# A look at Securing the Automotive Ethernet

Robert Moskowitz
HTT Consulting
July 2016

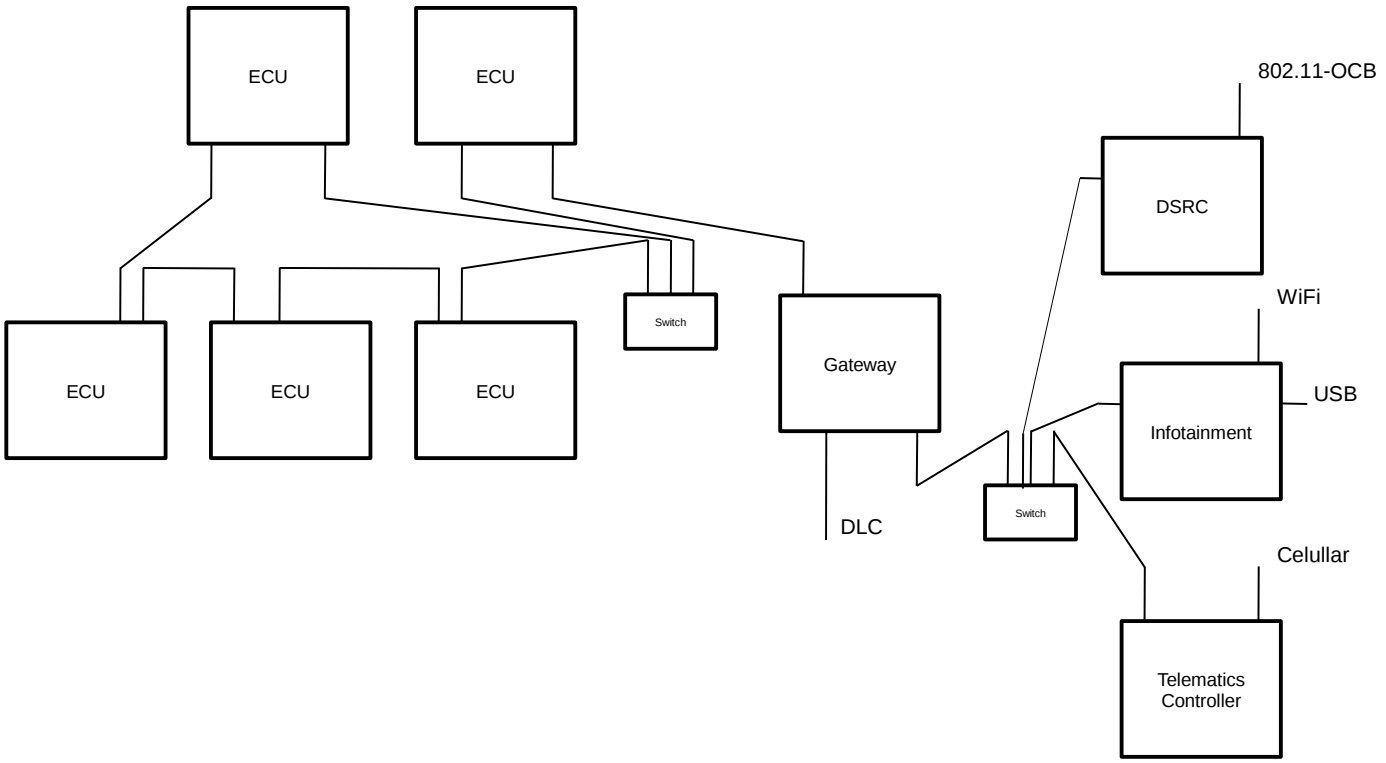
# View of the Network and components

- Two classes of networks
  - Safety Network
  - Infotainment Network
- All Ethernet networks bridged together
  - As one Network
  - Any filtering between 'segments' would have to be by MAC (Layer 2) addresses
  - Excludes diagnostic (DLC) port and WiFi
    - These are separately isolated from ALL other Auto networks by Firewalls and applications

