# Draft Standard for Local and metropolitan area networks—

# Time-Sensitive Networking for Aerospace Onboard Ethernet Communications

Unapproved draft, prepared by the
**Time-Sensitive Networking (TSN) Task Group of IEEE 802.1**

Sponsored by the
**LAN/MAN Standards Committee**
**of the**
**IEEE Computer Society**

**This and the following cover pages are not part of the draft.** They provide revision and other information for IEEE 802.1 Working Group members and participants in the IEEE Standards Association ballot process, and will be updated as convenient. New participants: Please read these cover pages, they contain information that should help you contribute effectively to this standards development project. Blank pages allow for the addition of cross-references to changed text without forcing renumbering of all pages in the draft. Pages are numbered from 1 (including cover pages) for the convenience of reviewers whose PDF viewers do not easily accommodate different numbering sequences. Pages will of course be renumbered prior to publication.

The text proper of this draft begins with the Title page.

# Editors' Foreword

This draft is prepared for the second task group ballot.

# Participation in 802.1 standards development

All participants in the standardization activities of IEEE 802.1 should be aware of the Working Group Policies and Procedures, and the fact that they have obligations under the IEEE Patent Policy, the IEEE Standards Association (SA) Copyright Policy, and the IEEE SA Participation Policy. For information on these policies see 1.ieee802.org/rules/ and the slides presented at the beginning of each of our Working Group and Task Group meeting.

As part of our IEEE 802® process, the text of the PAR (Project Authorization Request) and CSD (Criteria for Standards Development) of each project is reviewed regularly to ensure their continued validity. The PAR is summarized in these cover pages and a links are provided to the full text of both PAR and CSD. A vote of "Approve" on this draft is also an affirmation that the PAR and CSD for this project are still valid.

Comments on this draft are encouraged. NOTE: All issues related to IEEE standards presentation style, formatting, spelling, etc. are routinely handled between the 802.1 Editor and the IEEE Staff Editors prior to publication, after balloting and the process of achieving agreement on the technical content of the standard is complete. Readers are urged to devote their valuable time and energy only to comments that materially affect either the technical content of the document or the clarity of that technical content. Comments should not simply state what is wrong, but also what might be done to fix the problem.

Full participation in the work of IEEE 802.1 requires attendance at IEEE 802 meetings. Information on 802.1 activities, working papers, and email distribution lists etc. can be found on the 802.1 Website:

http://ieee802.org/1/

Use of the email distribution list is not presently restricted to 802.1 members, and the working group has a policy of considering comments from all who are interested and willing to contribute to the development of the draft. Individuals not attending meetings have helped to identify sources of misunderstanding and ambiguity in past projects. The email lists exist primarily to allow the members of the working group to develop standards, and are not a general forum. All contributors to the work of 802.1 should familiarize themselves with the IEEE patent policy and anyone using the email distribution list will be assumed to have done so. Information can be found at http://standards.ieee.org/db/patents/

Comments on this draft may be sent to the 802.1 email exploder, to the Editor, or to the Chairs of the 802.1 Working Group and Time-Sensitive Networking (TSN) Task Group.

Abdul Jabbar
Editor, P802.1DP
Email:jabbar@ge.com

Janos Farkas
Chair, 802.1 TSN Task Group
Email:Janos.Farkas@ericsson.com

Glenn Parsons
Chair, 802.1 Working Group
+1 514-379-9037
Email: glenn.parsons@ericsson.com

NOTE: Comments whose distribution is restricted in any way cannot be considered, and may not be acknowledged.

**All participants in IEEE standards development have responsibilities under the IEEE patent policy and should familiarize themselves with that policy, see http://standards.ieee.org/about/sasb/patcom/materials.html**

As part of our IEEE 802 process, the text of the PAR and CSD (Criteria for Standards Development, formerly referred to as the 5 Criteria or 5C's) is reviewed on a regular basis in order to ensure their continued validity. A vote of "Approve" on this draft is also an affirmation by the balloter that the PAR is still valid.

# Draft development

During the early stages of draft development, 802.1 editors have a responsibility to attempt to craft technically coherent drafts from the resolutions of ballot comments and from the other discussions that take place in the working group meetings. Preparation of drafts often exposes inconsistencies in editor's instructions or exposes the need to make choices between approaches that were not fully apparent in the meeting. Choices and requests by the editors' for contributions on specific issues will be found in the editors' Introduction to the current draft and at appropriate points in the draft.

The ballot comments received on each draft, and the editors' proposed and final disposition of comments on working group drafts, are part of the audit trail of the development of the standard and are available, along with all the revisions of the draft on the 802.1 website (for address see above).

During the early stages of draft development the proposed text can be moved around a great deal, and even minor rearrangement can lead to a lot of 'change', not all of which is noteworthy from the point of the reviewer, so the use of automatic change bars is not very effective. In early drafts change bars may be omitted or applied manually, with a view to drawing the readers attention to the most significant areas of change. Readers interested in viewing every change are encouraged to use Adobe Acrobat to compare the document with their selected prior draft. Note that the FrameMaker change bar feature is useless when it comes to indicating changes to Figures.

# PAR (Project Authorization Request) and CSD

Extracts from the PAR, as approved by IEEE NesCom 3rd December 2020:

https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8705

and the CSD (Criteria for Standards Development):

https://mentor.ieee.org/802-ec/dcn/21/ec-21-0096-00-ACSD-p802-1dp.pdf

follow.

This is a joint development with:

SAE Avionics Networks AS-1 A2 IEEE and SAE Joint Development Procedure.[1]

**PAR Scope:**

This standard specifies profiles of IEEE 802.1 Time-Sensitive Networking (TSN) and IEEE 802.1 Security standards for aerospace onboard bridged IEEE 802.3 Ethernet networks. The profiles select features, options, configurations, defaults, protocols, and procedures of bridges, end stations, and Local Area Networks to build deterministic networks for aerospace onboard communications.

**PAR Purpose:**

This standard specifies profiles for designers, implementers, integrators, and certification agencies of deterministic IEEE 802.3 Ethernet networks that support a broad range of aerospace onboard applications including those requiring security, high availability and reliability, maintainability, and bounded latency.

**PAR Need for the Project:**

The aerospace segment does not have profiles of IEEE 802.1 TSN standards. The lack of standardized TSN profiles makes the definition of the aerospace manufacturers requirements and the implementation of those requirements by suppliers more difficult and costly. Thus, there is a need to standardize the selection and use of IEEE 802.1 and IEEE 802.3 standards and features in order to be able to deploy secure, highly-reliable converged networks, and enable certification as a basis for compliance and design assurance.

**CSD managed objects [extract]**

…managed object…definitions will not be developed…because this project will specify profiles that define the use and configuration of functions specified in other IEEE 802 standards, thus relying on the managed objects specified by the referred standards. [Partial extract from the CSD].

**CSD broad market potential [extract]**

IEEE 802.1 Time-Sensitive Networking (TSN) gives an opportunity to unify networking for aerospace onboard Ethernet communications. TSN is the foundation to provide interoperability and connectivity for aerospace applications on converged networks to support traffic that has high-reliability and deterministic latency requirements. However, the breadth of choices in the use of the TSN features inhibits the interoperability of products designed for a particular market. By narrowing the focus, this profile expands the market for bridges, end stations, network interface cards, and integrated circuits. The specification and use of TSN features in these scenarios via TSN profiles is beneficial for suppliers offering and/or developing TSN products, e.g., in order to ease interoperability and deployment.

Many aerospace manufacturers, suppliers, and customers consider TSN as the next generation networking technology enabler to meet the deterministic latency, security, and high reliability requirements of aerospace onboard networks. The TSN profiles for aerospace are essential for them.

**CSD compatability [extract]**

The project will comply with IEEE Std 802, IEEE Std 802.1AC, and IEEE Std 802.1Q.

[1] https://www.ieee802.org/1/files/private/dp-drafts/IEEE-SAE_Joint_Dev_Procedure-TSN_Aerospace_Profile.pdf

# Introduction to the current draft

**This introduction is not part of the draft, and will be revised for SA ballot. A set of cover pages will be retained for use during SA ballot.**

This is the second draft of P802.1DP. Both technical and editorial comments are welcome. Reviewers are encouraged to provide “suggested remedy” when providing a comment. This draft addresses the comments from previous task group ballot according to the comment disposition document

This page intentionally left blank.

This page intentionally left blank.

**P802.1DP/Draft 1.1**

**December 29, 2023**

# Draft Standard for Local and metropolitan area networks—

# Time-Sensitive Networking for Aerospace Onboard Ethernet Communications

Unapproved draft, prepared by the

**Time-Sensitive Networking (TSN) Task Group of IEEE 802.1**

Sponsored by the

**LAN/MAN Standards Committee**
**of the**
**IEEE Computer Society**



IEEE Standards Activities Department
445 Hoes Lane
Piscataway, NJ 08854, USA

**Abstract:** This standard specifies a profiles of IEEE 802.1 Time-Sensitive Networking (TSN) for aerospace onboard bridged IEEE 802.3 Ethernet networks. The profile selects features, options, configurations, defaults, protocols, and procedures of bridges, end stations, and Local Area Networks to build deterministic networks for aerospace onboard communications.

**Keywords:** Bridged Network, IEEE 802.1Q™, LAN, local area network, MAC security, MACsec, privacy, Virtual Bridged Network, virtual LAN, VLAN Bridge

---

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA



Print: ISBN 978-X-XXX-XXX-X STDXXXXX
PDF: ISBN 978-X-XXX-XXX-X STDPDXXXXX

# Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

## Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

## Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

## Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

## Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[2]

## Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

## Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

1. Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
2. Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

## Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

## Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

## Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

## Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

## Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.[5]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the

3. Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.
4. Available at: https://standards.ieee.org/standard/index.html.
5. Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

IEEE SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

## IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

# Participants

<<The following lists will be updated in the usual way prior to publication>>

At the time this standard was completed, the IEEE 802.1 working group had the following membership:

**Glenn Parsons,** *Chair*
**Jessy Rouyer,** *Vice Chair*
**Janos Farkas,** *Security Task Group Chair*
**Abdul Jabbar,** *Editor*

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

A.N. Other

<<The above lists will be updated in the usual way prior to publication>>

When the IEEE-SA Standards Board approved this standard on <dd> <month> <year>, it had the following membership:

*Chair*
*Vice-Chair*
*Past Chair*
*Secretary*

*Member Emeritus

<<The above lists will be updated in the usual way prior to publication>>

# Introduction

This introduction is not part of IEEE Std 802.1DP-20XX, IEEE Standard for Local and metropolitan area networks—Time-Sensitive Networking for Aerospace Onboard Ethernet Communications

This standard specifies profiles of IEEE 802.1 Time-Sensitive Networking (TSN) and IEEE 802.1 Security standards for aerospace onboard bridged IEEE 802.3 Ethernet networks.

This standard was first published as IEEE Std 802.1DP-20XX.

This standard contains state-of-the-art material. The area covered by this standard is undergoing evolution. Revisions are anticipated within the next few years to clarify existing material, to correct possible errors, and to incorporate new related material. Information on the current revision state of this and other IEEE 802 standards may be obtained from

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854-4141
USA

# Contents

# Figures

# Tables

# Draft Standard for Local and Metropolitan Networks —

# Time-Sensitive Networking for Aerospace Onboard Ethernet Communications

# 1. Overview

The standardization of Ethernet communication technology in IEEE Std 802.3™, specifying transmission over the physical media of individual Local Area Networks (LANs), and in IEEE Std 802.1Q™, specifying Bridges that interconnect IEEE 802® LANs,[1] has facilitated widespread deployment of networks that connect significantly more end stations, with significantly greater bandwidth, and at significantly reduced cost compared to prior technology. All these metrics have been improved by several orders of magnitude—reducing costs through the multi-vendor provision of common components (bridges, end station interfaces, integrated circuit and circuit designs, connectors, and software) for a wide range of network applications.

The use of Ethernet communication technology in networks with high-reliability and deterministic latency requirements is further supported by Time-Sensitive Networking (TSN) provisions in IEEE Std 802.1Q, IEEE Std 802.1AS, IEEE Std 802.1CB, and the security provisions in IEEE Std 802.1AE and IEEE Std 802.1X. The provisions in these standards can be used in various ways, and include options that address different network requirements and parameters that vary by network and application scale. Network design, time to deploy, and component development, selection, validation, and configuration for a particular network can all benefit from consistent choices, across similar networks and network applications, of the provisions, parameters, and options specified in the relevant standards. A set of such choices comprises a *profile* of those standards and target networks.

This standard is a profile for use in Ethernet networks supporting aerospace onboard communications. These networks and their network components have stringent verification requirements, so the profile emphasizes not just what capabilities are to be available and how they are used, but also what optional capabilities are not used. All available capabilities can be subject to time-consuming and expensive verification, so omission of unused capabilities is desirable and can be required.

## 1.1 Scope

This standard specifies profiles of IEEE 802.1 Time-Sensitive Networking (TSN) and IEEE 802.1 Security standards for aerospace onboard bridged IEEE 802.3 Ethernet networks. The profiles select features, options, configurations, defaults, protocols, and procedures of bridges, end stations, and Local Area Networks to build deterministic networks for aerospace onboard communications.

## 1.2 Purpose

This standard specifies profiles for designers, implementers, integrators, and certification agencies of deterministic IEEE 802.3 Ethernet networks that support a broad range of aerospace onboard applications including those requiring security, high availability and reliability, maintainability, and bounded latency.

## 1.3 Introduction

The TSN suite of standards are broad ranging, and intended for use in a variety of environments that require bounded latency, synchronization, reliability, isolation, and high availability. This standard selects the TSN features that are directly applicable to Aerospace Onboard Ethernet Communications and explains how the associated TSN standards are used. This standard narrows the focus from the broad set of available TSN features to those that are applicable to aerospace onboard networks.

The profile describes aerospace use cases and associated functional requirements to explain how TSN is expected to be used in aerospace platforms. The conformance clause, Clause 5, specifies mandatory and

[1] IEEE and IEEE 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

optional features that are expected to be provided by conformant implementations of systems, system components, and system functions used in aerospace onboard Ethernet networks.

Aerospace OEMs and suppliers at all tiers should be able to use this standard to specify and design the network and network components required to implement the systems and functions required by aerospace platforms. Component and technology suppliers are expected to benefit by understanding which TSN features are required to allow OEMs and higher-tier suppliers to implement conformant aerospace onboard networks.

# 2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in the text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 802®, IEEE Standard for Local and metropolitan area networks: Overview and Architecture.[2,3]

IEEE Std 802.1AC™, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

IEEE Std 802.1AS™, IEEE Standard for Local and metropolitan area networks—Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks.

IEEE Std 802.1CB™, IEEE Standard for Local and metropolitan area networks—Frame Replication and Elimination for Reliability.

IEEE Std 802.1Q™, IEEE Standard for Local and metropolitan area networks—Bridges and Bridged Networks.

IEEE Std 802.3™, IEEE Standard for Ethernet.

IEEE Std 1588™, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

IETF RFC 7950, The YANG 1.1 Data Modeling Language, August 2016.

IETF RFC 8343, A YANG Data Model for Interface Management, March 2018.

[2] IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://standards.ieee.org/).
[3] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

# 3. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[4]

This standard makes use of the following terms defined in IEEE Std 802.

*<<Editor’s Note: The following definitions are reproduced from IEEE Std 802.1Q here to ease the readability of this standard. These definitions cannot be changed within the scope of this document>>*

**end station:** A functional unit in an IEEE 802® network that acts as a source of, and/or destination for, link layer data traffic carried on the network.

NOTE—An end station (or end station functionality in an intermediate system, e.g., in a bridge) is characterized by the use of an individual MAC address assigned to that end station as the source address of frames originating from that end station and reception of frames with that destination MAC address.

**Frame:** A unit of data transmission on an IEEE 802 Local Area Network (LAN) that conveys a Media Access Control (MAC) Protocol Data Unit (MPDU).

This standard makes use of the following terms defined in IEEE Std 802.1Q.

**Centralized Network Configuration (CNC):** A centralized component that configures network resources on behalf of TSN applications (users).

**Centralized User Configuration (CUC):** A centralized entity that discovers end stations, retrieves end station capabilities and user requirements, and configures TSN features in end stations.

