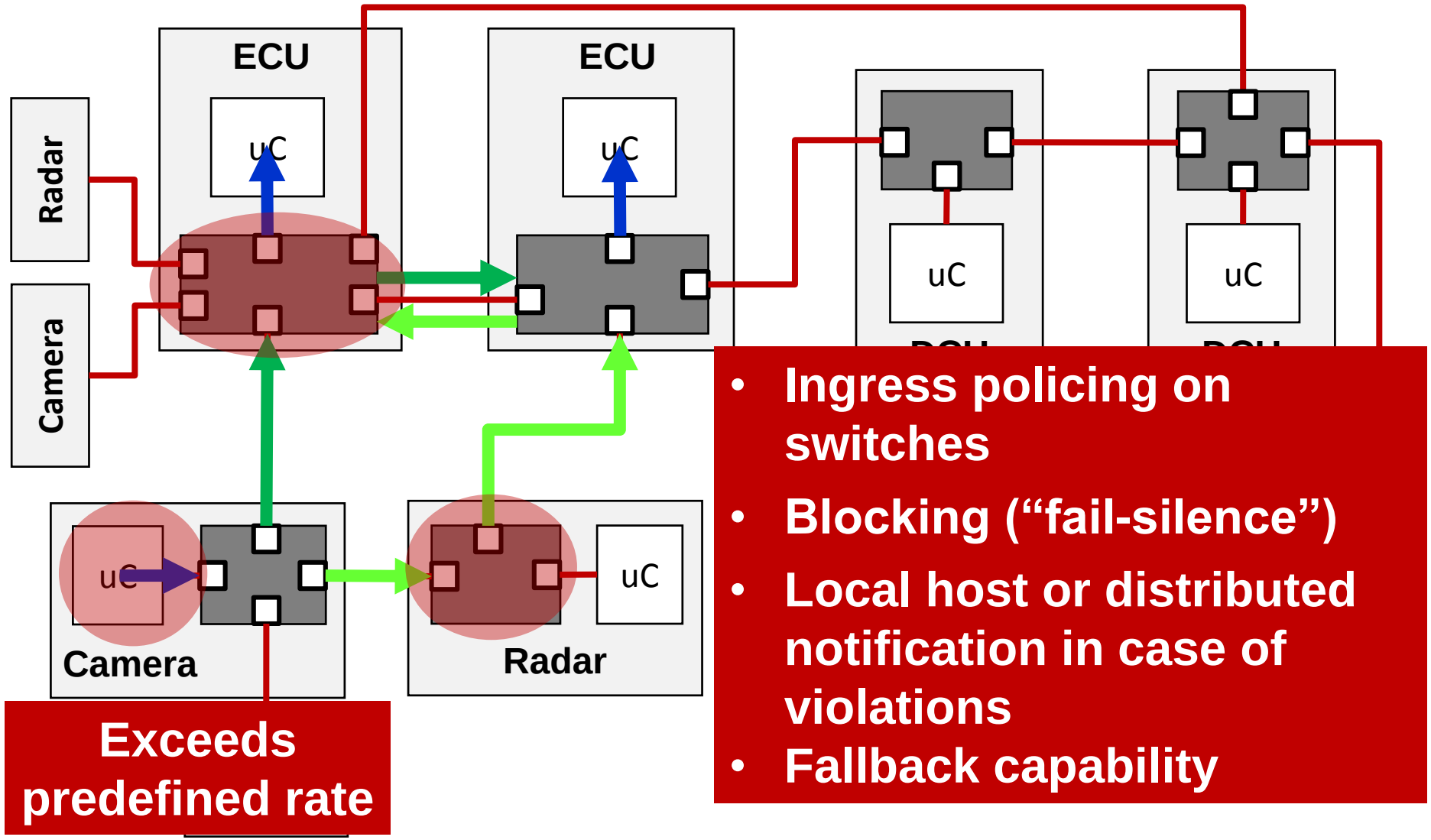


Per-Stream Filtering and Policing

- Protection against bandwidth violation, malfunctioning, malicious attacks, etc. (802.1Qci)
- Decisions on per-stream, per-priority, etc.
- Stream Filter → Defense
  - Filters, Counters
- Stream Gate → Defense
  - Open or Closed
  - can be time-scheduled
- Meter → Defense
  - Bandwidth Profile of MEF 10.3
  - Marking



Per-Stream Filtering and Policing in a Car



Deterministic Low Latency

Task/Issue

TSN support

Synchronization

Timing & Synchronization (P802.1AS-Rev)