# Purpose of this talk

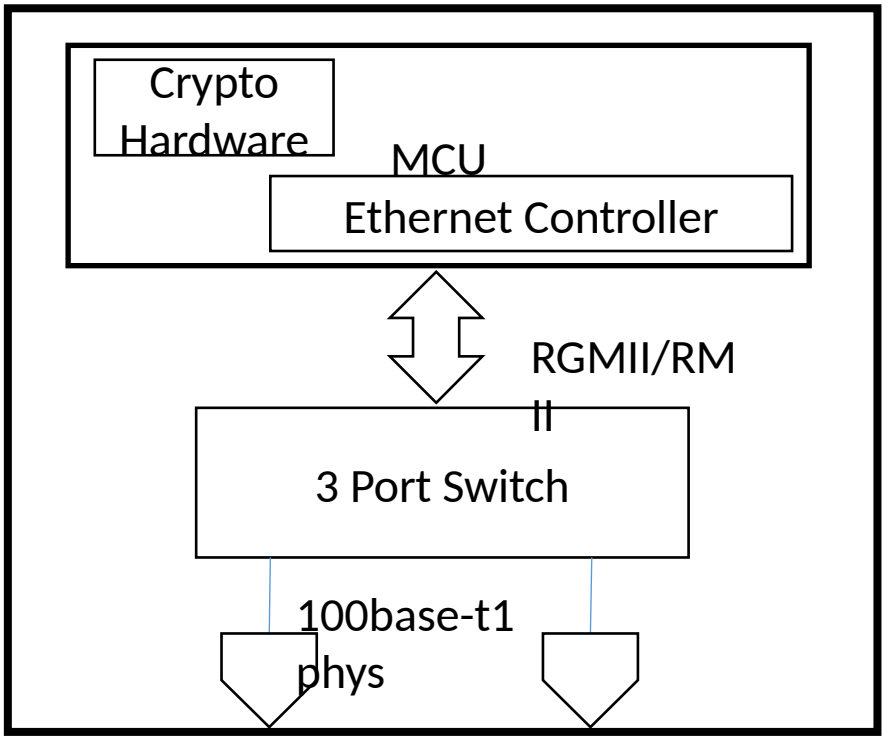
- Review of potential Automotive Ethernet network design and components
- Need for Security at OSI Layer 2 (MAC)
- Identify areas of mismatches between 802.1 standards and constraints of the presented networks.
- Discussion on how to resolve presented challenges.

# Automotive Ethernet(s)



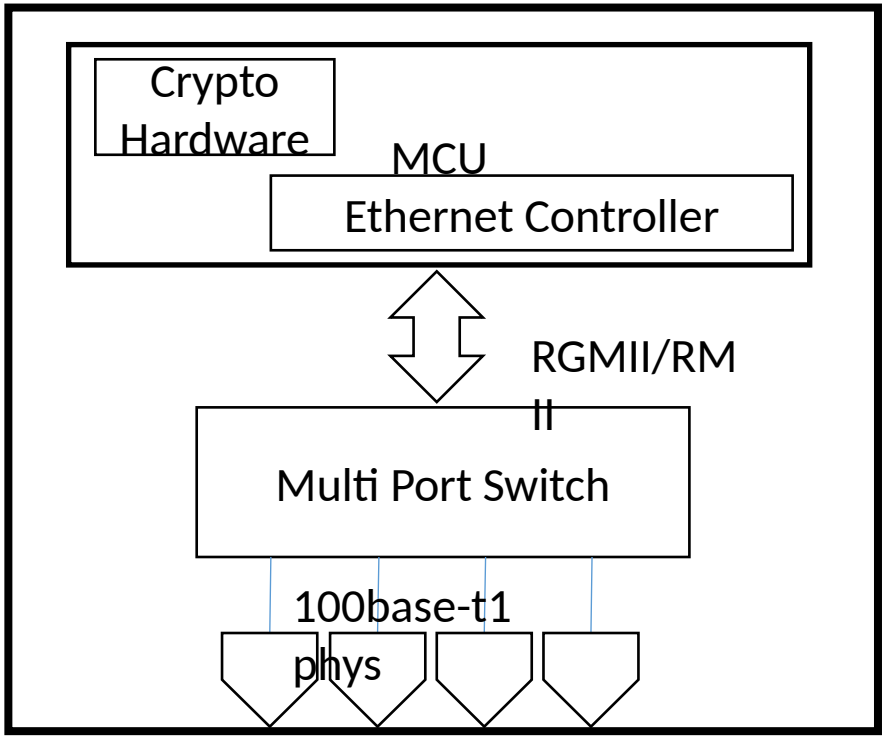

Possible Auto Ethernet with 802.1CB safety ring(s), plus Infotainment/WAN switched segment. All bridged via a Gateway that also brings in CAN and LIN.