**Media Access Control (MAC) Bridge:** A Bridge that does not recognize Virtual Local Area Network (VLAN) tagged frames.

**packet:** A protocol data unit, comprising data, addressing, and protocol identification information, sent by an instance of an identified class of protocol entities and transmitted in one or more frames (e.g., an IPv6 packet).

**policing:** A process of monitoring network traffic and deliberately dropping frames that are in excess of previously defined criteria.

**Stream:** A unidirectional flow of data (e.g., audio and/or video) from a Talker to one or more Listeners.

**Tagged frame:** A frame that contains a tag header immediately following the Source MAC Address field of the frame.

**Talker:** The end station that is the source or producer of a stream.

The following terms are specific to this standard:

**onboard:** A system, systems or that is, or are, permanently installed on the aerospace platform. This does not include test or instrumentation systems or systems installed on the ground to support platform operations.

**traffic:** A sequence of frames forwarded in a network.

**time-aware:** An adjective to describe use of time that is synchronized with other stations using a protocol (e.g., IEEE Std 802.1AS).

[4] *IEEE Standards Dictionary Online* is available at https://dictionary.ieee.org.

# 4. Abbreviations and acronyms

*<< Editor's Note: The list of abbreviations are reproduced from IEEE Std 802.1Q to improve the readability of this standard.>>*

The following abbreviations and acronyms are used in this standard: [5]

| | |
|---|---|
| ATS | Asynchronous Traffic Shaping |
| AV | Audio/Video |
| BNF | Backus-Naur Form |
| CBS | Credit Based Shaper |
| C-DA | Customer Destination MAC address |
| C-TAG | C-VLAN tag |
| C-VID | Customer VLAN Identifier |
| C-VLAN | Customer Virtual Local Area Network |
| CFM | Connectivity Fault Management |
| CID | Company ID [6] |
| CNC | Centralized Network Configuration |
| CUC | Centralized User Configuration |
| DAL | Design/Development Assurance Level |
| DoS | Denial of Service |
| FTTM | Fault-Tolerant Timing Module |
| GM | Grand Master |
| IP | Internet Protocol |
| LAN | Local Area Network (IEEE Std 802) |
| LLC | Logical Link Control |
| MAC | Medium Access Control |
| NETCONF | Network Configuration Protocol |
| PICS | Protocol Implementation Conformance Statement |
| PTP | Precision Time Protocol (IEEE Std. 1588) |
| QoS | Quality of Service |
| TAS | Time Aware Shaper |
| TSN | Time-Sensitive Networking |
| YANG | Yet Another Next Generation [7] |

[5] The abbreviations listed include those defined in standards referenced by this profile and used in this profile.

[6] See https://standards.ieee.org/develop/regauth/tut/eui.pdf.

[7] YANG is best viewed as a name, not an acronym.

# 5. Conformance

This clause specifies mandatory and optional capabilities provided by conformant implementations of systems, system components, and system functions for use in aerospace onboard Ethernet communications. Clause 6 describes the networks and attached devices that are the subject of the specified profiles, and requirements that are particular to, or emphasized in, aerospace applications. Clause 7 maps the functional requirements introduced to the provisions of individual standards. Clause 8 specifies conformant profiles in line item detail by reference to those standard, and is referenced by this clause.

## 5.1 Requirements terminology

For consistency with existing IEEE and IEEE 802.1™ standards, requirements are expressed using the following terminology: [8]

a) ***Shall*** is used for mandatory requirements.
b) ***May*** is used to describe implementation or administrative choices ("may" means "is permitted to," and hence, "may" and "may not" mean precisely the same thing).
c) ***Should*** is used for recommended choices (the behaviors described by "should" and "should not" are both permissible but not equally desirable choices).

Protocol Implementation Conformance Statements (PICS) reflect the occurrences of the words "shall," "may," and "should" within the standard.

The standard avoids needless repetition and apparent duplication of its formal requirements by using ***is***, ***is not***, ***are***, and ***are not*** for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementer or administrator, or whose conformance requirement is detailed elsewhere, is described by ***can***. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by ***cannot***. The word ***allow*** is used as a replacement for the phrase "Support the ability for," and the word ***capability*** means "can be configured to."

## 5.2 Protocol Conformance Statement (PCS)

A claim of conformance to a profile specified in this standard attests to the implementation of a system, system component, or system functionality specified in referenced standards with the profile's selection of, and constraints upon, system parameters and options.

The supplier of an implementation that is claimed to conform to this standard shall provide the information necessary to identify both the supplier and the implementation, and shall complete a copy of the relevant PCS proforma provided in this standard together with the Protocol Implementation Conformance Statements (PICS) for the referenced standards, as identified in the PCS.

## 5.3 Conformance Classes

This profile includes conformance requirements and options for bridges and end stations that support a multitude of aerospace use cases. While some TSN features are required for certain use cases, the use of such features may be non-optimal in other use cases. Therefore, this standard defines two profiles applicable

[8] Originally derived from ISO/IEC style requirements, and consistent with the terminology specified in the ISO/IEC Directives Part 2:2021, Clause 7 (http://www.iec.ch/members_experts/refdocs).

to end stations and Bridge components. The Asynchronous profile defines an aerospace profile that is targeted towards implementations that do not support time synchronization and TSN features that are dependent on time synchronization. The Synchronous profile defines the requirements for aerospace networks that support both synchronous and asynchronous TSN features. In this regard, a device conformant to synchronous profile also supports requirements defined in asynchronous profile. The Asynchronous profile, is therefore a subset of Synchronous profile.

In each profile, this standard recognizes two types of devices, herein defined as Type 1 and Type 2, to distinguish more capable devices with abundant resources from less capable devices that are often resource constrained. Both types of classes apply to the two profiles, resulting in total of 4 potential conformance classes for each conformant component: Asynchronous Type1, Asynchronous Type2, Synchronous Type1, and Synchronous Type2. Aerospace use cases may include a mixture of Type 1 and Type 2 conformant devices as needed to provide the required system capabilities.

### 5.3.1 Type1 Conformance Class

The Type 1 conformance class imposes fewer requirements than the Type 2 conformance class and is expected to be used for smaller and less performant systems and those that have tighter cost constraints.

### 5.3.2 Type2 Conformance Class

The Type 2 conformance class imposes more requirements than the Type 1conformance class and is expected to be used for higher performant and larger systems.

Note: Potential aerospace deployments may use both Type1 and Type2 conformant devices in the same vehicle based on the system requirements.

*<< Editor’s Note: Comments to include additional base requirements from 802.1Q along with justification for inclusion are invited.>>*

## 5.4 Bridge component requirements

### 5.4.1 Common Bridge component requirements

A bridge component implementation claiming conformance to any conformance class in this document shall:

a) Support VLAN Bridge component requirements according to IEEE Std 802.1Q-2022, 5.4 except for items g), h), and o)

a) Support C-VLAN component requirements according to IEEE Std 802.1Q-2022, 5.5 except for item d)

b) Allow the FDB to contain Static and Dynamic VLAN Registration Entries (8.8) for more than one VID, up to a maximum of 4094 VIDs, according to IEEE Std 802.1Q-2022, 8.8.

c) Support the strict priority algorithm for transmission selection on each port for each traffic class according to IEEE Std 802.1Q-2022, 8.6.8.1

d) Support the operation of the credit-based shaper algorithm according to IEEE Std 802.1Q, 8.6.8.2 on all ports as the transmission selection algorithm for at least 2 traffic classes

e) Support stream identification components according to IEEE Std. 802.1CB-2017, 5.3

f) Support Per-Stream Filtering and Policing (PSFP) according to IEEE Std 802.1Q-2022, 8.6.5.2 items a), b), and d)
    1) support the maximum SDU size filtering according to IEEE Std 802.1Q-2022, 8.6.5.3.1
    2) support the flow metering according to IEEE Std 802.1Q-2022, 8.6.5.5
    3) support the monitoring of PSFP as specified in 7.7.2.4

g) Support minimum number of stream identification and filtering entries as defined in Table 7-1
h) Support the management entities for configuration of bridge functions as specified in 7.6

### 5.4.2 Asynchronous Type1 Bridge component requirements

A bridge component claiming conformance to asynchronous Type1 class of this document, shall

a) Support common bridge component requirements according to 5.4.1
b) Support at least four queues according to IEEE Std 802.1Q-2022, 8.6.6

### 5.4.3 Asynchronous Type2 Bridge component requirements

A bridge component claiming conformance to asynchronous Type2 class of this document, shall

a) Support asynchronous Type1 bridge component requirements according to 5.4.2
b) Support FRER according to IEEE Std. 802.1CB-2017, 5.15
c) Support monitoring for FRER as specified in 7.7.2.5

### 5.4.4 Synchronous Type1 Bridge component requirements

A bridge component claiming conformance to synchronous Type1 class of this document, shall

a) Support common bridge component requirements according to 5.4.1
b) Support at least eight queues according to IEEE Std 802.1Q-2022, 8.6.6
c) Support at least 2 PTP Instances according to IEEE Std 802.1AS-2020, clause 5.4.1 items a) through e) and g) through j) on all ports
d) Support external port configuration capability on all ports according to IEEE Std 802.1AS-2020 5.4.2 item g)
e) Support the PTP fault-tolerant timing module as specified in 7.1.2.2
f) Support PSFP stream gating according to IEEE Std 802.1Q-2022, 8.6.5.2 item c)
g) Support the enhancements for scheduled traffic as specified in IEEE Std 802.1Q-2022 8.6.8.4 on all ports
h) Support the monitoring requirements of scheduled traffic as specified in 7.7.2.2
i) Support the stream gating for PSFP as specified in IEEE Std 802.1Q-2022, 8.6.5.4 and 8.6.10

### 5.4.5 Synchronous Type2 Bridge component requirements

A bridge component claiming conformance to synchronous Type2 class of this document, shall

a) Support Type1 bridge component requirements according to 5.4.4
b) Support at least 3 PTP Instances according to IEEE Std 802.1AS-2020, clause 5.4.1 items a) through e) and g) through j) on all ports
c) Support FRER according to IEEE Std. 802.1CB-2017, 5.15
d) Support monitoring for FRER as specified in 7.7.2.5

## 5.5 Bridge component options

### 5.5.1 Common Bridge component options

A bridge component implementation claiming conformance to any conformance class in this document may:

a) Support the operation of the credit-based shaper algorithm according to IEEE Std 802.1Q, 8.6.8.2 on all ports as the transmission selection algorithm for all traffic classes

b) Allow translation of VIDs through support of the VID Translation Table or through support of both he VID Translation Table and Egress VID translation table on one or more Bridge Ports according to IEEE Std 802.1Q, 6.9

### 5.5.2 Asynchronous Type1 Bridge component options

A bridge component implementation claiming conformance to asynchronous Type1 conformance class in this document may:

a) Support at least eight queues according to IEEE Std 802.1Q-2022, 8.6.6

### 5.5.3 Asynchronous Type2 Bridge component options

A bridge component implementation claiming conformance to asynchronous Type2 conformance class in this document may:

a) Support at least eight queues according to IEEE Std 802.1Q-2022, 8.6.6

### 5.5.4 Synchronous Type1 Bridge component options

A bridge component implementation claiming conformance to synchronous Type1 conformance class in this document may:

a) Support at least 3 PTP Instances according to IEEE Std 802.1AS-2020, clause 5.4.1 items a) through e) and g) through j) on all ports

### 5.5.5 Synchronous Type2 Bridge component options

A bridge component implementation claiming conformance to synchronous Type2 conformance class in this document may:

a) Support some number of PTP instances greater than 3 according to IEEE Std 802.1AS-2020, clause 5.4.1 items a) through e) and g) through j) on all ports

## 5.6 End station component requirements

### 5.6.1 Common end station component requirements

An end station component claiming conformance to any conformance class in this document shall

a) Support the strict priority transmission selection algorithm according to IEEE Std 802.1Q-2022, 8.6.8.1 on all ports for at least two traffic classes

b) Support the operation of the credit-based shaper algorithm according to IEEE Std 802.1Q-2022, 8.6.8.2 on all ports as the transmission selection algorithm for at least two traffic classes

c) Support management entities for configuration of the end station as specified in 7.6

### 5.6.2 Asynchronous Type1 end station requirements

An asynchronous Type1 end station that conforms to the provisions of this standard shall:

a) Support the common end station component requirements of 5.6.1

### 5.6.3 Asynchronous Type2 end station component requirements

An asynchronous Type2 end station that conforms to the provisions of this standard shall:

a) Support the asynchronous Type1 end station requirements of 5.6.2
b) Support the FRER Talker end system required behaviors as specified in IEEE Std 802.1CB-2017, Clause 5.6.
c) Support the FRER Listener end system required behaviors as specified in IEEE Std 802.1CB-2017, Clause 5.9
d) Support the monitoring requirements of FRER as specified in 7.7.2.5

### 5.6.4 Synchronous Type1 end station component requirements

A synchronous Type1 end station that conforms to the provisions of this standard shall:

a) Support the common end station component requirements of 5.6.1
b) Support at least 2 PTP Instances according to IEEE Std 802.1AS-2020, 5.4.1 items a) through e) and g) through j) on all ports
c) Support external port configuration capability on all ports according to IEEE Std 802.1AS-2020 5.4.2 item g)
d) Support PTP fault-tolerant timing module as specified in 7.1.2
e) Support end station requirements for enhancements for scheduled traffic according to IEEE Std 802.1Q-2022, 5.25
f) Support the monitoring requirements of scheduled traffic as specified in 7.7.2.2

### 5.6.5 Synchronous Type2 end station component requirements

A synchronous Type2 end station that conforms to the provisions of this standard shall:

a) Support the synchronous Type1 end station component requirements of 5.6.4
b) Support at least 3 PTP Instances according to IEEE Std 802.1AS-2020, 5.4.1 items a) through e) and g) through j) on all ports
c) Support the FRER Talker end system required behaviors as specified in IEEE Std 802.1CB-2017, Clause 5.6
d) Support the FRER Listener end system required behaviors as specified in IEEE Std 802.1CB-2017, Clause 5.9
e) Support the monitoring requirements of FRER as specified in 7.7.2.5

## 5.7 End station component options

### 5.7.1 Common end station component options

An end station component claiming conformance to any conformance class in this document may:

a) Support the use of customer VLAN identifiers
b) Support the use of per-stream VID and PCP

### 5.7.2 Asynchronous Type1 end station component options

An asynchronous Type1 end station that conforms to the provisions of this standard may:

a) <TBD>

### 5.7.3 Asynchronous Type2 end station component options

An asynchronous Type2 end station that conforms to the provisions of this standard may:

a) Support operation of the per-stream credit-based shaper algorithm for more than one stream according to talker behavior as specified in IEEE Std 802.1Q-2022, 34.6.1.1
b) Support FRER stream splitting function as specified in IEEE Std. 802.1CB-2017, clause 7.7 on more than one port and for some number of Compound Streams greater than 1
c) Support FRER talker end system required as specified in IEEE Std. 802.1CB-2017, clause 5.6 on more than one port
d) Support FRER talker end system required as specified in IEEE Std. 802.1CB-2017, clause 5.6 for some number of Compound Streams greater than 1
e) Support FRER listener end system required behaviors as specified in IEEE Std. 802.1CB-2017, clause 5.9 on more than one port
f) Support FRER listener end system required behaviors as specified in IEEE Std. 802.1CB-2017, clause 5.9 for some number of Compound Streams greater than 1

### 5.7.4 Synchronous Type1 end station component options

A synchronous Type1 end station that conforms to the provisions of this standard may:

a) Support at least 3 PTP Instances according to IEEE Std 802.1AS-2020, 5.4.1 items a) through e) and g) through j) on all ports

### 5.7.5 Synchronous Type2 end station component options

A synchronous Type2 end station that conforms to the provisions of this standard may:

a) Support FRER stream splitting function as specified in IEEE Std. 802.1CB-2017, clause 7.7 on more than one port and for some number of Compound Streams greater than 1
b) Support FRER talker end system required as specified in IEEE Std. 802.1CB-2017, clause 5.6 on more than one port
c) Support FRER talker end system required as specified in IEEE Std. 802.1CB-2017, clause 5.6 for some number of Compound Streams greater than 1
d) Support FRER listener end system required behaviors as specified in IEEE Std. 802.1CB-2017, clause 5.9 on more than one port
e) Support FRER listener end system required behaviors as specified in IEEE Std. 802.1CB-2017, clause 5.9 for some number of Compound Streams greater than 1
f) Support some number of PTP instances greater than 3 according to IEEE Std 802.1AS-2020, clause 5.4.1 items a) through e) and g) through j) on all ports

# 6. Aerospace Onboard Networks (informative)

This informative clause provides the context necessary to understand the network functions (Clause 7) required in aerospace onboard networks and inform the profiles (Clause 8) specified by this standard. It provides a general introduction to onboard aerospace networks (6.1) and describes the following topics:

a) Network design constraints (6.2)
b) Network topologies (6.3)
c) Application and traffic characteristics (6.4)

Note: This clause does not limit the aerospace profile to the use cases described within the clause. The profile as defined by Clause 5 of this standard is expected to be used by industry for all relevant applications.