Reduce latency variation

Synchronization Accuracy: n*100ns

Shared network

Scheduled Traffic (802.1Qbv)
Frame Preemption
(802.3br, 802.1Qbu)

Critical & non-critical traffic

Braking Steering actuation

Latency variation: n*1µs
End-to-end latency: 100µs

Network set-up

TSN Configuration & SRP Enhancements (P802.1Qcc)

Resource reservation

Asynchronous QoS

Asynchronous Traffic Shaping (P802.1Qcr)

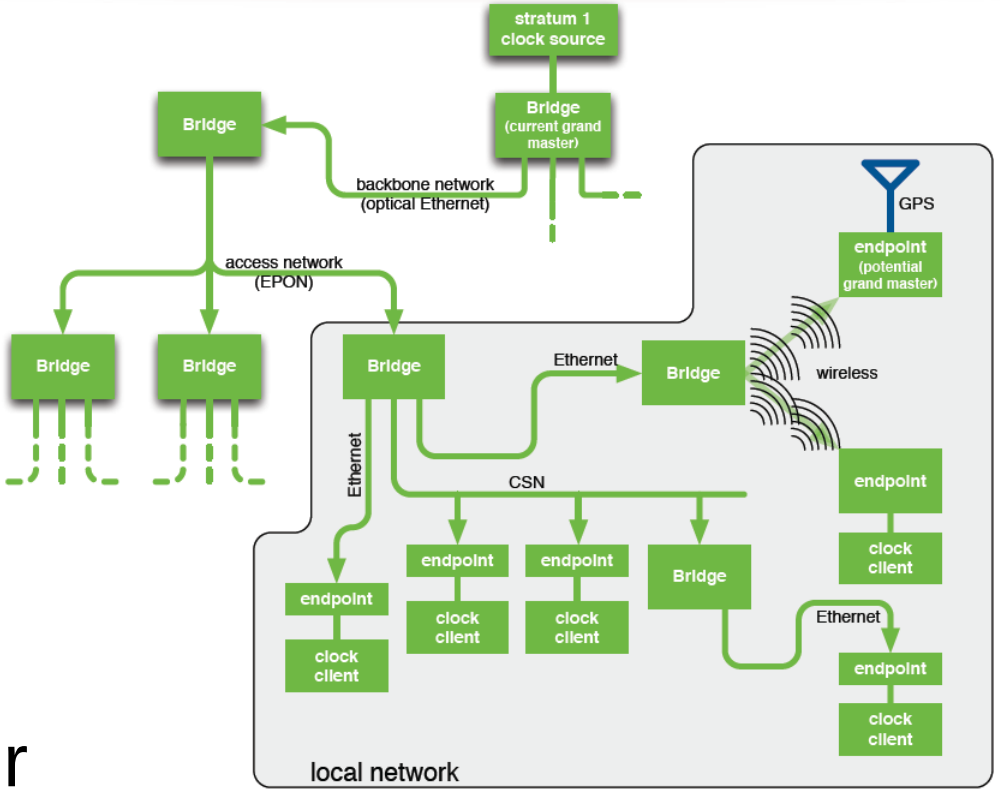
Simplicity, e.g., for security

Automation

The right packet at the right time!