# Automotive ECUs



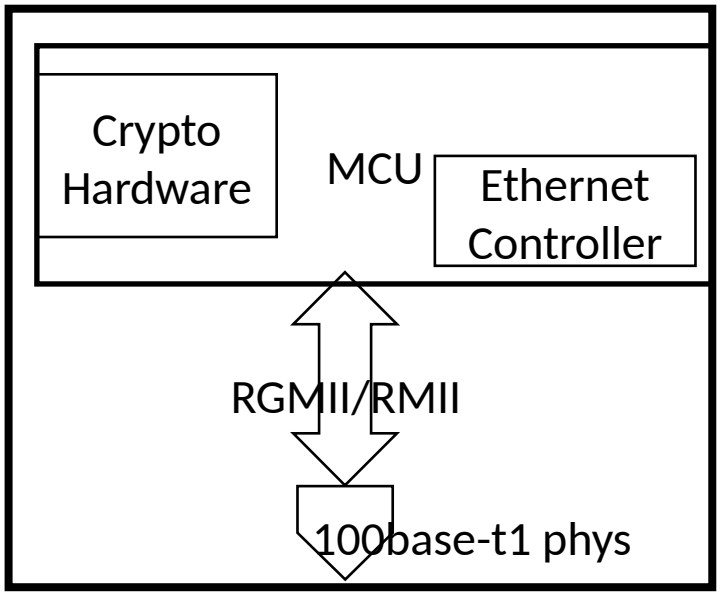

Typical ECU with internal switch

# Automotive ECUs




Main ECU with internal switch

# Automotive ECUs




Simple ECU

# Trust in the Automotive Ethernet

- Only trusted devices
  - How to build trust and maintain it
    - SHE component on CANbus-FD uses knowledge based enrollment and shared master keys
  - Plug-n-Play of consumer devices NOT supported
    - No neat kickstarter LIDAR permitted!
    - Consumer supplied devices on WiFi or USB only
  - Component replacement by certified devices only post production changes
    - New or used

# Trust in the Automotive Ethernet

- All trusted devices will be OEM certified
  - Including ALL field installed devices
  - Trusted to obtain OEM certificates for trusted operation
- Field replacement will ONLY occur with active connection to the OEM Backend security services
  - Via wireless or diagnostic connection
  - No backend connection?  Move vehicle to site with it.

# Trust in the Automotive Ethernet

- Isolate non-trusted devices
  - People will attach devices to the Ethernet if for no other reason than it is there
  - They can inject DDos events
    - Which can be detected and mitigated by trusted devices
  - And can attack and corrupt trusted devices
    - There is little defense against a trusted, yet compromised device

# Trust in the Automotive Ethernet

- Protection for all traffic at all layers
  - Not all messaging is IP-based
    - Nor is all IP messaging assured to be protected
  - Integrity is adequate for some traffic, Confidentiality will be required for some
    - Note even a potential confidentiality requirement for camera feed
      - Ride share
    - Confidentiality for all has performance cost?
  - Plus Ethernet control is non-IP
    - E.G. TSN control plane

# Trust in the Automotive Ethernet

- Cryptographic agility to meet
  - International mandates
    - E.G. China requirements
      - Already providing SMS4 in existing vehicles
  - Advancements in attacks and protections

# Proposed Security Solutions

- IEEE 802.1AE
  - SHE provides AES but not GCM
  - No crypto components for embedded switches
    - Non-trivial cost increase to add crypto
- IEEE 802.1X
  - Need *fast* enabling at engine start
- IEEE 802.1AR
  - Device supplier buy-in
  - IETF anima protocols for enrollment?
  - EDDSA support.  Plus Auto OIDs