## 6.1 Introduction to Aerospace Networks

Aerospace networks architectures can be broadly categorized by use cases from either a commercial or military perspective and analyzed from either a current or future perspective.

### 6.1.1 Current Network Architectures

Current network architectures in aerospace are often domain based, wherein a domain defines a set of functional communication blocks. For example aircraft control domain, vehicle management domain, etc. Domains are isolated by physically separate networks. Furthermore, within a given domain there are sub-domains that are also segregated in to physically separate networks. For example, in aircraft control domain the fly-by-wire (or flight control) network is a separate network from avionics network.

The current aerospace use cases also limit the use of Ethernet to lower criticality communications, which are not necessarily flight critical. For example, fly-by-wire networks on existing aircraft are based on non-Ethernet data buses.

#### 6.1.1.1 Commercial Aircraft

Networks are used in commercial aircraft to support varying levels of capabilities from supporting passenger entertainment to the actual control of the aircraft. Modern commercial aircraft can be subdivided into three networking domains: Aircraft Control Domain (ACD), Airline Information Services Domain (AISD), and the Passenger Information and Entertainment Services Domain (PIESD) as shown in Figure 6-1.

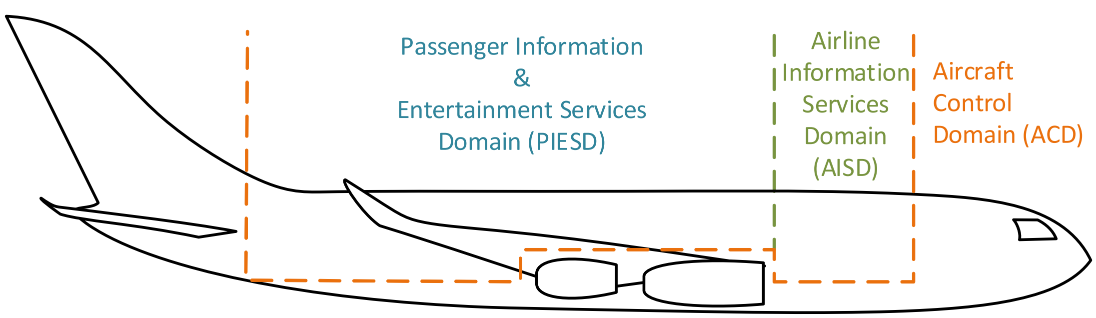


**Figure 6-1—Commercial Aircraft Network Domains**

The Aircraft Control Domain (ACD) networks host equipment that contribute to the safe flight of the aircraft. Functions typically hosted on the ACD network include electronic flight display systems, engine monitoring and alerting systems, flight management systems, flight controls, and other control systems that are housed outside of the passenger cabin. Due to the high criticality of the functions hosted, the ACD network has high safety requirements and deterministic [9] behavior is required.

In the ACD, networks were initially brought on the aircraft in order to reduce size, weight, and power (SWaP). In legacy aircraft, function specific federated equipment were interconnected by lower bandwidth point to point data buses such as ARINC 429. Modern aircraft employ integrated modular avionics (IMA) that reduces the amount of federated equipment and wires. In an IMA system, a general purpose processor is used to host the applications from multiple systems. The network provides an interconnect between the IMA processing, other functions hosted on the network, and to data concentrators that provide legacy interfaces. SWaP savings occur due to the reduction in equipment needed and the reduction in wiring due to consolidation of buses as depicted in Figure 6-2. I

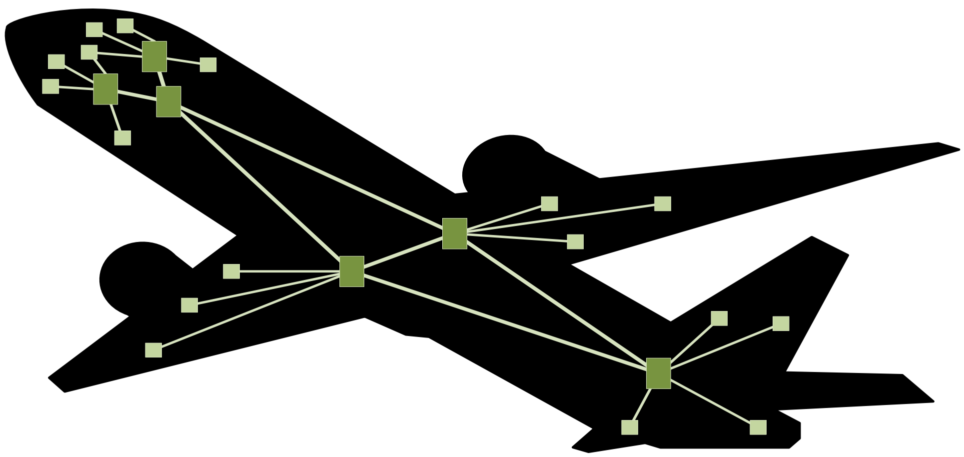

**Figure 6-2—Commercial Integrated Modular Avionics Depiction**

The Airline Information Service Domain (AISD) supports non-essential airline operational activities. It typically provides a general purpose processing platform as well as connectivity off the aircraft and between the other domains on the network. The AISD has high security requirements, but limited safety and determinism requirements due to the non-essential functions supported.

The Passenger Information and Entertainment Services Domain (PIESD) provides passenger network and entertainment services. On large commercial aircraft, this includes supporting the needs of hundreds of passengers. This drives high performance requirements. Interestingly, the PIESD has high availability requirements based on customer expectations.

#### 6.1.1.2 Military Aircraft

Military aircraft also use onboard networks to support functionality from the flight critical to mission oriented. A military aircraft can be subdivided into two domains: Air Vehicle System (AVS) and Vehicle Mission System (VMS). The AVS of the military aircraft is similar to the ACD of commercial aircraft. It encompasses the systems necessary for safe flight of the aircraft.

The Mission System of the military aircraft is responsible for supporting the varied missions of the aircraft. Depending on the type of aircraft, this could be delivering a weapon, search-and-rescue operations, and transport of equipment or personnel. The requirements for the VMS network vary based on the mission

[9] The meaning of determinism can vary with the use case and might range from microsecond timing control to bounded timing behavior in the 1-100 millisecond range.

equipment installed. The VMS equipment may include one or more high performance mission computers and typically has higher bandwidth needs than the AVS.

### 6.1.2 Future Network Architectures

As described in clause 6.1, the current aerospace network architectures tend to be domain based with multiple sub-domains in each domain. This poses a challenge to future platforms that require significant inter-domain communications coupled with more stringent size, weight and power, and cost (SWaP-C) requirements. Zonal architectures provide one solution to address these challenges and reduce the cabling needs in the aircraft while simultaneously converging the different-data buses.

Traditional aerospace system architectures have evolved from a domain, or function, based approach where each system was designed in isolation and overlaid onto the vehicle hardware in such a way that independent interconnects were often provided in the same physical areas. However, more recent approaches in civil, military, and also satellite platforms, have adopted a zonal approach where data is consolidated locally and communicated over shared buses between zones, often involving shared I/O and processing components. This zonal approach relies on logical separation of functions over a shared infrastructure rather than on physical separation as has traditionally been the case and reduces the duplication of interconnect infrastructure to provide the required level of fault tolerance. By supporting the partitioning of traffic flows, TSN supports the convergence of application functions onto a single physical network to reduce weight and cost by eliminating separate physical networks. In an example of this approach, it might be possible to envisage a flight control, or weapon release system, sharing network resources with a video distribution system.

Time-sensitive networking supports future networks and enables features that are required for the full range of use cases and traffic types to implement functions with a single network technology. Thus, adoption of TSN would significantly increase the number of and scale of the Ethernet networks on an aircraft, including the number of end stations, Bridges, and streams.

## 6.2 Network Design Constraints

Although there is considerable variability in the requirements and use cases of commercial and military aircraft, the aerospace profile of TSN attempts to balance the requirements of these use cases.

As in any system, the primary purpose of the network is to support the system and enable it to fulfill it’s design objectives. The functional aspects of this are ultimately measured through technical performance provided by the networking technology, typically interpreted as the ability to transport data from A to B in a time *T*, however this performance must be measured against market factors as well as regulatory constraints imposed on the aerospace industry. These factors are discussed here briefly to provide an overview of the design constraints that frame the aerospace TSN profile.

### 6.2.1 Performance & Technology

Performance is addressed here through quantifiable physical characteristics whereas technology is addressed through qualitative measures related to the use of the technology in an avionics system.

Each unique use case has differing requirements related to the bandwidth needs of connected nodes, the latency required for transmission of data through the network, and for the level of determinism needed to support individual applications. Bandwidth needs for military mission systems are often orders of magnitude greater than for aircraft control networks, although aggregate bandwidth needs for passenger networks are also increasing driven by passenger expectations and demand.

Hand in hand with the increased bandwidth needs for mission or passenger networks, the need for tight control of latency and jitter to support streaming services, whether this be for sensor data or for audio and video streams, drives the need for quality-of-service provision. Commercial transport aircraft, and some military platforms, have been using the quality-of-service provisions of ARINC 664 Part 7 for many years to provide bounded latency determinism to support of aircraft system functions and this is expected to be expanded by the addition of closed loop control functions that require strict delivery deadlines associated with mechanical and electronic control systems.

Determinism can also be considered to include the need for guaranteed delivery, and whilst true guaranteed delivery has typically been deferred to individual applications and aircraft functions, increased availability of data through provision of redundant data paths and redundant data sources has been, and will continue to be, the predominant means of ensuring data delivery in the aerospace network.

Demonstration of determinism, or at least proof thereof, has been central to the regulatory framework for many years and widespread adoption of what is essentially an asynchronous communication medium places stringent requirements on aerospace system designers to show aviation safety authorities, either by demonstration or by mathematical analysis, that network latencies can meet the safety requirements of the systems hosted on the various aircraft networks.

Security is rapidly becoming a central theme for aerospace systems and security features common in modern infrastructure networks are expected to be adopted in aerospace networks. Whether this is through authenticated access mechanisms and secure networks, or secure partitioning of network domains, physical security is no longer going to be the default operating paradigm.

Central to the reason for adoption of Ethernet as the preferred networking technology for aerospace networks, as has been seen over the last 20-30 years, are the levels of standardization and interoperability seen amongst a wide range of suppliers, as well as the ability to accommodate physical as well as functional growth that this standardization has brought. The availability of integration and test equipment and tools brought over from telecommunications, industrial and automotive markets also plays a large part in the attractiveness of Ethernet based networks to the aerospace industry.

### 6.2.2 Market Factors

Market factors impact all the anticipated use cases in aviation and TSN can be seen to offer clear technical and economic advantages that are made more compelling by the development of a profile specifically targeting Aerospace applications.

TSN is not a separate standard but comprises a set of amendments to the IEEE standard for Bridges and Bridged Networks to support time-aware functions. With the wide set of features that comprise TSN it is imperative that both operators and suppliers agree on a subset of the standards that are needed to avoid a situation where different components claim to support TSN but do not support the same set of TSN standards and are not inter-operable at the equipment level. The development of an industry profile to constrain the use of TSN standards is therefore a critical component that leads to a uniform supplier base to minimize the developmental and operating costs for aerospace networks.

Flexibility to support multiple traffic profiles with a single networking technology that is widely available and conforms to open standards, notwithstanding any dissimilarity needs, reduces the life-cycle costs of the aircraft by limiting variation in technology and equipment for maintenance and support tasks. Supported systems and functions may or may not be on the same physical network.

The larger industrial ecosystem that results from the use of open standards, and the natural evolution that arises from sharing these with wider industry, should lead to more reliable supply chain options and longevity in that supply chain to support the long service life that is expected in the aerospace industry.

### 6.2.3 Regulatory Considerations

The use cases described in section 6.3 cover the full range of aviation functional hazard classifications ranging from no functional effect through to catastrophic effect. An aerospace TSN network therefore needs to be developed following processes agreed with safety authorities responsible for oversight of the selected application. By harmonizing the use of TSN within the aerospace community it becomes possible to gain consensus between users of the technology and the applicable safety authorities for how the various TSN capabilities can meet the required safety standards. It is not in the scope of this standard to provide support for demonstrating the compliance of a TSN implementation with the appropriate regulations governing the particular application.

Central to the arguments for safety of the systems supported by the TSN network are established mechanisms for analyzing the probability of faults that lead to impaired system functionality, whether this relates to the equipment providing the network services or to the behavior of the functions implemented on that equipment. With regard to the functions provided by TSN, defining the constraints within which these functions operate greatly simplifies the effort required to demonstrate a level of determinism appropriate to the intended scope of operation and to thereby analyze the effects of failures associated with each of the performed functions.

Whether this relates to such failures as loss of synchronization and the methods needed to reduce the chance of this to an acceptable level, or the failure of filtering mechanisms in equipment that forms a part of the network, techniques can be agreed for the analysis of these failures and then reused across similar applications.

Without involvement of industry or government safety authorities, or details of specific network implementations, it is not possible or appropriate to propose or describe methods for achieving regulatory approval for the application of TSN networks in aerospace applications. This purpose of this TSN profile is therefore limited to supporting commonality between applications and reducing to number of analyses that need to be considered.

## 6.3 Network topologies

Network topologies for a range of aerospace platform use cases have been analyzed and are summarized here to inform the reader of potential use cases that have been considered in the development of this profile. The inclusion of a use case does not necessarily mean that the TSN profile shall support the use case. Similarly, the exclusion of a use case does not imply that it is not supported by the TSN

The aerospace use cases examined to develop a summary of use cases are listed below. Abbreviations are used as described in 6.1.1above.

- — Small Business Aircraft - ACD/AISD
- — Large Passenger Aircraft - ACD/AISD
- — Large Passenger Aircraft - PIESD
- — Small and Combat Military Network - AVS
- — Small and Combat Military Network - VMS
- — Large Military Network - VMS
- — Unmanned Military Network - AVS & VMS
- — Rotary Wing Aircraft - AVS
- — Rotary Wing - VMS
- — Satellite Network
- — Fibre Channel over TSN Backbone (AS6509)

The individual use cases can be analyzed from the perspective of various qualitative and quantitative characteristics to provide fair comparisons. The characteristics defined in Table 6-1 are used to define aerospace use cases.