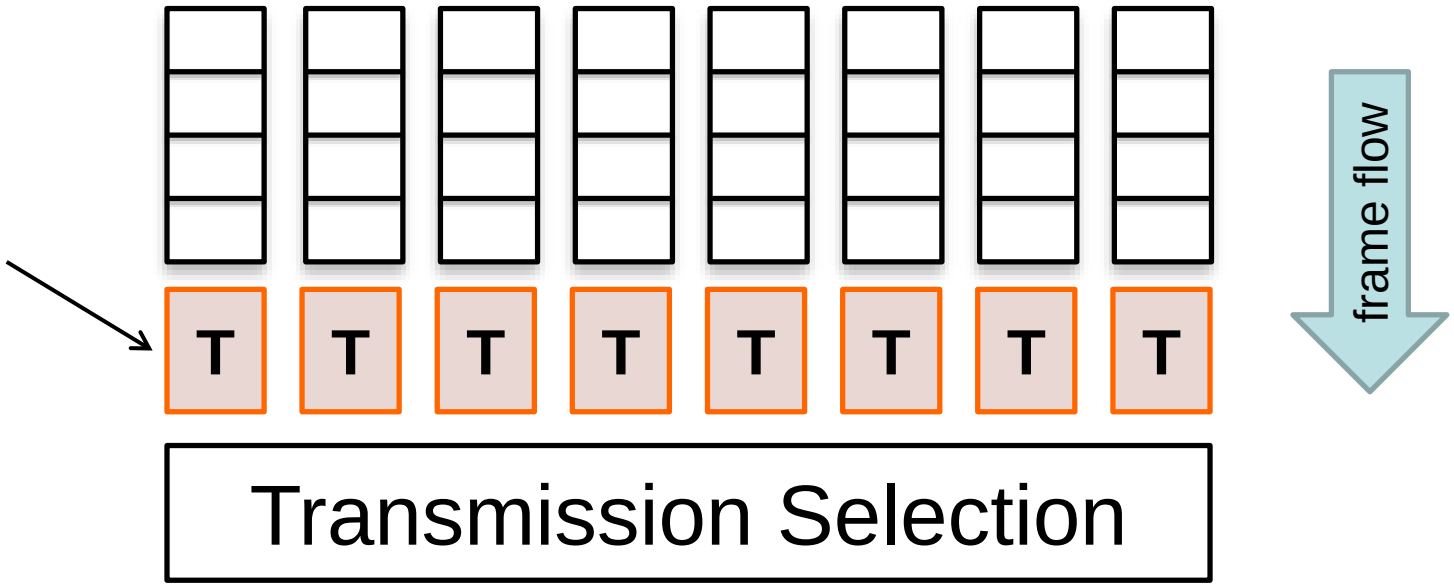
Timing & Synchronization

- A profile of IEEE 1588v2 for Layer 2 Ethernet (P802.1AS-Rev)
- Redundancy
  - Redundant paths
  - Redundant Grand Masters
- Improved scalability
- Improved support for long chains, rings
- More responsive
- Faster Grand Master change over
- Reduce Best Master Clock Algorithm (BMCA) convergence time
- Multiple domains with synchronization information



Scheduled Traffic

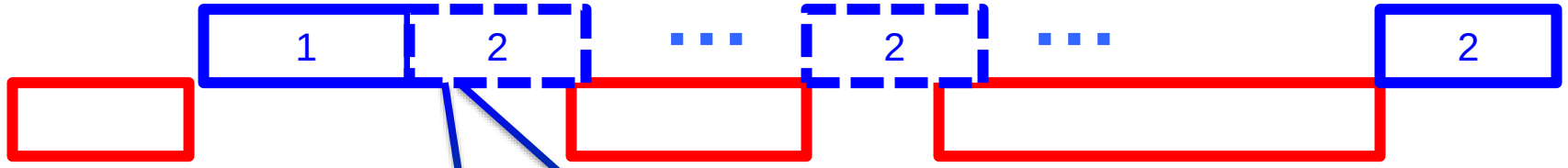
- Reduces latency variation for Constant Bit Rate (CBR) streams, which are periodic with known timing
- Time-based control/programming of the 8 bridge queues (802.1Qbv)
- Time-gated queues
- Gate: Open or Closed
- Periodically repeated time-schedule
- Time synchronization is needed



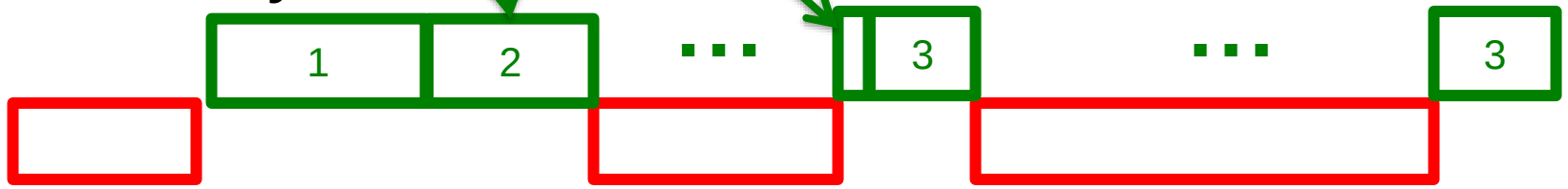
Frame Preemption

- Express frames suspend the transmission of preemptable frames (802.3br and 802.1Qbu)
- Scheduled rocks of critical packets in each cycle:

- Conflict excessively with non-guaranteed packet rocks:

