IEEE 802 LAN/MAN STANDARDS COMMITTEE (LMSC)

CRITERIA FOR STANDARDS DEVELOPMENT (CSD)

Based on IEEE 802 LMSC Operations Manuals approved 15 November 2013
Last edited 20 January 2014

1. IEEE 802 criteria for standards development (CSD)

The CSD documents an agreement between the WG and the Sponsor that provides a description of the project and the Sponsor's requirements more detailed than required in the PAR. The CSD consists of the project process requirements, 1.1, and the 5C requirements, 0.

1.1 Project process requirements

1.1.1 Managed objects

Describe the plan for developing a definition of managed objects. The plan shall specify one of the following:

a) The definitions will be part of this project.
b) The definitions will be part of a different project and provide the plan for that project or anticipated future project.
c) The definitions will not be developed and explain why such definitions are not needed.

This project will use method a, adding to or modifying the managed objects already in IEEE Std 802.1Q-2014.

1.1.2 Coexistence

A WG proposing a wireless project shall demonstrate coexistence through the preparation of a Coexistence Assurance (CA) document unless it is not applicable.

a) Will the WG create a CA document as part of the WG balloting process as described in Clause 13? (yes/no)
b) If not, explain why the CA document is not applicable.

This project is not a wireless project.

1.2 5C requirements

1.2.1 Broad market potential

Each proposed IEEE 802 LMSC standard shall have broad market potential. At a minimum, address the following areas:

a) Broad sets of applicability.
b) Multiple vendors and numerous users.

While a specific market segment (Automotive Networking) triggered the initiation of this project, the capabilities are applicable on all TSN markets, which has certainly proven broad enough to justify TSN standards. A large fraction of the vendors participating in TSN are offering and/or developing products in this area. Broad industrial network control systems, Mission critical systems as found in, but not limited to, current and next generation Automotive Systems require low and predictable latencies while utilizing reliable transport and avoiding common

cause failure dependencies. Automotive and Industrial network control market segments are in the order of hundreds of millions nodes, similar in size as that of information technology segments.

1.2.2 Compatibility

Each proposed IEEE 802 LMSC standard should be in conformance with IEEE Std 802, IEEE 802.1AC, and IEEE 802.1Q. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with IEEE 802.1 WG prior to submitting a PAR to the Sponsor.

a) Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?
b) If the answer to a) is no, supply the response from the IEEE 802.1 WG.

As an amendment to 802.1Q, compatibility is assured.

The review and response is not required if the proposed standard is an amendment or revision to an existing standard for which it has been previously determined that compliance with the above IEEE 802 standards is not possible. In this case, the CSD statement shall state that this is the case.

1.2.3 Distinct Identity

Each proposed IEEE 802 LMSC standard shall provide evidence of a distinct identity. Identify standards and standards projects with similar scopes and for each one describe why the proposed project is substantially different.

As a straightforward extension of 802.1Q VLAN Bridge capabilities, its distinct identity is assured. No similar IEEE 802 standard capabilities are known to IEEE 802.1.

This project differs from existing and ongoing 802.1Q mechanisms as follows:

- 802.1Q-2014 FQTSS, formerly 802.1Qav, does not incorporate the achieved level of isolation among malicious devices nor does it provide the achieved Quality of Service
- 802.1Qch and 802.1Qbv depends on the reliability and availability of clock synchronization, does not achieve similar high link utilizations and, in case of 802.1Qbv, requires network-wide TDMA configuration/planning
- 802.1Qci (ingress policing) can complement the aforementioned egress mechanisms to improve reliability. However, as an independent ingress mechanism, it degrades effective QoS of 802.1Q-2014 FQTSS by introducing “safety margins”

1.2.4 Technical Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence that the project is technically feasible within the time frame of the project. At a minimum, address the following items to demonstrate technical feasibility:

a) Demonstrated system feasibility.
b) Proven similar technology via testing, modeling, simulation, etc.

The technical feasibility has been demonstrated by dedicated analysis. Moreover, feasibility has been shown by modeling and simulation (see http://www.ieee802.org/1/files/public/docs2015/new-tsn-specht-ubs-queues-0521-v0.pdf).

This project is based on mature virtual LAN bridging and transmit selection and scheduling.

The project can be related to IETF Integrated Services and IETF Differentiated Services/Class based Service in 802.1Q, both shown to be feasible. The intended mechanism reaches QoS levels achievable with per flow queueing mechanisms (typically found in the Integrated Service Model) but at significant lower implementation complexity.

1.2.5 Economic Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence of economic feasibility. Demonstrate, as far as can reasonably be estimated, the economic feasibility of the proposed project for its intended applications. Among the areas that may be addressed in the cost for performance analysis are the following:

a) Balanced costs (infrastructure versus attached stations).
b) Known cost factors.
c) Consideration of installation costs.
d) Consideration of operational costs (e.g., energy consumption).
e) Other areas, as appropriate.

The well-established balance between infrastructure and attached stations will not be changed by this enhancement.

The cost factors, including installation and operational factors, are well known from similar technologies and proportional to the benefits gained.

Providing hard real-time guarantees combined with fault isolation and common cause failure avoidance promises to significantly reduce the operational costs of a cyber-physical system.