### Table 6-1—Use Case Characteristics

| Characteristic | Description |
|---|---|
| Number of Nodes | Denotes the total number of networking nodes in an instantiation of the use case.<br>Includes both end stations and Bridges.<br>May be specified as a range or a maximum value. |
| Physical Topology | Denotes the type of physical topology in use, where in “physical topology” represent the hardware level connectivity between devices. Examples include star, ring, mesh, and point-to-point.<br>One or more topologies may be specified. |
| Number of Switch Hops | Denotes the number of hops between source and destination.<br>May be specified as a range or a maximum value. |
| Max Number of Streams per Switch | Denotes the number of unique data streams traversing a Bridge in the network. Each unique data streams requires three functions by the Bridge: stream identification, stream policing, and stream shaping. These functions serve the overall aerospace requirement that the Bridge is able to maintain isolation between unique data streams and provide guaranteed quality of service for each data stream.<br>May be specified as a range or a maximum value. |
| Network Redundancy | Describes the network redundancy architecture in the current instantiations of the use case.<br>One of more redundancy architectures may be specified. |
| Redundancy Mode | Denotes the mode of redundancy. Options include standby, active, hot-active, active-active with voting.<br>One or more modes may be specified. |
| Data Rates | Denotes the data rate(s) of the physical media.<br>May be specified as one or more rates |
| Media type | Denotes the type of media, which may include the physical medium as well as MAC protocol.<br>Examples include 100BASE-TX, Shielded Twisted Pair.<br>May be specified as one or more media types. |
| Worst Case Link Utilization | Denotes the link utilization of the most congested link in the network. Due to aerospace certification requirements, the worst case link utilization as designed/configured may be different from the worst case utilization as realized on the wire. This field can be used to specify both the “as configured” and “as realized on wire” variants of the link utilization.<br>May be specified as a range or maximum value. |
| Dissimilarity, Integrity, & Security | When applicable, denotes the use of dissimilarity, integrity, & security features. Additionally, the method by which such a feature is achieved in the current instantiation of the use case may be specified. |
| Maintenance and Monitoring | When applicable, denotes the use of maintenance and monitoring features. Additionally, the method by which such a feature is achieved in the current instantiation of the use case may be specified. |
| Certification Requirements | Specify if any certification requirements apply to this use case.<br>Specify if it is Mandatory, Desired, Do Not Care. |
| Supported Traffic types | Listing of Traffic Types from section 6.4 that exist in this use case. |

The use case characteristics presented during development of this standard are summarized in Table 6-2 and discussed in the following sub-sections. The list is not intended to be exhaustive, but provides typical use cases considered sufficient to drive development of the standard.

**Table 6-2—Summary of Aerospace Use Cases**

| Characteristic | Current Use | | Known/ Desired Future Use | Use case driving the most restrictive bound |
|---|---|---|---|---|
| | Lower Bound | Upper Bound | | |
| Number of Nodes | 5 | 100 | 500 | Large Passenger Aircraft (ACD) |
| Physical Topology | Master/Slave Bus, Point-to-point, Ring (daisy chained), switched star or combination | | Hybrid - Ring and Star | N/A |
| Number of Switch Hops | 0 | 5 | 15-30 | Large Passenger Aircraft (PIESD) |
| Max Number of Streams per Switch | 50 | 2000 | 4096 | Large Passenger Aircraft (ACD) |
| Network Redundancy | Two independent networks (A,B). End systems are dual homed to redundant LANs (ARINC664 part 7); Fault-tolerant Ring; None on point-to-point links. Subsystem or full system level redundancy (dual, triple, or quad) | | same as current use cases | All fault-tolerant use cases |
| Redundancy Mode | Bus Failover (Hot Standby), Frame Failover (Hot Active); Hot Active with voting | | same as current use | DAL[*] A/B systems |
| Data Rates | 10 Kbps | 1 Gbps | 100 Gbps | MIL-STD-1553 and Satellites on the low bound. Military VMS on the high end. |
| Media type | Copper: 1394,1553, RS-485/422, ARINC 429/629, Ethernet. Multimode Fiber: Fibre Channel, 100BASE-SX and 1000BASE-SX | | Optical fiber for higher data rates | All aircraft |
| Worst Case Link Utilization | 95% (worst case-configured)<br>80% (realized on the wire); higher for deterministic buses | | reduced to support application growth | Large passenger aircraft for configured, Military Flight Networks for realized |
| Dissimilarity, Integrity, & Security | No dissimilarity, integrity, or security features | Dissimilarity in design/implementation, high integrity additions, monitoring, security for isolation between assurance levels and cross-domain traffic | no change | Flight critical systems (e.g. ACD in large passenger aircraft, or AVS in military vehicles) |
| Maintenance and Monitoring | No maintenance or monitoring functions | Monitoring/Maintenance with SNMP or other means | Mandatory MIBS for TSN Network | Systems requiring high utilization. |
| Certification Requirements | None, self certified | HW/SW design and development assurance; IMA and Safety | no change | Passenger Aircraft (ACD) |
| Supported Traffic types | All traffic types | | no change | All aircraft |

[*]Design/Development Assurance Level according to SAE ARP4754

### 6.3.1 Number of Nodes

Control domains (ACD or AVS) typically have between 10 and 100 nodes depending upon the size and extent of the network and this is expected to remain constant going forward in time. The lower bound represents smaller military vehicle and satellite applications but these are expected to increase as more systems are added to the main networks.

Going forward the main driver for expanding the network comes from large passenger aircraft where airline and passenger information and entertainment networks (AISD & PIESD) are expected to grow as airlines compete through provision of improved passenger experiences.

### 6.3.2 Physical Topology

Almost all conceivable network topologies can be found across the aerospace use cases examined, and this is expected to remain the case going forward.

The most common topology encountered is that of a switched star, with larger networks cascading switches so that traffic traverses a number of switch hops to reach it's final destination. Ring networks are also important, particularly where switches are impractical or where bandwidth demands are high, providing one of the main drivers for Bridged end stations. Ring networks are most commonly found in military applications. Point to point links are also found where bandwidth requirements or weight restrictions make the use of switches impractical.

Redundancy and availability requirements complicate the network topology discussion. Civil passenger aircraft often employ redundant networks with dual-ported end stations as typified by ARINC 664 Part 7 networks. Elsewhere, redundant paths can be seen to provide redundancy in a single unified network. Both of these examples further driving the need for Bridged end stations and frame redundancy mechanisms.

### 6.3.3 Number of Switch Hops

The number of switch hops is largely an outcome of the size of the network and a trade off between switch size/capacity and wire-weight. Latency and determinism requirements have tended to put an upper bound on the number of switch hops. However, the reduced latency available with time-sensitive networking is likely to see the number of hops increase, particularly in larger cabin applications.

### 6.3.4 Max Number of Streams per Switch

The number of streams per switch is largely driven by the size and complexity of the network, and is usually controlled by the system integrator as part of the network configuration. Whilst ARINC 664 Part 7 specifies a minimum of 4096 streams, or Virtual Links, per switch this is not seen in current networks. However, as networks become larger, particularly for large passenger aircraft and with the addition of small devices to current networks, this number of streams is expected to be realized and may expand to as many as 10,000 streams.

The number of streams per switch must also be balanced against the practicalities of the technology and whilst the majority of aerospace use cases are expected to be met through the use of commercial technology the limits of that technology must also be considered. The future upper bound of 4096 streams is therefore considered a reasonable compromise.

### 6.3.5 Network Redundancy

Where network redundancy is required, current use cases most commonly achieve this by implementing two independent (A,B) networks and dual-homed end nodes (e.g. ARINC 664 Part 7). TSN Ethernet offers additional methods for achieving redundancy, including use of mesh or ring networks, and use of bridged end stations as well as dual-homed end nodes.

Point-to-point links do not by themselves provide redundancy unless this is managed at the system level where dual, triplex or sometimes quad redundancy may be encountered.

### 6.3.6 Redundancy Mode

A variety of redundancy mechanisms can be found, with bus fail-over (hot standby), frame fail-over (hot active) and hot active with voting being the most common.

### 6.3.7 Data Rates

Data rates, particularly at the lower bound, are largely tied to the historical/legacy systems that are being migrated to an Ethernet based network. At the upper bound, data rates have been limited by available technologies with high bandwidth applications being migrated from older RF links and bespoke transmission schemes. Future uses are expected to follow advances in commercial technology with 100 Gbps Ethernet seen as the most likely next step in performance.

### 6.3.8 Media type

Aerospace applications have traditionally relied on copper interconnects as there is a long established acceptance of the technology and an understanding of how to install the technology in the specific environment. This has led to the situation where lower speed Ethernet links also use copper media for lower speeds (below 100 Mbps) and shorter distances.

The advent of higher aggregate data rates and high bandwidth data streams are however driving a need to adopt optical fiber media for anything above 100 Mbps.

### 6.3.9 Worst Case Link Utilization

Driven by the desire to stay with copper media interfaces and the ability to statically configure networks for determinism, link utilization has been pushed to the limit in the worst case analysis. Because this is very much a worst-case analysis, to provide evidence of bounded latency determinism, the reality is that this level of utilization is extremely rare and the reality is usually well below 50%.

However, In rare cases this level of utilization can also be encountered in practice when tight control of the traffic is managed by a single function or application. In these cases, provided that the system integrator can demonstrate control of the traffic loading then 80% or even higher utilization might indeed be encountered.

### 6.3.10 Dissimilarity, Integrity, Maintenance, Monitoring, Security [DIMMS]

Dissimilarity and integrity tend to be associated with safety critical systems and are generally mandated by the relevant aviation safety authorities, particularly with regard dissimilarity. Both of these come at considerable cost in an aerospace environment but are essential for certain systems.

Maintenance operations, whilst important to the end user, are often afforded a lower importance by the OEM because they do not directly contribute to the aircraft function and are therefore harder to place a value on. Monitoring however is crucial as this relates to the assessment of continued safe operation of the system and fall within the purview of the aviation safety authorities.

Security in the realm of aerospace networks should not be confused with cybersecurity, although there is certain commonality involved. Whereas cybersecurity addresses the activities performed by an organization to safeguard its digital assets, security relates most simply to the protection of information from unauthorized interaction. In the aerospace network security therefore relates to the physical and logical separation of network domains. Most commonly mandated for military networks security is becoming more relevant to civil aircraft networks, particularly where data is shared between network domains such as the AISD and PIESD. Robust logical partitioning, through VLANs, and cross-domain security therefore become increasingly important for aerospace networks.

### 6.3.11 Certification Requirements

Certification requirements are generally set by the safety authority responsible in the domain in which the platform is intended to operate. For civil applications this is generally a national or regional organization, whereas for military applications the acquisition organization may be responsible, following guidelines such as, but not limited to, DO-254 and DO-178 as set by one or more of the civilian authorities. Satellite systems may be regulated by the European Cooperation for Space Standardization (ECSS) or similar organizations.

The responsible safety authority will set standards for developmental design assurance to ensure that equipment, systems and aircraft are safe to operate within a defined scope. In relation to time-sensitive networking this will include oversight of activities intended to show that the network will provide the intended behavior and performance consistent with it's intended application and may include test or mathematical analysis consistent with acceptable means of compliance as outlined by the authority.

Specification of the certification requirements for a time-sensitive network is outside of the scope of this profile document.

### 6.3.12 Supported Traffic types

Traffic types are described in detail in 6.4 but a generic listing of current traffic types is provided here for information.

- File Transfers - Mission Loading, Video Transfer, Image Transfer, Nav/Map data
- Asynchronous Parametric Data – sensors, displays,
- Synchronous Parametric Data – closed loop control and Inertial
- Command and Control – Weapons release authorization, commands
- Audio Streaming – Cockpit audio, cabin PA,
- Video Streaming – Uncompressed real-time video (ARINC818), compressed video streams
- Maintenance and Health Monitoring – fault reporting, testing
- Fiber Channel over TSN (FCoT) – HS1760 (weapons systems), and other FC based applications
- Extremely High BW Source - raw Radar data
- Raw IQ data and Raw Plot data
- Network control and infrastructure traffic

The different aerospace platforms will use traffic of these types in different mixes to achieve the desired behavior and performance. There is no correct mix of traffic types.

## 6.4 Application and traffic characteristics

Aerospace applications have been analyzed here in terms of the traffic that they use to communicate. This has been performed in a two-step process where first the characteristics used to define the traffic were defined and second where example applications were analyzed using the defined characteristics to provide a summary of the traffic types used in aerospace applications. The applications analyzed and their characteristics are not exhaustive but illustrate the complete range of traffic types that are encountered in typical aerospace applications on an aerospace network.

### 6.4.1 Traffic Type Characteristics

Traffic type characteristics are listed in Table 6-3 that enable a comparison of the most common traffic types encountered in the aircraft applications that are described in Table 6-1 and Table 6-2.

**Table 6-3—Aerospace Traffic Type Characteristics**

| Characteristic | Description |
|---|---|
| Periodicity | Traffic types comprise data streams that can either be<br>**Periodic**: transmitted in a cyclic/periodic (e.g. signal transmission) or<br>**Aperiodic**: transmitted in a acyclic/sporadic (e.g. event-driven) manner |
| Typical Period | Period denotes the planned data transmission interval (often also called “cycle”) at the application layer.<br>#: Specify period for cyclic traffic<br>**N/A:** for aperiodic/acyclic traffic |
| Application Synchronized to Network | Is the application producing traffic type synchronized to the network time at the application layer?<br>**YES** or **NO** |
| Data Delivery Guarantee Mode | Packet(s) are delivered to all receivers:<br>**Deadline**: before a specified time, relative to cycle time. (applies to periodic data)<br>**Latency**: within a predictable timespan from the start of the transmission<br>**Bandwidth**: if bandwidth utilization is within in the resources reserved by the sender<br>**None**: no special delivery requirements |
| Delivery Guarantee Value | **#**: Typical quantification of the data delivery guarantee for 80% of the use cases.<br>If “deadline” mode is used, specifies if the data will be delivered in the same period or not. |
| Application Tolerant to Jitter | Application’s tolerance of a certain amount of latency variation of the packet’s transmission (a.k.a Jitter)<br>**yes**: application can tolerate jitter as specified (always yes for “Bandwidth” and “none” delivery modes)<br>**no**: highly sensitive application requires negligible jitter |
| Tolerable Jitter Value | **#**: Value of acceptable jitter for periodic applications<br>**NEG**: Jitter must be negligible<br>**N/A**: if data delivery guarantee mode is “bandwidth” or **“**none**”** |
| Application Tolerant to Packet Loss | An application’s tolerance to a certain amount of consecutive packet loss<br>**Yes**: app can tolerate loss due to recovery mechanism in upper layer protocols or basic redundancy<br>**No**: app cannot tolerate a single packet loss |
| Tolerable Packet Loss Value | **#**: Num of consecutive packet loss tolerable to app.<br>**0**: if application is not tolerant to packet loss |
| Application Payload Size Variability | **fixed**: application payload size remain fixed<br>**variable**: app payload varies from one packet to packet |
| Payload Value (Bytes) | **#**: size/range of application data (payload) to be transmitted in the Ethernet frames. |
| Data Criticality | Criticality of this data for operation of the critical parts of the system:<br>**high**: highly critical for the operation. (DAL A, B),<br>**medium**: relevant but not continuously needed for the operation (Dal C, D),<br>**low**: not relevant for operation (DAL E). |

### 6.4.2 Traffic Type Analysis Summary

The traffic use case analysis in tables 6-1 and 6-2 separated traffic types broadly into Military Aircraft and Commercial Aircraft groupings [B80]. The bounds of these traffic types are summarized here in Table 6-4.

**Table 6-4—Summary of Aerospace Traffic Types**

| Traffic Characteristic | Current Use (range) | | Known/ Desired Future Use Bound | Use Case Driving the Most Restrictive (right) Bound |
|---|---|---|---|---|
| | Left Bound (loosest) | Right Bound (tightest) | | |
| Synchronism | Asynchronous | Synchronous | no change | Ultra-low latency and/or jitter (right bound) |
| Application synchronized to network? | No | Yes | no change | Ultra-low latency and/or jitter |
| Periodicity or Cycle Time | Aperiodic | <1 ms | 100 µs | Flight critical controls, sensors, and weapon systems |
| Latency Mode Guarantee Value | 100 ms | 1 ms | 100 µs | high criticality asynchronous events |
| Tolerance to interference (delay variation/ jitter) | up to latency limit | < 1 µs | no change | fly-by-wire, synchronous sensors |
| Tolerance to Loss* | 3 consecutive frames | zero | no change | Parametric data (left bound), Flight control or weapon release (right bound) |
| Payload size | 8 bytes | 2112 bytes | no change | Sensor data (left bound) Fibre Channel over TSN (right bound) |
| Data Criticality | no safety effect | DAL A | no change | Safety critical and flight control |

*All aerospace systems are robust to losses and failures. This entry therefore indicates desirable behavior.

Synchronism and whether the application is synchronized to the network are used here to capture how traffic synchronization relates to the application behavior. Synchronized traffic may or may not be synchronized to the application, and in most cases applications will not be synchronized to the network. However, where ultra-low latency is necessary, and an asynchronous boundary between the network and the application cannot be tolerated then it is reasonable, even necessary, to synchronize the application to the network. Examples of this would be fly-by-wire or safety-critical closed-loop control functions. The reader should be aware however that this requirement is sometimes levied because that was how it was implemented previously, and it may not actually be a functional requirement.