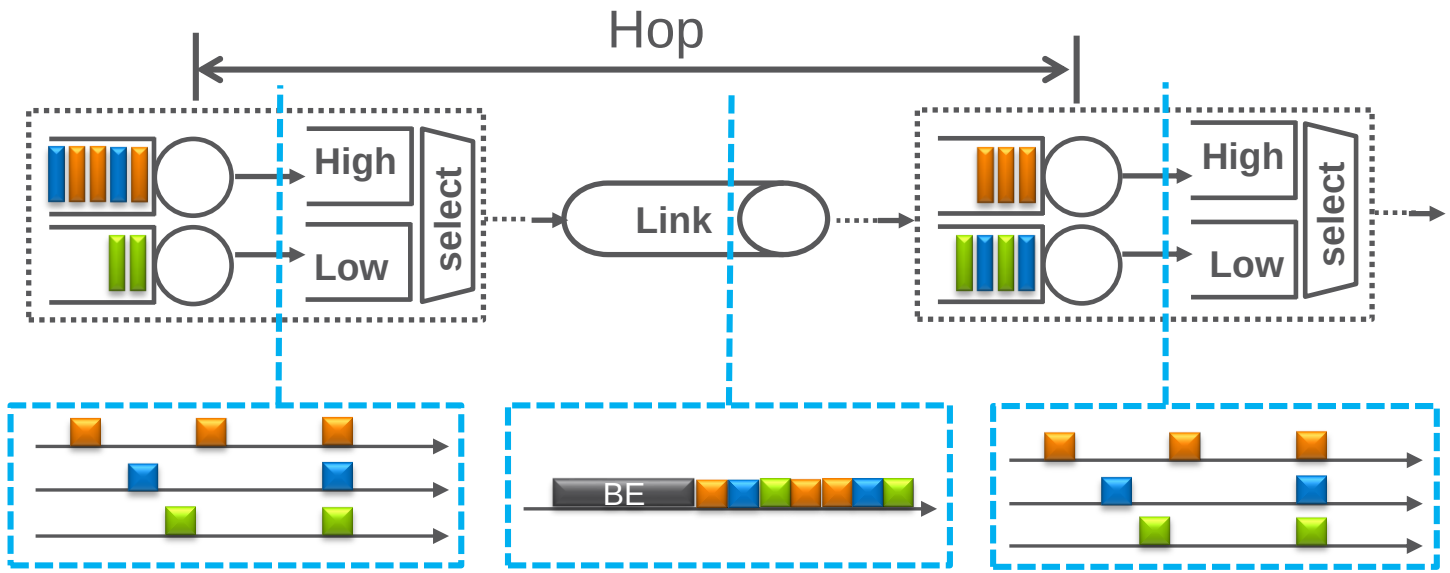


- Problem solved by preemptive sand between the rocks:
  → reduced latency variation for rocks & more bandwidth for sand



Asynchronous Traffic Shaping

- Zero congestion loss without time synchronization
- Asynchronous Traffic Shaping (P802.1Qcr ATS)
  - Smoothen traffic patterns by re-shaping per hop
  - Prioritize urgent traffic over relaxed traffic



SECURITY

Security

- What's different about the car network
- Threats
- Countermeasures

➢ Enrollment, authentication, authorization, ..
  - Knowing what is/what is meant to be attached to the network, where

➢ Data Authenticity and Integrity
  - Knowing received data was transmitted by the apparent source
  - So filters/policers/shapers operate on trustworthy information, doing what they were intended to do

Security: The Car Network

What's different about the car network?

- *As compared to the provider networks, backbone networks, large enterprise and industrial networks 802.1 has worried about in the past*

- Small, simple, though no single blueprint
- Small number of flows
- Severely resource constrained (particularly power)
- Infrequent repair by stopping (roadside or limp home)
  - Can require external network access or equipment
- Network configuration can be/is fixed
  - At least when car is in operation, perhaps by initial build
  - Reliability/redundancy pre-configured/continuously operational

Security: Threats

- Attacks on data recipients *and* resources
  - Including bandwidth allocation and timing for shared links
- Wide range of attached devices
  - Some complex (easily compromised)
  - Some with external access (e.g. infotainment)
  - Problems include accident and misuse as well as malice
  - Can be installed by many different organizations/people
- Vulnerability
  - Some links deliberately open: external sensors, trailer hitches etc.
  - Others might be deemed inaccessible, particularly when car is in motion
  - Conventional to consider attacker's cost/benefit vs alternative attack vectors
  - But 'reputational risk' of new technology may skew calculation
  - Can never defend against 'wire cutting' attacks