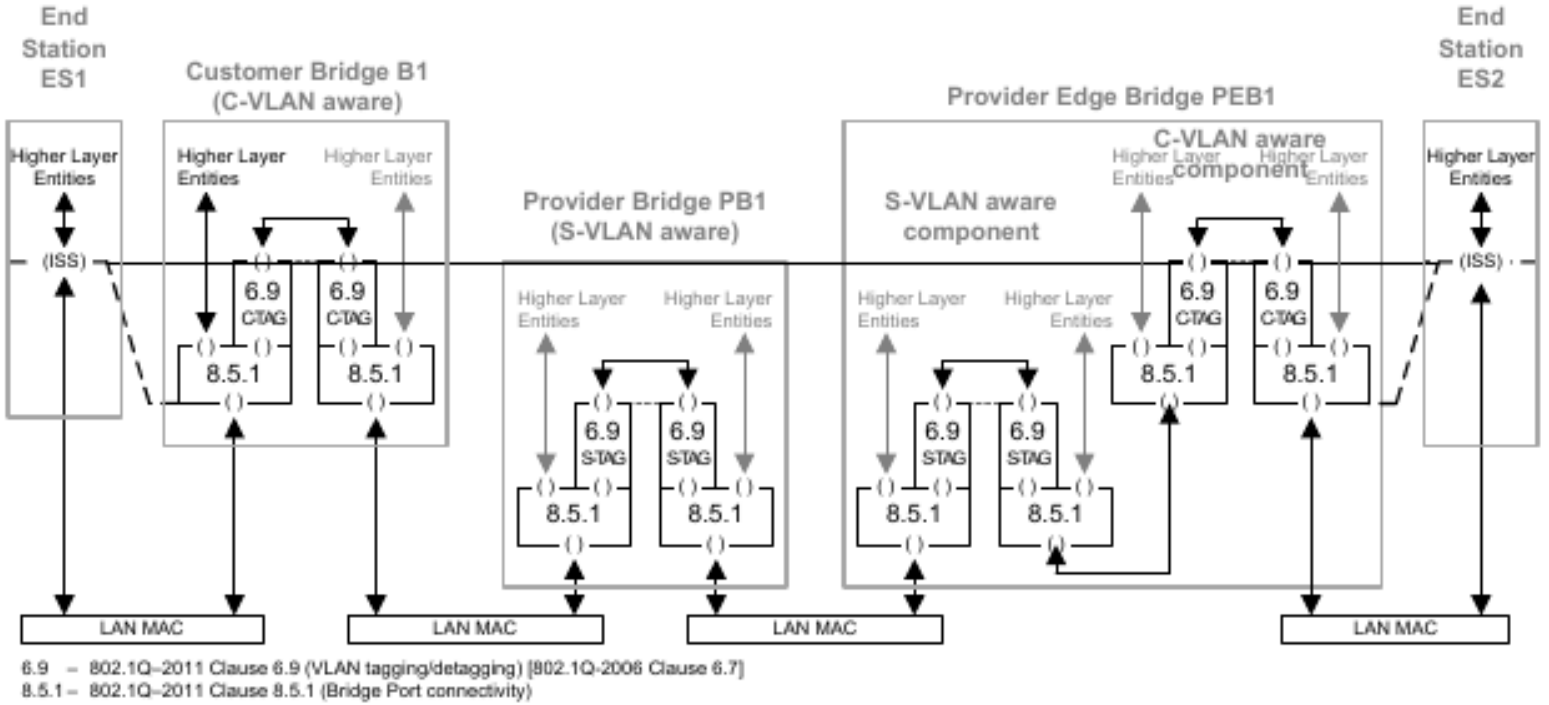
# Recommended Solution Components

- IEEE 802.1AR X.509 Device Identity for separate PKIs for Supplier(s) and OEM
  - Supplier certificate for 'Factory Default' Identity
    - Maintains Supplier involvement with parts
    - And provides reused part initialization methodology
  - OEM certificate is for operational use
  - Third level of PKI possible for Infotainment products
    - Separation of domains of trust
  - Third party Diagnostic units could have LDevID from each OEM!