Two categories of traffic are generally considered candidates for migration to TSN, namely Ethernet based traffic (ARINC 664 or COTS), and non-Ethernet traffic (ARINC 429/629, Fibre Channel, MIL-STD-1553, IEEE 1394). Current Ethernet systems are asynchronous and have cycle times of 50 ms or higher and will use bounded latency to support safety requirements. Current non-Ethernet systems are often physically partitioned/segmented, can have cycle times of 1 ms or higher, are sensitive to both latency and delay variation and require determinism. As mentioned above, whether these tight latency/jitter requirements are needed on all signals isn't clear, but there are certainly functions that do require this.

Aerospace systems are inherently designed to be tolerant to network frame loss, but eliminating congestion loss should remain an objective. Based on the analysis of existing systems, future TSN-based systems need to address the requirements of both Ethernet and non-Ethernet traffic with the potential evolution to use cases requiring sub-millisecond latency.

# 7. Required functions for aerospace networks

This clause provides requirements specific to this document and the aerospace use case.

## 7.1 Time synchronization

Time synchronization is an essential component of the aerospace TSN synchronous profile to support the primary time-aware functions needed for time-sensitive aerospace applications. The forwarding of time-aware traffic from transmitting nodes through TSN capable Bridges requires tight control of transmission windows and forwarding gates, for which synchronization within the network is essential. Synchronization to external time references (e.g. UTC or TAI) is not necessary for TSN to operate in an aerospace environment but may be required by system level functions and is covered by [B19]. Deterministic traffic using rate-constrained shaping can also benefit from tight timing synchronization to minimize frame loss brought about by network components operating at different frequencies. Use of scheduled traffic in any segment of the network requires the presence of time synchronization for, at least, that segment of the network.

A synchronous Type1 or synchronous Type2 Bridge or end station is required to support IEEE Std 802.1AS-2020 gPTP functionality. Bridges or end stations conformant to the asynchronous profile defined in this standard are not required to support time synchronization.

The static nature of aerospace networks extends to clock selection with the result that aerospace equipment does not perform best master clock selection or use the associated algorithm (BCMA) described in IEEE Std 802.1AS-2020.

Enhancements for scheduled traffic described in IEEE Std 802.1Q, 8.6.8.4, are required for all aerospace components that support scheduled traffic. These features provide transmission gates for each supported traffic queue that open and close according to the determined traffic profile. It should be noted that the number of entries in the associated gate control list will be device specific and will impact the ability to schedule the network. A lower number of gate control entries may mean that multiple traffic streams must be scheduled in the same transmission gate, possibly resulting in output contention and therefore affecting worst case latency and jitter.

It is important for aerospace applications to consider fault-tolerance, including availability and integrity of the synchronizing function to provide reliable and trustworthy system behavior. Mechanisms to support fault-tolerance of time synchronization in IEEE Std 802.1AS-2020 (gPTP) include provisions for multiple time domains, multiple GMs, multiple time distribution trees, and multiple PTP Instances per port in Bridges and end stations. The use of these features must be carefully considered by the system designer to meet the fault tolerance objectives. An aerospace network is typically expected to tolerate multiple (typically 2) simultaneous arbitrary faults in Bridges, end stations, links, and GMs to maintain availability and integrity of time synchronization.

To achieve the required level of fault-tolerance for the aerospace use case, this standard defines a fault-tolerant timing Module (FTTM), to provide fault tolerance amongst available PTP Instances and time values as a time-aware higher level application in accordance with IEEE Std 802.1AS-2020, Clause 9. The FTTM would be supported by Bridges and end stations conformant to the synchronous profile of this standard. A FTTM is expected to operate with PTP Instances, GMs, and time values under normal operating conditions and is not expected to address startup or restart of grandmasters. The default operation of the FTTM is described in this standard.

### 7.1.1 Time synchronization concepts

#### 7.1.1.1 Time agreement generation and preservation

Time agreement generation and preservation is the process by which multiple time source nodes (GMs) come to an agreement on the time and maintain that agreement in the presence of both faults and oscillator drift. This process preserves both the collective accuracy and relative precision of the set of GMs.

Time agreement generation and preservation is outside the scope of this profile document.

#### 7.1.1.2 Time agreement propagation

Time agreement propagation is the process of propagating the time established by time agreement generation from time source nodes (GMs) to time destination nodes (PTP End Instances). Time agreement propagation is performed as per IEEE Std 802.1AS-2020.

#### 7.1.1.3 Dependent PTP Domains

Dependent PTP domains share one or more common time source components. This could be a common GM, continuously synchronized GMs, or GMs that share a common (continuously connected) clock source.

Because dependent PTP domains share one or more common influencers, they do not, on their own, enable end-to-end integrity checking of the time synchronization function. However, they can be used to improve the availability of a given time source and can provide partial integrity checks. For example, an application that receives timing from a single GM through more than one redundant sync trees has increased availability of that GM's time and can check the integrity of the sync trees by comparing the time received from them. However, because the time originates from a single GM, the integrity of that GM's time cannot be confirmed and, thus, end-to-end integrity of the time synchronization function is not achieved.

When a set of dependent PTP domains is used in combination with other PTP domains, which are independent (see 7.1.1.4), it can be reduced to a single independent domain and enhance the ability to achieve end-to-end integrity of the time synchronization function. This operation is performed by the Fault-Tolerant Timing Module (see 7.1.2).

Dependent PTP domains can be identified by one of the following methods:

- — They have the same PTP domainNumber, majorSdoID, and minorSdoID. This indicates that PTP messages from the same PTP GM are received by two PTP End Instances that are serviced by the FTTM.
- — They have different PTP domainNumbers but have the same gmtimeBaseIndicator. This indicates that the PTP messages come from different PTP GMs that share the same clockSource.
- — They have PTP domainNumbers that are defined by a management entity, which is out of scope of this standard, to be dependent.

NOTE 1—Per IEEE Std 802.1AS, the domainNumber is in the range 0 to 127, the majorSdoID is 0x1, and the minorSdoID is 0x00.

NOTE 2—Faults that cause the masquerading of any of the above PTP fields can be mitigated by the FTTM (see 7.1.2).

#### 7.1.1.4 Independent PTP Domains

Independent PTP domains do not share any common time source components with each other and therefore deliver independent time values.

Because independent PTP domains do not share any common influencers, they can enable end-to-end integrity checking of the time synchronization function, provided they track sufficiently closely.

Independent PTP domains need to be synchronized to each other in a fault-tolerant manner such that a fault in one domain does not impact the other synchronized domains (see 7.1.1.1). For example, time agreement mechanisms can be used to align the clocks of two independent GMs.

Because the independent PTP domains are synchronized to each other, they provide a redundant source of time to the end application and, thus, also improve the availability of the time synchronization function to the end application.

#### 7.1.1.5 Time error accumulation

As PTP time propagates through a network from a GM PTP Instance to a PTP End Instance, time error accumulates due to the following reasons:

— Timing errors at the GM (TEgm)
— Timing errors at intermediate PTP Relay Instances (TErly)
— Timing errors at the PTP End Instance (TEend)
— Link asymmetry between PTP Instances (TElnk)

The above time errors are illustrated in Figure 7-1.

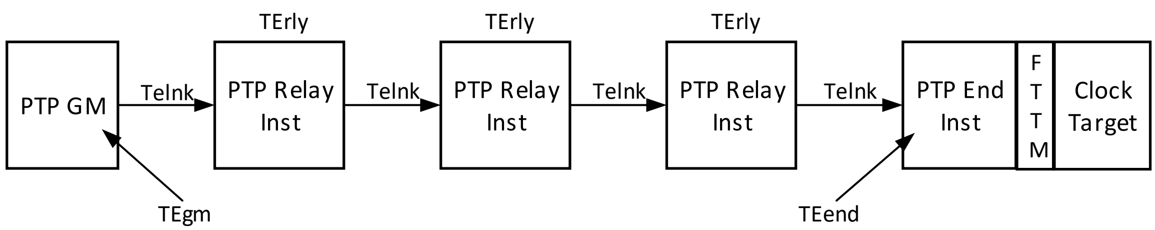


**Figure 7-1—Time error accumulation across a network**

TEgm, TErly, and TEend have constant and dynamic components. TElnk only has a constant component.

It is possible to determine the maximum potential value of each of the above time errors and, thus, the maximum potential time error at the PTP End Instance. This result, maxAccumTE (see 7.1.2.3.2.1), if available, can be used by the FTTM to select the best PTP domain to present to the ClockTarget.

The ENHANCED_ACCURACY_METRICS TLV from IEEE P1588a/D3.5 can be used to accumulate the maximum constant and dynamic time errors of each PTP instance and the connecting links, on a hop-by-hop basis, in the path from the GM to, but not including, the final PTP End Instance. This TLV is carried in PTP Announce messages.

### 7.1.2 Fault-Tolerant Timing Module

A fault-tolerant timing Module (FTTM), operating at the application layer per IEEE Std 802.1AS-2020 clause 9, is specified for aerospace applications to be implemented in all time-aware Bridges or end stations that support multiple time domains. The FTTM manages the selection of a clock source from amongst two or more PTP domains (and PTP Instances) to support increased availability and integrity. The FTTM also supports single domain solutions but, in this scenario, it does not provide any enhancements for increased availability or integrity.

Figure 7-2 illustrates the FTTM operating with three PTP Instances. The FTTM can also use the local oscillator's clock (OSC CLK) as an input to its selection algorithm.

A default selection algorithm is defined in 7.1.2.3.

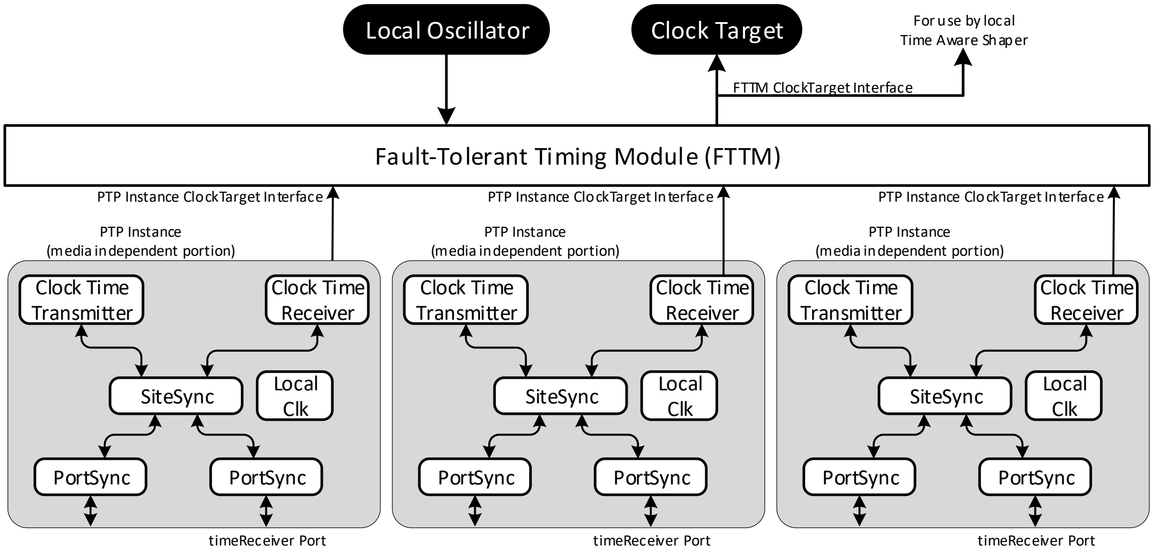


**Figure 7-2—Fault-Tolerant Timing Module in operation**

### 7.1.2.1 Scope and assumptions

The following list provides the detailed assumptions and goals for the FTTM:

a) An aerospace network and its configuration are static during normal operation.

b) All PTP ports are configured using the external port configuration provision of IEEE Std 802.1AS-2020 (i.e. the BCMA is not used).

c) There is no administrative reconfiguration during run-time in the event of faults.

d) While one domain is supported by the FTTM, more than one domain is required for fault tolerance in aerospace networks. To support interoperability, a minimum number of domains therefore needs to be specified.

e) PTP domains are recognized as being dependent or independent as defined in clause 7.1.1.3 and 7.1.1.4 respectively

### 7.1.2.2 FTTM functional description

The FTTM shall consist of the following functions:

— ClockTarget application interfaces (see 9 of IEEE Std 802.1AS-2020) where PTP End Instances serve as the ClockTimeReceiver entities and the FTTM serves as the ClockTarget entity.

— ClockTarget application interface(s) (see 9 of IEEE Std 802.1AS-2020) where the FTTM's output (FTTM_OUTPUT) serves as the ClockTimeReceiver entity to the application's ClockTarget entity.

— Zero or more instances of a Dependent Domain Selection Algorithm (DDSA).

— One selection multiplexer for each set of dependent domains.

— One instance of an Independent Domain Selection Algorithm (IDSA).

— One selection multiplexer for all independent domains.

— A local oscillator clock (OSC_CLK).

A functional diagram of the FTTM is shown in Figure 7-3.

The ClockTarget interfaces that pass timing information from the PTP End Instances to the FTTM are designated as, from the FTTM's perspective, input ClockTarget interfaces. They may be any of the types defined in clause 9 of IEEE Std 802.1AS-2020, ClockTargetEventCapture, ClockTargetTriggerGenerate,

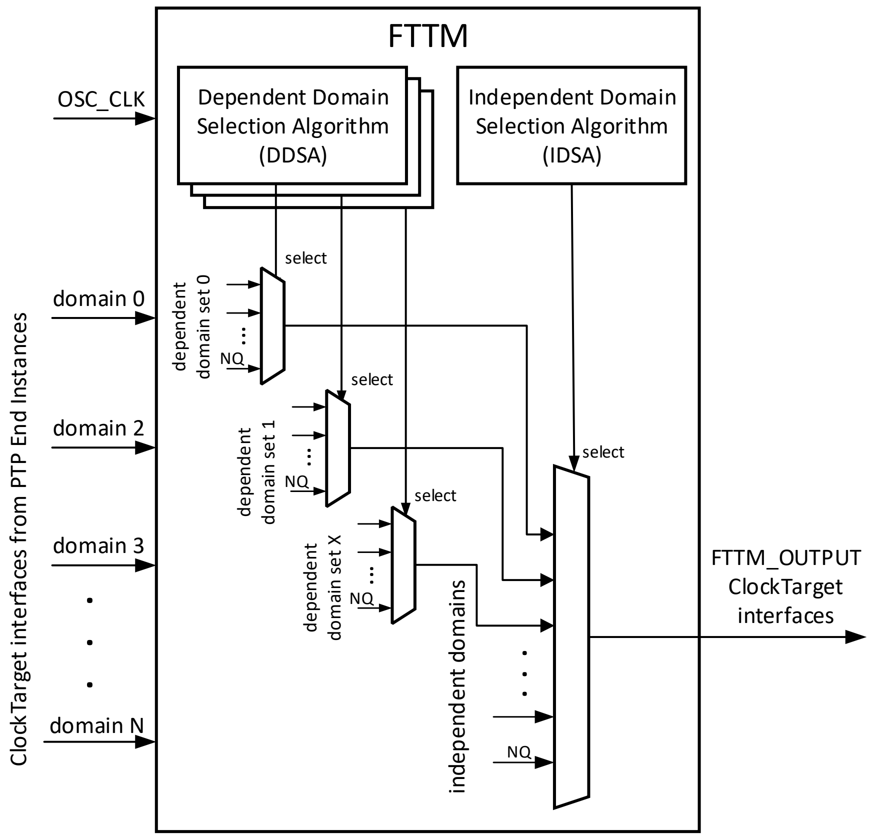


**Figure 7-3—FTTM functional diagram**

and ClockTargetClockGenerator, or they may be of another type. However, they should all be of the same type. The ClockTargetPhaseDiscontinuity interface should also be provided by the PTP End Instances to the FTTM.

These input ClockTarget interfaces can be for domains that have a dependency with one or more domains of other input ClockTarget interfaces or can be for domains that have no dependency with the domains of other input ClockTarget interfaces.

The DDSA and the IDSA each analyze their own set of input ClockTarget interfaces and, based on some criteria (e.g., see 7.1.2.3.2 d, e, and f for examples), determine which corresponding domain(s) provide a time that can be trusted. Being trusted does not mean the domain is definitely non-faulty. However, as long as a domain remains trusted (i.e., as long as its time continues to pass the said criteria), it can be deemed to be non-faulty by the DDSA or IDSA.