Security: Countermeasures

- Separate functions, separate devices
  - Can securely verify device code/config but not easy
- Fixed network configuration and filters
- Enrollment, authentication, authorization, provisioning
  - Know what is connected where and what it is allowed to do
  - Device Identity ➔ Authorized Device
- Data authenticity and integrity
  - Data received was transmitted by claimed source
  - Authorized Device ➔ Data authenticity and integrity
- Apply filters/policers/shapers to known good data
  - Data authenticity and integrity ➔ Data segregation, limitation
  - An attack that can't arrive at the intended target has been effectively dealt with

Security: Enrollment .. provisioning

- Locate the device within the network
  - Don't require separate SKUs per component position
  - Asymmetric VLAN tagging of enrollment/authentication packets
  - Don't trust device's apparent MAC address
- Enrollment and authentication protocol (multiple choices)
  - Supported by 802.1AR X.509 IDevID (Initial Device Identifier)
  - Require Internet (or equivalent) access, assume car stationary
  - Participants: Device, in-car controller, device and car mfr.s
  - Does device belong in this car/compatible with other devices ?
  - Has it been stolen/salvaged/subject to recall ?
  - Install 802.1AR LDevID (Local DevID, can support auth/reauth)
  - Provision device/location dependent & independent addresses/VLANs
  - Provision MACsec CAKs (symmetric crypto keys)

Security: Data Integrity/Authenticity

- MACsec Key Agreement (MKA, 802.1X)
  - MACsec CAKs prove prior authentication/authorization
    - Don't reauth every time ignition switched on
  - Can be used without MACsec data protection for non-vulnerable links
    - But see 'reputational risk'
  - Distributes/refreshes MACsec data protecting keys (SAKs)
- MACsec (802.1AE)
  - Full rate constant delay (TSN friendly) implementations)
  - Integrity only option (where confidentiality not required)
  - Protection and verification hop-by-hop
  - Single hop can skip over switches (e.g. a Provider Network, 802.1AEcg)
    - Viable where full mesh connectivity not required and intermediate links not vulnerable
    - But see 'reputational risk'

SUMMARY

Summary

- Automotive networks have requirements not usually seen in the enterprise
- 802.3 PHYs provide fast start-up, automotive EMC performance, and support smaller, lighter-weight media
- 802.1 provides reliability and deterministic latency
- 802.1 provides security

Q & A

Thank You!

Further Reading

- IEEE Std 802.3bf -2011 Media Access Control (MAC) Service Interface and Management Parameters to Support Time Synchronization Protocols
- IEEE Std 802.3bp -2016 Physical Layer Specifications and Management Parameters for 1 Gb/s Operation over a Single Twisted-Pair Copper Cable (1000BASE-T1)
- IEEE Std 802.3bw -2015 Physical Layer Specifications and Management Parameters for 100 Mb/s Operation over a Single Balanced Twisted Pair Cable (100BASE-T1)
- IEEE Std 802.3br-2016 Specification and Management Parameters for Interspersing Express Traffic
- P802.3.2 (IEEE 802.3cf) YANG Data Model Definitions Task Force
- P802.3cg 10 Mb/s Single Twisted Pair Ethernet Task Force
- P802.3ch Multi-Gig Automotive Ethernet PHY Task Force

Further Reading

- http://www.ieee802.org/1, http://www.ieee802.org/1/pages/tsn.html
- IEEE 802.1 TSN for Automotive – flyer
- Introduction to IEEE 802.1 TSN
- A Time-Sensitive Networking Primer: Putting It All Together
- Heterogeneous Networks for Audio and Video: Using IEEE 802.1 Audio Video Bridging
- Tutorial on IEEE 802.3br Interspersing express traffic (IET) and IEEE 802.1 Time-Sensitive Networking
- Tutorial on Deterministic Ethernet

Further Reading

- IEEE Std 802.1AE-2006 MAC Security
- IEEE Std 802.1AEbn-2011 Amendment: GCM-AES-256 Cipher Suite
- IEEE Std 802.1AEbw-2013 Amendment: Extended Packet Numbering
- IEEE Std 802.1X-2010 Port-Based Network Access Control
- IEEE Std 802.1Xbx-2014 Amendment: MAC Security Key Agreement Protocol (MKA) Extensions
- P802.1AR-Rev/D2.2 Secure Device Identity
- P802.1Xck Amendment: YANG Data Model
- RFC 7030 Enrollment over Secure Transport