# Challenges with IEEE Recommendations

- Can embedded switches function similar to provider bridges?
  - 802.1AEcg addendum
- If so can 802.1X flow 'through' switches from ECU to Controllers and/or Gateway?
- What are the affordable options?
- Only AES-GCM in 802.1AE
  - SMS4 support?  Is GCM available with SMS4?

# IEEE 802.1AE across Provider Bridges 802.1AEcg?



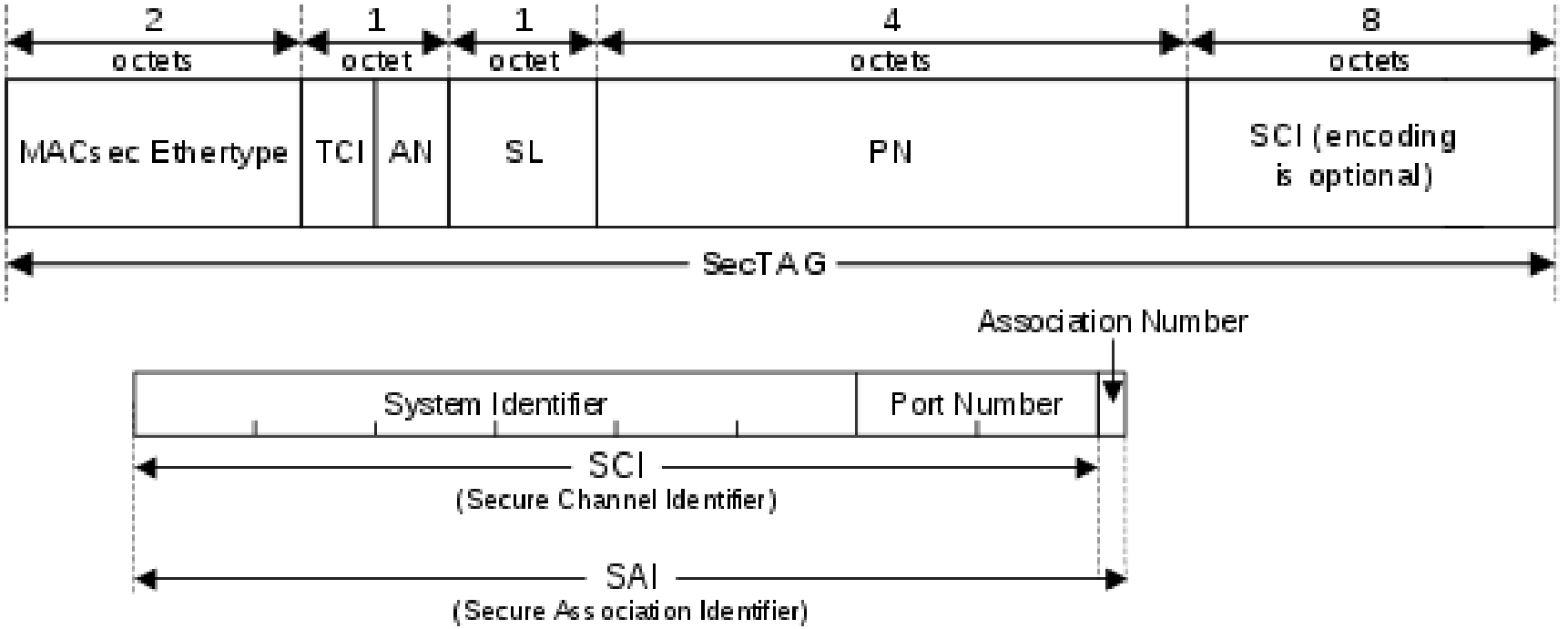

If ECU switches could function as Provider Bridges, then desired functionality achieved?

# Challenges with IEEE Recommendations

- VLAN priority bits used for safety network QOS
  - These are within encrypted payload
  - Each VLAN a 1AE Communications Association with Security Channel identified VLAN
    - Priority bit = SCI port number?

# VLAN prioritization across Provider Bridges

- If encrypted, VLAN priority can be mapped into SCI port number



# Next steps

- Work with 802.1 TG to crystallize any needed additions to the 802.1 security standards
- Follow through with appropriate work efforts

# Questions?