Each set of input ClockTarget interfaces that share a common dependency shall be processed as a group by one instance of the DDSA. This grouping allows each DDSA instance to produce an output that is independent from the outputs of the other DDSAs and from the other ClockTarget interfaces that are connected as inputs to the IDSA. Each instance of the DDSA shall select one of its input domains or the Not Qualified (NQ) domain (see 7.1.2.2.1), if none of its input domains can be determined to be trusted, as its result. The selected domain's ClockTarget interface is passed to the output of the DDSA. This output is passed to the IDSA as an independent domain.

The set of input ClockTarget interfaces that share no dependency with each other, which include the output ClockTarget interfaces of all instances of the DDSA, shall be processed by an IDSA. The FTTM's local oscillator clock, OSC_CLK, may be used by the IDSA as a frequency reference to infer additional information about the qualities of the input domains. The IDSA shall select one of its input domains or the NQ domain, if none of its input domains can be determined to be trusted as its result. The selected domain's ClockTarget interface shall be passed to the output of the IDSA and becomes the output of the FTTM, FTTM_OUTPUT. This output is passed to the application ClockTarget entity.

Any domain that has an isSynced status (see 18.4.4.1 of P802.1ASdm/D1.3) equal to FALSE or a gmPresent status (see 10.2.4.13 of IEEE Std 802.1AS-2020) equal to FALSE shall be declared to be untrusted. Other conditions for determining whether a domain is trusted are determined by the associated algorithm.

The default DDSA is described in 7.1.2.3.5. Other algorithms for the DDSA may also be used by the FTTM.

The default IDSA is described in 7.1.2.3.6. Other algorithms for the IDSA may also be used by the FTTM.

#### 7.1.2.2.1 Not Qualified (NQ) domain

The Not Qualified (NQ) domain is used to represent the condition where none of the input domains to the DDSA or to the IDSA can be determined to be trusted The NQ domain contains the ClockTarget interface from any one of the input domains (arbitrarily selected) being processed by the algorithm but shall have the isSynced status (per P802.3ASdm) and the gmPresent status forced to FALSE, to indicate the untrusted condition. All the possible parameters in the NQ domain are listed below.

— domainNumber = the domainNumber from the arbitrarily selected domain from the set of input domains being processed by the algorithm
— timeReceiverTimeCallback = the timeReceiverTimeCallback value from the arbitrarily selected domain
— isSynced = FALSE
— gmPresent = FALSE
— errorCondition = the errorCondition value from the arbitrarily selected domain
— clockPeriod = the clockPeriod value from the arbitrarily selected domain
— timeReceiverCallbackPhase = the timeReceiverCallbackPhase value from the arbitrarily selected domain
— grandmasterIdentity = the grandmasterIdentity value from the arbitrarily selected domain
— gmTimeBaseIndicator = the gmTimeBaseIndicator value from the arbitrarily selected domain
— lastGmPhaseChange = the lastGmPhaseChange value from the arbitrarily selected domain
— lastGmFreqChange = the lastGmFreqChange value from the arbitrarily selected domain

### 7.1.2.3 Default Fault-Tolerant Timing Module operations

#### 7.1.2.3.1 General

The default state-machine for the FTTM and its associated parameters and algorithms are defined in this subclause.

7.1.2.3.2 describes the parameters used by the default DDSA and IDSA algorithms.

7.1.2.3.3 and 7.1.2.3.4 describes the two default selection algorithms, the closest-pair selection algorithm and the mid-value selection algorithm, respectively, that can be used by the DDSA and the IDSA.

7.1.2.3.5 describes the default FTTM state-machine that selects the ClockTarget interface from a trusted input domain, if one exists, and presents it to the application.

#### 7.1.2.3.2 Common parameters of the default FTTM algorithms

a) $\mathrm{maxAccumTE_y}$

The parameter maxAccumTEx is the maximum non-faulty accumulated time error magnitude for domain x, from its GM (TEgm), through all intermediate PTP Relay Instances (TErly) and the corresponding links (TElnk), to the PTP End Instance (TEend) that is connected to the FTTM. See 7.1.1.5.

$$\mathrm{maxAccumTE_x} = (\max(|\mathrm{TEgm_x}|) + \Sigma\max(|\mathrm{TErly_x}|) + \Sigma\max(|\mathrm{TElnk_x}|) + \max(|\mathrm{TEend_x}|))$$

b) $\mathrm{maxAgms_{xy}}$

The parameter $\mathrm{maxAgms_{xy}}$ is the maximum accepted time skew magnitude between two non-faulty PTP GMs, GMx and GMy. This value is equal to the worst-case time error magnitude between the two GMs when they are not faulty. See TEgm in 7.1.1.5.

$$\mathrm{maxAgms_{xy}} = (\max(|\mathrm{TEgm_x}|) + \max(|\mathrm{TEgm_y}|))$$

This parameter is defined per pair of GMs to cover the case where each pair has a different value.

c) $\mathrm{maxAps_{xy}}$

The parameter $\mathrm{maxAps_{xy}}$ is the maximum accepted propagation skew magnitude between the time of two non-faulty domains, x and y. This value is equal to the worst-case time error magnitude between the two domains, x and y, from the perspective of the FTTM, resulting from their propagation paths when they are not faulty. See TErly, TElnk, and TEend in 7.1.1.5.

$$\mathrm{maxAps_{xy}} = \Sigma\max(|\mathrm{TErly_x}|) + \Sigma\max(|\mathrm{TElnk_x}|) + \Sigma\max(|\mathrm{TEend_x}|) + \Sigma\max(|\mathrm{TErly_y}|) + \Sigma\max(|\mathrm{TElnk_y}|) + \Sigma\max(|\mathrm{TEend_y}|)$$

This parameter is defined per pair of domains to cover the case where each pair has a different value.

d) $\mathrm{maxAs_{xy}}$

The parameter $\mathrm{maxAs_{xy}}$ is the maximum accepted skew magnitude between the time of two non-faulty domains, x and y. This value is equal to the worst-case time error magnitude between two synchronized domains, x and y, from the perspective of the FTTM, when they are not faulty.

$$\mathrm{maxAps_{xy}} = \mathrm{maxAgms_{xy}} + \mathrm{maxAps_{xy}} + \mathrm{maxAccumTE_x} + \mathrm{maxAccumTE_y}$$

This parameter is defined per pair of domains to cover the case where each pair has a different value.

e) $\mathrm{hyst_{xy}}$

The parameter $\mathrm{hyst_{xy}}$ is the hysteresis magnitude for the time skew of two non-faulty domains, x and y. The hysteresis enables the definition of one time skew level for the FTTM algorithm to move into a state and another time skew level to move out of that state. Thus, the FTTM algorithm changes state only when the skew level passes a given threshold.

This parameter is defined per pair of domains to cover the case where each pair has a different value.

f) ToDx

The parameter ToDx is the time of domain x at a given instant.

g) num_ind_domains

The parameter num_ind_domains is equal to one less than the number of independent domains that the IDSA has to process. A value of zero means there is only one independent domain to process.

h) num_dep_domains

The parameter num_dep_domains is unique to each dependent-pair selection algorithm instance and is equal to one less than the number of dependent domains that the particular dependent-pair selection algorithm has to process.

i) dep_domain_sel

The parameter dep_domain_sel identifies whether the algorithm is used for selecting between dependent domains or independent domains. When TRUE, the algorithm is used for selecting between dependent domains. When FALSE, the algorithm is used for selecting between independent domains.

#### 7.1.2.3.3 Closest-pair selection algorithm

The closest-pair selection algorithm selects the domain that has the highest precedence amongst all the trusted domains. It may be used by the DDSA or the IDSA.

The closest-pair selection algorithm compares all possible combinations of domain pairs to determine which pairs have times that match within their specified maxAs threshold. Any domain from a domain pair that matches within the maxAs threshold is deemed to be trusted and is made available for selection as the output of this algorithm. The domain that has the highest user-configured precedence amongst all the trusted domains is selected.

Domain characteristics that could be used for setting the user-configured precedence are:

— The domain's maxAccumTE (see 7.1.1.5). Domains with smaller maxAccumTE values could be given higher precedence.
— The domain's GM quality. Domains with a higher quality GM could be given higher precedence.

Pseudo-code that represents the closest-pair selection algorithm is given in Figure 7-4. This pseudo-code assumes that the highest precedence domains are assigned to the lowest identification index, x (e.g., ToDx, ClockTarget interface x).

#### 7.1.2.3.4 Mid-value selection algorithm

The mid-value selection algorithm selects the domain that has the median time amongst all the trusted domains. It may be used by the DDSA or the IDSA.

The mid-value selection algorithm compares all possible combinations of independent domain pairs to determine which pairs have times that match within their specified maxAs threshold. Any domain from a domain pair that matches within the maxAs threshold is deemed to be trusted and is made available for selection as the output of this algorithm. The trusted domain that has the median time amongst all the trusted domains is selected. If the number of trusted domains is even, the selected domain of the two median domains is the one with the smaller ToD value.

Pseudo-code that represents the mid-value selection algorithm is given in Figure 7-5.

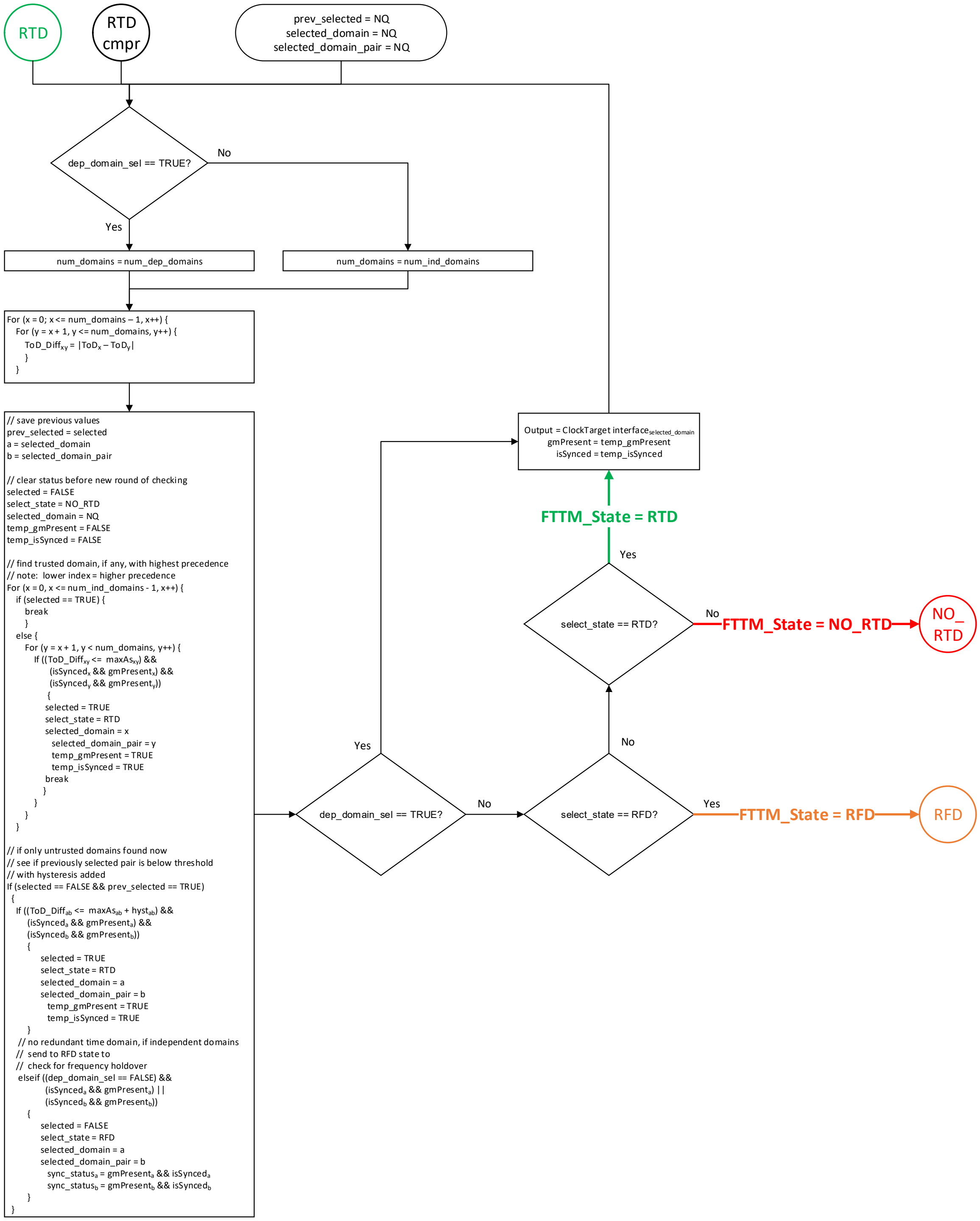


**Figure 7-4—Pseudo-code for closest-pair selection algorithm**

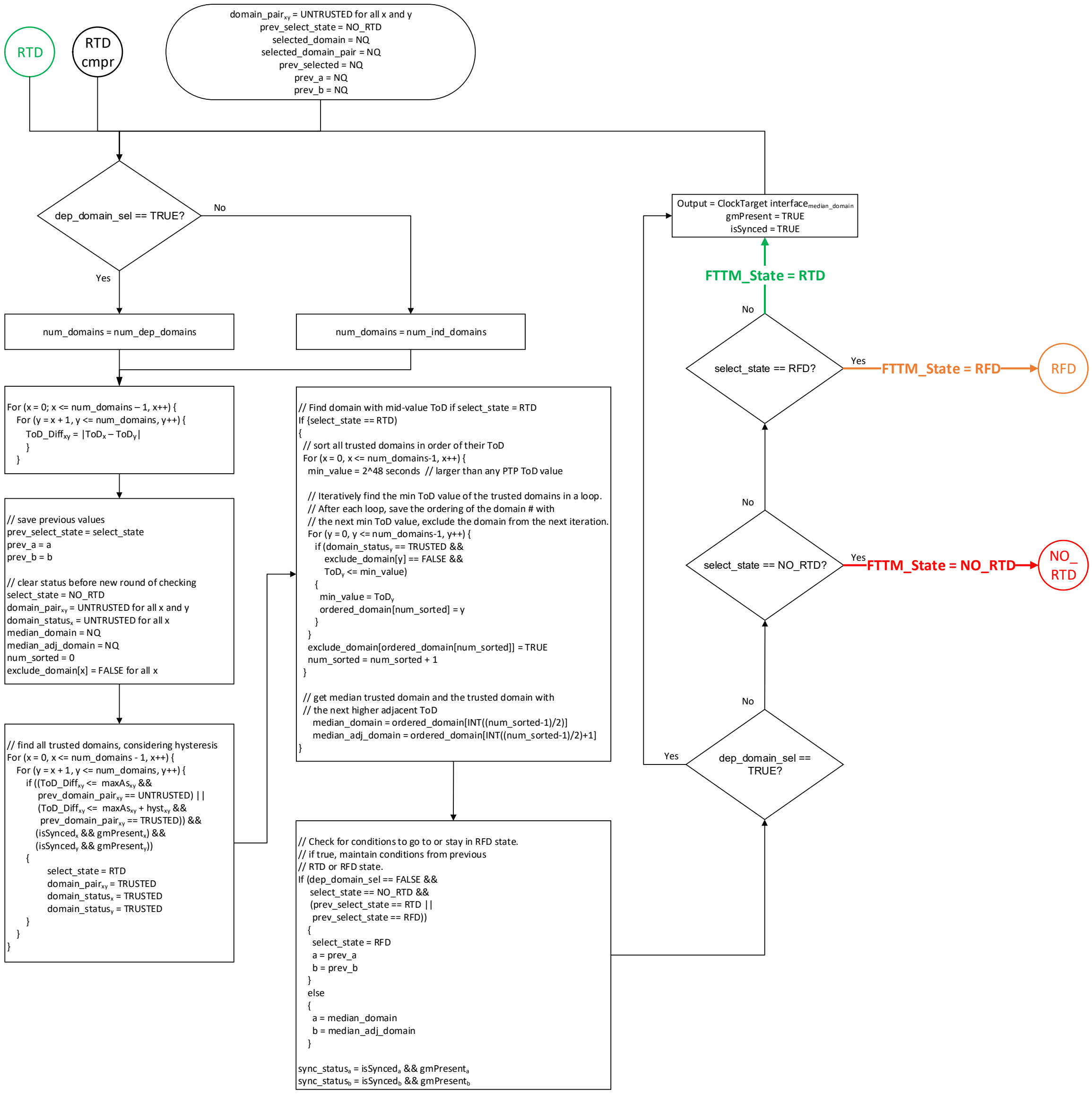


**Figure 7-5—Pseudo-code for mid-value selection algorithm**

#### 7.1.2.3.5 Default DDSA

The default DDSA uses either the closest-pair selection algorithm of 7.1.2.3.3 or the mid-value selection algorithm of 7.1.2.3.4 to select the output ClockTarget interface from amongst its input dependent domains.

