Suggestions for Automotive Profile outline

Norman Finn
Huawei Technologies Co. Ltd
dg-finn-auto-prof-outline-0119-v02

Purpose of this presentation

- This deck is intended to **stimulate thought** within the IEEE 802.1 Time-Sensitive Networking Task Group on how to organize IEEE P802.1DG Automotive In-Vehicle Profile.
- The author has attempted, in this deck, to **capture** as much as possible of the discussion on v01 of this same deck at the IEEE 802.1 TSN meeting on Jan. 10, 2019.
- This deck can thus help to **attract participants** to the TSN meetings and teleconferences to broaden the participation, and thus improve the quality of the Automotive In-Vehicle Profile.

Fundamental questions to answer, first

- Are we describing **one** way to build an in-vehicle network, or a **box of tools** for people designing automotive networks**?**
  - This presentation assumes we want a box of as few tools as possible.
- Are we building relationships (as with P802.1CM ←→ CPRI) with other SDOs who are writing standards that call out P802.1DG**?**
  - This presentation assumes that the answer is, “Yes.”
- How much security do we do**?**
  - This presentation assumes that we will describe some available security features. The industry needs a comprehensive security plan.
- These questions have a big impact on the document. If the above assumed answers are incorrect, this presentation is of questionable value.

Notes

- The toolbox assumption leads this contribution to describe the tools in a bit more detail before dropping into the actual profiles that select among the tools presented. It is even possible that we will want to define tools that no profile requires. **But,**
- The document is a toolbox, not a catalog. We only pick features that are definitely applicable, and do not describe obscure options.
- Security affects all aspects of the document. That's why the Security section is near the front of the document. Security is likely too large a subject to be comprehensively covered in this document. Every clause will refer back to the Security clause.

P802.1DG table of contents

1-4 **IEEE-SA required clauses**

5 **The meat of the standard**

6-7 **Requirements**
8 **(requirements and toolbox)**

9-13 **Toolbox**

14 **The meat of the standard**
C **Requirements**

1. Overview, 2. Normative references, 3. Definitions, 4. Abbreviations
5. Conformance
6. Automotive In-Vehicle Networks
7. Life cycle
8. Security
9. Traffic separation
10. Synchronized time
11. Latency and congestion loss
12. Topology and redundancy
13. Protocols
14. Profiles

C. Informative annex: Safety

1. Overview, 2. Normative references, 3. Definitions, 4. Abbreviations

- These sections, of course, are mandated by the IEEE Standards Association.
- Also:
  - Introduction
  - Table of Contents
  - Annex A: Profile Conformance Statement
  - Annex <last>: Non-normative references
  - Annex Z: Working Group scratch pad

5. Conformance

1. Requirements terminology (explains shall, must, should)
2. PCS: describes use of PCS in Annex A
3. Automotive Bridge
4. Two-port Chained Station (3-port Bridge + end station)
   - This is an example of a device we might define. Too early to say.
5. Automotive end station

- There may be more than one profile defined, in which case the some of 5.3, 5.4, or 5.5 may be doubled.

6. Automotive In-Vehicle Networks

- The purpose of this clause is not historical or simply informative; the purpose is to justify a number of requirements on an automotive in-vehicle Bridged LAN. These requirements will be called out throughout the rest of the document to drive/justify the specifications.

1. Brief introduction to existing in-vehicle networks
   - Including sample architecture to serve for further discussions
2. Interfacing with existing non-Ethernet networking technologies
3. Related standards' requirements on DG (e.g. AutoSAR)
4. Failure mode operations
5. Fast start-up issues
6. Maintenance mode operations
7. Supported physical media
8. Robustness

7. Life cycle

- The network behavior changes greatly over time

1. Component manufacture / test
2. Manufacturing
3. Start-up sequence
4. Normal operation
5. Software updates
6. Fail-safe operation
7. In-shop maintenance

8. Security

- See also “notes”

1. Summary of useful external documents.
2. Threats
3. Cryptographic tools
4. Physical security tools
5. Application of these tools to following sections of this document

9. Traffic separation

1. Separation by VLAN
   - Separating groups of functional units on different VLANs
2. Topology separation
   - Multiple versions of the active topology can share a physical network: MST, SPB, SPB+PCR, configuration, network manager.
3. Physical separation
   - Separating groups of functional units on different LANs.
4. Connectivity by router
   - Selectively connecting different groups by IETF routing
5. Connectivity by application gateway
   - Selectively connecting different groups above the frame/packet layers.

10. Synchronized time

1. Precision Time Protocol
   - Pick a profile and options
2. Robust and Secure PTP (Crypto is not enough!)
   - Certainly, 802.1AS-2019 will be useful.
   - Perhaps we call out an RFC.

11. Latency and congestion loss

1. Best effort flows
2. Continuous vs. Intermittent flows
   - Intermittent flows can be scheduled. Hard to mix both types on same port.
3. Time scheduling for intermittent flows.
4. Bounded latency, zero congestion loss
   - Pick queuing method(s) for continuous flows.
5. Frame preemption
6. Cut-through forwarding
7. Separation by time (802.1Qbv)
8. Separation by traffic class
9. Filtering and policing (so that misbehavior cannot ruin latency)

12. Topology and redundancy

1. Physical topology verification and/or determination
   - Does the physical topology match expectations?
2. Best-effort active topology determination
   - Pick one: MST, SPB, none (no loops) or a non-802.1 ring protocol.
3. Critical flow active topology determination
   - Pick one: None (no loops), FRER paths, or a non-802.1 ring protocol.
4. Frame Replication and Elimination for Reliability (FRER)
   - End-to-end, not ladder. Pick one: Configuration, SPB+PCR, net manager.
5. End station duplication.
   - Impact on the network, relationship to FRER.

13. Protocols

1. Other IEEE 802 protocols required
   - One section for each protocol. 802.1AX? LLDP? Ether OAM? CFM?
2. Configured reservations for TSN flows
   - This will certainly be required. Where do addresses come from? (9.1?)
3. Reservations made by network controller
   - Pick one: NETCONF? RESTCONF? SNMP? Application controller?
4. Reservations made by peer-to-peer protocols
   - Or not. If allowed, RAP? MSRP? A variant of either?

14. Profiles

- One or two (hopefully one) profiles, for devices conformant to Clause 5, that will meet the needs of a significant market.

1. Profile 1
    1. Overview
    2. Selection of tools
    3. Specific profile parameters
2. Profile 2 …

C. (Informative annex) Safety

Thank you