#### 7.1.2.3.6 Default IDSA

The default IDSA uses the state machine shown in Figure 7-6 and described in this subclause to select the output ClockTarget interface from amongst its input independent domains. This state-machine shall have the following three states:

- — NO_RTD: No redundant time domain found.
- — RTD: Redundant time domain found.
- — RFD: Redundant frequency used to maintain time domain.

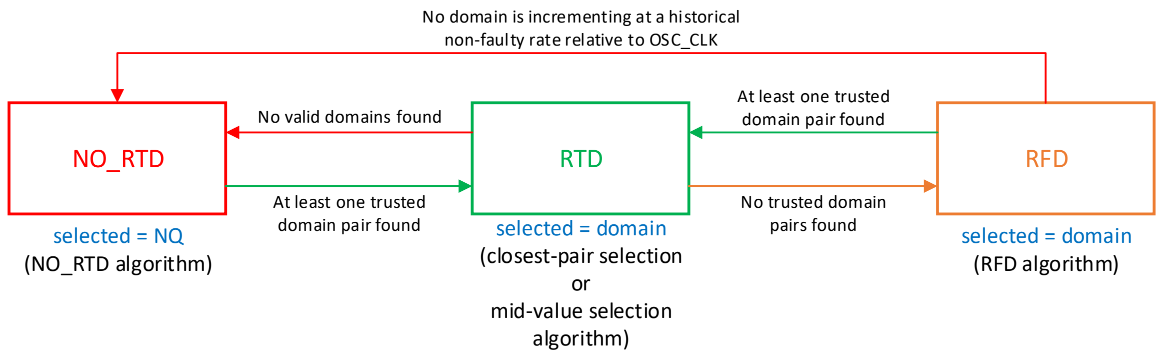


**Figure 7-6—Default state-machine for FTTM**

In the NO_RTD state, the algorithm compares the skew between all combinations of independent domain pairs, x and y. If any pair of independent domains does not exceed its pre-configured threshold, maxASxy, then the two independent domains of the pair are declared to be trusted. The algorithm moves to the RTD state if at least one trusted pair is found. For the special case where there is only one domain, the algorithm of the NO_RTD state connects that domain's incoming ClockTarget interface to the FTTM's output ClockTarget interface.

Pseudo-code that represents the algorithm used by NO_RTD state is shown in Figure 7-7.

In the RTD state, the algorithm continuously checks if no valid domains are found (i.e., none have acquired synchronization to a GM). If this occurs, then the state-machine moves back to the NO_RTD state. Otherwise, the algorithm continuously monitors all combinations of domain pairs to determine which, if any, domains can be deemed to be trusted. If any trusted domains are found, it selects one of the trusted domains to be its output and connects that domain's incoming ClockTarget interface to the FTTM's output ClockTarget interface. The selection is performed using either the closest-pair selection algorithm of 7.1.2.3.3 or the mid-value selection algorithm of 7.1.2.3.4.

The state-machine remains in the RTD state if the selection algorithm detects at least one trusted domain pair. If the selection algorithm no longer detects any trusted domain pairs even after accounting for hysteresis (see 7.1.2.3.2, e), then the state-machine moves to the RFD state.

In the RFD state, the algorithm continuously checks for the presence of trusted domain pairs. If any trusted domain pair is found, then the FTTM moves back to the RTD state. Otherwise, the RFD algorithm checks the current and historical qualities of the last selected domain and its partner (when they were still a trusted domain pair) to determine whether a valid time can still be presented at the FTTM's output interface. If at least one domain from that domain pair is determined, by using the current and historical rateRatio and rateRatioDrift qualities of the domain, to still be within the required thresholds relative to the frequency of OSC_CLK, then the algorithm remains in the RFD state. If no domain from that domain pair remains within the required thresholds, the FTTM moves to the NO_RTD state. Pseudo-code that represents the algorithm used by RFD state is shown in Figure 7-8.

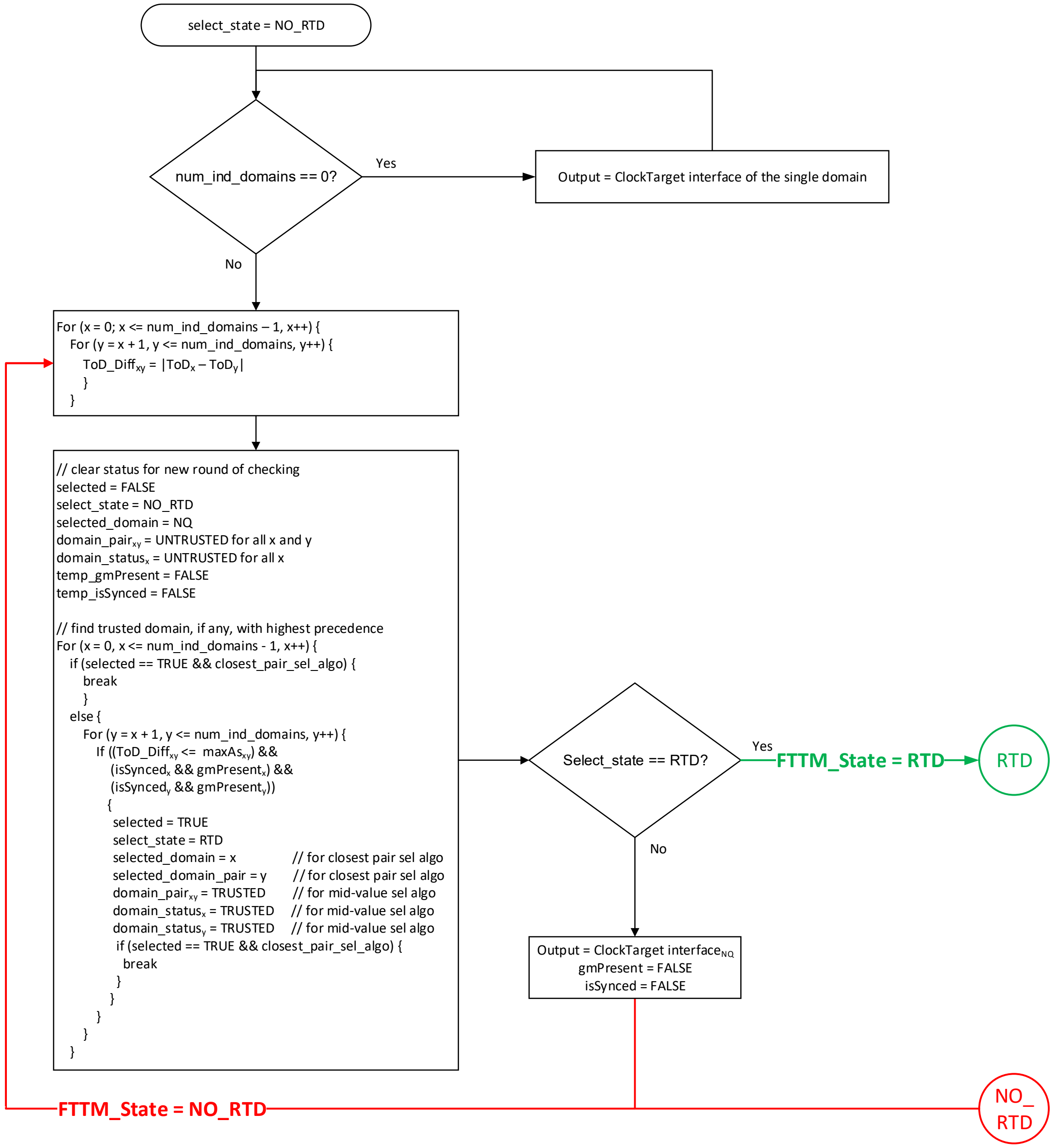


**Figure 7-7—Pseudo-code for default algorithm of FTTM NO_RTD state**


**Figure 7-8—Pseudo-code for default algorithm of FTTM RFD state**

## 7.2 Traffic Shaping

The use cases defined in clause 6 require shaping of the traffic at egress port of Bridges or end stations to meet the latency and packet delay variation (jitter) requirements defined in Table 6-4. Traffic shaping is specified according to the profile being used, synchronous or asynchronous, and the type of traffic shaping required at the egress port.

Two traffic shaping methods are considered applicable to the aerospace use cases:

j) Credit-based shaper as defined in IEEE Std 802.1Q-2022, Clause 8.6.8.2 and

k) Time-aware shaper as defined in IEEE Std 802.1Q-2022, clause 8.6.8.4

The credit-based shaper (CBS) is used by asynchronous implementations to shape the transmissions of a stream on the basis of the aggregate rate or bandwidth. CBS does not require network-wide time synchronizations and may be used in aerospace scenarios that do not support time synchronization. The CBS may also be configured in Bridges to shape the flow of unregulated traffic arriving at the Bridge.

The time-aware shaper (TAS) is used by synchronous implementations to schedule the transmissions of a stream across the network to achieve required latency, jitter, and isolation. A device supporting time-aware shaping is required to also support time synchronization as defined in clause 7.1 since time-aware scheduling requires all devices to have the same notion of time or a common reference clock. The TAS may also be configured in Bridges to synchronize asynchronous flows that arrive at the Bridge from non-time-aware components.

Bridge and end station implementations may support both CBS and TAS on the same port and users should consider the interaction between the two shapers when evaluating the performance of such an implementation. For example, as described in IEEE Std 802.1Q-2022, clause 8.6.8, the credit for CBS accumulates only during the time that the gate assigned to the credit-based flow is open, so the CBS idle slope must be modified based on the duty cycle of the TAS schedule for the assigned output queue.

Whilst IEEE Std 802.1Q specifies 8 priority levels, this does not limit the number of queues provided by a Bridge or end station and an application may require the use of more than 8 queues. An example of this might be to support stream isolation and this could apply to either CBS or TAS.

## 7.3 Stream Policing

Aerospace applications require policing of traffic at each bridge in a network to prevent faults and failures in one device or application impacting other devices or applications. This requires monitoring and policing the network resources being consumed by each stream. For example, Avionics networks defined by ARINC 664 part 7 [B2] police streams at ingress of each bridge using Asynchronous Transfer Mode (ATM) [B3] approach.

This standard specifies the use of Per-Stream Filtering and Policing (PSFP) defined in IEEE Std 802.1-2022, clause 8.6.5 in Bridges to filter and police streams. Bridges may use PSFP, in combination with traffic shaping mechanism to meet the latency and jitter requirements of asynchronous streams. PSFP improves network robustness and prevents traffic overload conditions that might otherwise affect Bridges and receiving endpoints due to misconfiguration, malfunction, or Denial of Service (DoS) attacks. The default behavior for aerospace use cases is to discard frames that do not meet the PSFP criteria assigned to the corresponding stream filter. For time-aware streams, the number of stream gates needed to support stream gating may be significantly smaller than the required number of streams.

PSFP requirements for Bridges belonging to the different conformance classes defined in this standard are provided in Clause 5.

## 7.4 Traffic Isolation

Aerospace use cases require strict isolation between streams to support independence between individual functions and traffic flows at the system level. This is especially important in a scenario where the network converges traffic from sources that are certified to different design assurance levels (mixed-DAL). For example, a Bridge may have two streams arriving at two ports that are originating from data sources (talkers) at different design assurance levels, the two streams being forwarded to the same egress port. This

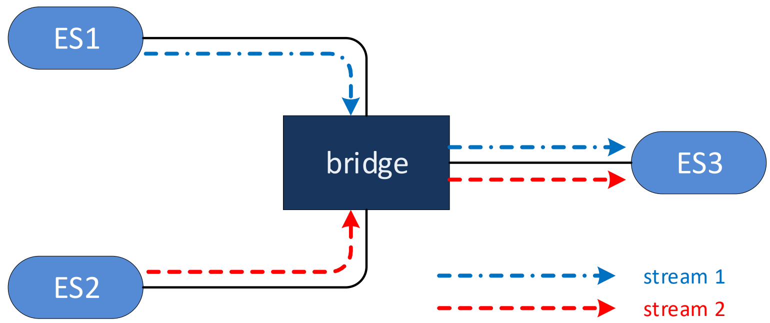


**Figure 7-9—Aerospace Stream Isolation**

is illustrated in Figure 7-9 where stream 1 and stream 2 originating from end stations ES1 and ES2 are forwarded by a Bridge to end station ES3. If the Bridge does not independently filter, police, and monitor each stream, faults in one stream could negatively affect the other stream at the output of the Bridge. Policing the streams in the Bridge ensures that all streams have sufficient resources to be forwarded without frame loss and with bounded latency to meet application requirements.

To support aerospace use cases, this standard requires per-stream isolation throughout the network and requires that Bridges identify, filter, and police each stream independently as defined in Clause 5. Depending on the size, complexity, and design of aerospace network implementations, Bridges will have different requirements for stream support, particularly with regards to the supported stream count. While some use cases may require very large stream counts per port, other aerospace use cases may benefit from Bridges supporting low stream count on constrained hardware.

This standard defines two sets of requirements for low and high stream count Bridge implementations compliant with this specification. Table 7-1 and Table 7-2 specify the minimum number of streams to be identified, filtered, and policed individually at compliant Bridges in an aerospace network.

**Table 7-1—Low Stream Count Bridge Requirements**

| Number of Ports | Minimum Stream Count |
|---|---|
| <=4 | 128 |
| 5-8 | 256 |
| 9-12 | 256 |
| 13-18 | 256 |
| >18 | 256 |

**Table 7-2—High Stream Count Bridge Requirements**

| Number of Ports | Minimum Stream Count |
|---|---|
| <=4 | 256 |
| 5-8 | 512 |
| 9-12 | 1024 |
| 13-18 | 2048 |
| >18 | >4095 |

The use of priority queues and the mapping of traffic types and classes to output queues is an important tool to ensure isolation between applications and functions hosted on the aerospace network.

With the diverse set of traffic types encountered in aerospace applications and the wide variation between applications it the mapping of priority to egress queues becomes a critical decision in the design of the aerospace network.

IEEE Std 802.1Q (8.6.6) provides recommendations for mapping priority to traffic classes depending upon the number of priorities and queues supported by components of the platform.

## 7.5 Network Redundancy

Aerospace use cases require network redundancy to overcome link and node failures. Existing solutions used in aerospace applications are either implemented as proprietary implementations at the application layer or in the network. For example, see ARINC 664 part 7 [B1].

The Type 2 conformance requirements defined in this standard specify the use of Frame Replication and Elimination for Reliability (FRER), as defined in IEEE Std 802.1CB-2017. FRER enables a flexible solution that supports different redundancy patterns as described in Annex C of IEEE Std 802.1CB-2017. FRER may be used to implement the commonly used aerospace redundancy pattern of dual redundant paths over physically separate networks (e.g. A/B network pattern). Bridge and end station requirements for FRER are described in Clause 5.

FRER enables the application to transmit a single copy of a frame that is replicated by the Bridge or end station for transmission over multiple disjoint paths. The duplicated frame is subsequently discarded at the receiving end station or Bridge, thereby providing seamless redundancy for applications that cannot tolerate packet loss.

Note that if the end node includes a Bridge as well as the end station function then the FRER function may be implemented in either the Bridge or end station.

## 7.6 Configuration

### 7.6.1 Aerospace Configuration Model Overview

Due to the safety and assurance requirements, aerospace networks are designed to be engineered networks with static topology best suited for fully centralized configuration model as specified in IEEE Std 802.1Q-2022, clause 46. The topology and stream requirements are derived from higher level system requirements. Therefore, the input data for centralized user configuration (CUC) and centralized network configuration

(CNC) module is derived from higher level system interface control document (ICD). Consistent with current aerospace practice, topologies and configurations are statically defined using out-of-band CUC/CNC functions and no direct communications occur between the CUC/CNC and Bridges or end stations. The CUC and CNC get the information required to generate network and user configuration in the form of static files. And similarly, CUC and CNC generate individual file-based device configurations that are loaded into equipment during manufacture or at major service events following an industry or implementation specific process. Aerospace qualified tools are used at each stage of configuration development to verify that configurations are accurate representations of the user requirements with configuration control maintained for individually identifiable items. Figure 7-10 depicts the configuration model as specified by this standard.

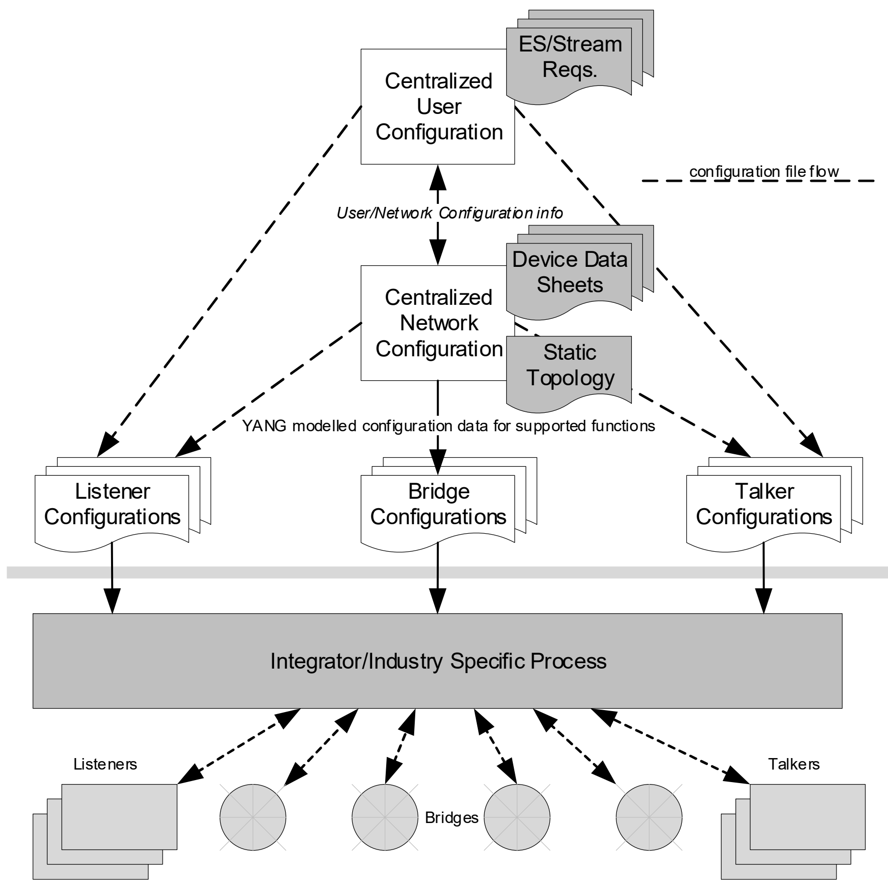


**Figure 7-10—Aerospace Configuration Model**

This standard specifies YANG data models to configure TSN functions at conformant end stations and Bridges. The aerospace YANG models used for the TSN features and network entities are specified in Table 7-3.

Note: Aerospace implementations may choose to utilize industry standards like ARINC 665-3 and ARINC 615A to convert the configuration instance data to binary representation and load them on aircraft. This approach is further discussed in Annex C.

Configuration of the end station talkers and listeners requires additional stream centric information (e.g., stream identification and tagging, stream shaping parameters) in addition to interface configuration. This standard specifies the use of UNI YANG model as defined in IEEE Std P802.1Qdj to provide the talker and listener configuration data to end stations.

Note: For talker and listener configuration, this standard only specifies the data model with which the instance data is provided to respective end stations. The standard does not define relevant managed objects. Aerospace implementations may choose to instantiate the talker/listener configuration in a custom manner.

### 7.6.2 YANG Data Models

This standard selects and specifies the use of YANG data models in aerospace applications from the list of YANG models defined in existing IEEE standards. Only the models used to represent the functionality associated with TSN features on Bridge and end station components are included here as part of the Aerospace Profile.

*<< Editor's Note: YANG for device data sheets and static topology definition are not included in this draft. Draft models referenced here are expected to be completed standards prior to completion of this standard>>*

**Table 7-3—YANG Data Models**

| Function | YANG Data Model & Status | Bridge and/or End Station | YANG Modules |
|---|---|---|---|
| Time Synchronization (IEEE Std 802.1AS™) | IEEE P802.1ASdn D1.1 (April 2023) | Bridge and End Station | ietf-yang-types<br>ieee1588-ptp<br>ieee802-dot1as-ptp |
| Time Aware Shaper (TAS) (IEEE Std 802.1Q™-2022 Clause 8.6.8.4) | IEEE P802.1Qcw D1.0 (December 2022) | Bridge and End Station | ieee802-dot1q-sched<br>ieee802-dot1q-sched-bridge |
| Credit Based Shaper (CBS) | IEEE P802.1Qdx Awaiting PAR approval | Bridge and End Station | ieee802-dot1q-cbs<br>ieee802-dot1q-cbs-bridge<br>ieee802-dot1q-cbs-if |
| Per-Stream Filtering & Policing (PSFP) | IEEE P802.1Qcw D2.0 (December 2022) | Bridge only | ieee802-dot1q-psfp<br>ieee802-dot1q-psfp-bridge |
| Frame Replications and Elimination for Reliability (IEEE Std 802.1CB™-2017) | IEEE Std 802.1CBcv-2021 Published | Bridge and End Station | ieee802-dot1cb-frer |
| Stream Identification (Bridge) | IEEE Std 802.1CBcv-2021 Published<br>IEEE Std 802.1CBdb-2021 Published | Bridge only | ieee802-dot1cb-stream-identification<br>ieee802-dot1q-bridge |
| End Station Configuration (Interface/Stream config.) | IEEE P802.1Qdj D1.0 (November 2022) | End Station only | ieee802-dot1dj-tsn-config-uni |
| Explicit/Static Forwarding | IEEE Std 802.1Qcp-2018 (IEEE Std 802.1Q™-2022) | Bridge only | ieee802-dot1q-bridge |

## 7.7 Monitoring and Management

### 7.7.1 Overview

Management and monitoring functions for aerospace applications have traditionally been a system level function specified by airframe manufacturers based on the need to monitor the equipment that provides the system functions and to ensure safe operation of the system. ARINC standardized protocols for aerospace maintenance operations are not widely adopted and the aerospace industry is inundated with numerous disparate solutions to monitor and manage aerospace equipment.

The introduction and use of commercial technologies such as Ethernet introduces the concept of standardized object management using a Management Information Base (MIB) as a database of objects used for managing network entities. Some system integrators and aircraft manufacturers have attempted to use the MIBs as the basis of the Monitoring and Management of their systems but beyond basic interface objects there has been insufficient industry consensus to allow this to work effectively.

With the adoption of TSN, the aerospace profile aims to promote standardization of a set of objects that can be implemented in hardware by device/chip vendors, thereby providing a basic capability across all components that conform to the aerospace profile. By standardizing this at the component level, the engineering and verification effort performed by the equipment supplier should be reduced such that the level of effort required to develop equipment can remain commensurate to the scale of the platform and with the level of design assurance required to ensure safe operation of the platform.

No attempt is made here to specify the means by which the management objects are retrieved by an aircraft management function. This standard only specifies the objects that must be maintained and available during operation (flight) in order to be conformant with the profile in an attempt to ensure that hardware devices provide the capability to support monitoring and management for aerospace TSN applications.

Note: While all management objects are to be supported as required by the IEEE Std 802.1Q, the management objects for configuration may not be exposed during runtime and may only be accessible via the static configuration files. The management objects defined in 7.7 are monitoring objects (counters) that are to be made available during runtime.

### 7.7.2 TSN Feature Specific Monitoring Objects

The following sections outline the objects considered necessary to support each of the functions outlined in Table 7-3 for a certifiable solution and are therefore specified in this standard. Other objects are not necessary and in some cases should not be exposed. Exposure of R/W objects in particular is discouraged for aerospace applications to minimize the safety impact on designs.

#### 7.7.2.1 Required Monitoring Objects for Time Synchronization

*<< Editor's Note: No objects have yet been defined for time synchronization in aerospace applications. Contributions are welcome. Please review AS-2020, and ASdn, and make proposals>>*

An aerospace component is required to support managed objects of the IEEE Std 802.1AS-2020 time synchronization function as shown in Table 7-4. The granularity of these objects is TBD.

**Table 7-4—Time Synchronization Managed Objects**

| Name | Data Type | Operations Supported* | Reference |
|---|---|---|---|
| | | | |

*R = read-only access

#### 7.7.2.2 Required Monitoring Objects for TAS

An aerospace component is required to support managed objects of the stream filter as shown in Table 7-5. The granularity of these objects is required to be per queue, per port.

**Table 7-5—Time Aware Shaper Managed Objects**

| Name | Data Type | Operations Supported* | Reference |
|---|---|---|---|
| TransmissionOverrun | counter | R | 12.29.1.1.2 |

*R = read-only access

No further managed objects are specifically required by this profile for the Time Aware Shaper.

#### 7.7.2.3 Required Monitoring Objects for Credit Based Shaper

No objects have yet been defined by this profile for the Credit Based Shaper.

#### 7.7.2.4 Required Monitoring Objects for PSFP

An aerospace component is required to support managed objects of the stream filter as shown in Table 7-6. The granularity of these objects is required to be per stream.

**Table 7-6—PSFP Stream Filter Managed Objects**

| Name | Data Type | Operations Supported* | Reference |
|---|---|---|---|
| MatchingFramesCount | counter | R | 8.6.5.3 |
| PassingSDUCount | counter | R | 8.6.5.3.1 |
| NotPassingSDUCount | counter | R | 8.6.5.3.1 |
| PassingFrameCount | counter | R | 8.6.5.4 |
| NotPassingFrameCount | counter | R | 8.6.5.4 |
| RedFramesCount | counter | R | 8.6.5.5 |

*R = read-only access

No further managed objects are specifically required by this profile for PSFP stream filters.

An aerospace component is required to support managed objects of the stream gates as shown in Table 7-7. The granularity of these objects is required to be per stream gate.

**Table 7-7—PSFP Stream Gate Managed Objects**

| Name | Data Type | Operations Supported* | Reference |
|---|---|---|---|
| StreamGateClosedDueToInvalidRx | boolean | RW | 8.6.5.4 |
| StreamGateClosedDueToOctetsExceeded | boolean | RW | 8.6.5.4 |

*RW = Read/Write access.

No further managed objects are specifically required by this profile for PSFP stream gates.

An aerospace component is required to support managed objects of the flow meter as shown in Table 7-8. The granularity of these objects is required to be per flow meter.

**Table 7-8—PSFP Flow Meter Managed Objects**

| Name | Data Type | Operations Supported* | Reference |
|---|---|---|---|
| MarkAllFramesRed | boolean | RW | 8.6.5.5 |

*RW = Read/Write access.

No further managed objects are specifically required by this profile for the PSFP flow meters.

#### 7.7.2.5 Required Monitoring Objects for FRER

An aerospace component is required to support managed objects of FRER as shown in Table 7-9 and in Table 7-10. The granularity of these objects is required to be per-port and per-stream and per-port respectively.

**Table 7-9—IEEE Std 802.1CB, FRER, Per-Port Managed Objects**

| Name | Data Type | Operations Supported* | Reference |
|---|---|---|---|
| frerCpSeqRcvyPassedPackets | counter | R | 10.9.1 |
| frerCpSeqRcvyDiscardPackets | counter | R | 10.9.2 |
| frerCpSeqEncErroredPackets | counter | R | 10.9.3 |

*R = read-only access.

No further managed objects are specifically required by this profile for per-port FRER objects.

**Table 7-10—IEEE Std 802.1CB, FRER, Per-Stream Per-Port Managed Objects**

| Name | Data Type | Operations Supported* | Reference |
|---|---|---|---|
| frerCpsSeqGenResets | counter | R | 10.8.2 |
| frerCpsSeqRcvyOutOfOrderPackets | counter | R | 10.8.3 |
| frerCpsSeqRcvyRoguePackets | counter | R | 10.8.4 |
| frerCpsSeqRcvyPassedPackets | counter | R | 10.8.5 |
| frerCpsSeqRcvyDiscardedPackets | counter | R | 10.8.6 |
| frerCpsSeqRcvyLostPackets | counter | R | 10.8.7 |
| frerCpsSeqRcvyTaglessPackets | counter | R | 10.8.8 |
| frerCpsSeqRcvyResets | counter | R | 10.8.9 |
| frerCpsSeqRcvyLatentErrorResets | counter | R | 10.8.10 |
| frerCpsSeqEncErroredPackets | counter | R | 10.8.11 |

*R = read-only access.

No further managed objects are specifically required by this profile for per-stream FRER objects.

# 8. Profiles

## 8.1 Introduction

This clause summarizes conformant profiles in line item detail by reference to individual IEEE 802 standards and other standards described in Clause 7 and as specified in Clause 5.

*<< Editor's Note: This Clause (still in progress) provides an easy to read summary of the profile and does not replace Clause 5. Comments on either keeping or removing this clause from the standard are invited.>>*

Bridges and end stations that provide TSN capabilities and that are used in aerospace applications are expected to conform with the generic IEEE Std 802.1Q standards for bridges and end stations and then additionally support the TSN standards required to implement the aerospace networks described in Clause 7.

To relate TSN conformance to the required aerospace functions this clause links the required functionality to the base TSN standards for bridge equipment and end stations in line with the descriptions in 7 whilst remaining consistent with the conformance described in 5.

## 8.2 Shaping, Policing and Isolation Requirements

To support implementation of TSN in aerospace applications a set of common feature capabilities are required for all bridges and end stations. These form the basis for all subsequent synchronous and redundancy capabilities used in the aerospace network. The functionality required for Bridges and end stations to perform Shaping, Policing and Isolation functions (in line with 7.2, 7.3 and 7.4) are described in the following tables, 8-1 and 8-2.

**Table 8-1—Bridge Common Features**

| TSN Feature Description | Reference | Conditions |
|---|---|---|
| Strict priority algorithm | IEEE Std 802.1Q-2022, 8.6.8.1 | |
| Credit-based shaper algorithm | EEE Std 802.1Q, 8.6.8.2 | supported on all ports for at least 2 traffic classes |
| Per-Stream Filtering and Policing (PSFP) | IEEE Std 802.1Q-2022, 8.6.5.2 items a), b), and c) | 1) Support maximum SDU size filtering according to IEEE Std 802.1Q-2022, 8.6.5.3.1<br>2) Support flow metering according to IEEE Std 802.1Q-2022, 8.6.5.5<br>3) Support monitoring of PSFP as specified in 7.7.2.4 |
| Stream identification and filtering entries | IEEE Std 802.1Q-2022, 8.6.5.3 | 7, Table 7-1 or Table 7-2 as appropriate for low or high stream count Bridges |

**Table 8-2—End Station Common Features**

| TSN Feature Description | Reference | Conditions |
|---|---|---|
| Credit-based shaper algorithm | EEE Std 802.1Q, 8.6.8.2 | on all ports for at least 2 traffic classes |

## 8.3 Time Synchronization

The functionality required for Bridges and end stations to perform Time Synchronization functions (in line with 7.1) are described in the following tables, 8-3 and 8-4.

**Table 8-3—Bridge Time Synchronization Features**

| TSN Feature Description | Reference | Asynchronous Profile | | Synchronous Profile | |
|---|---|---|---|---|---|
| | | Type 1 | Type 2 | Type 1 | Type 2 |
| PTP instances | IEEE Std 802.1AS-2020 | No | No | ≥3 | ≥3 |
| External port configuration | IEEE Std 802.1AS-2020, 5.4.2 item g | No | No | Yes (on all ports) | Yes (on all ports) |
| PTP fault-tolerant timing module | 7.1.2 | No | No | Yes | Yes |
| Enhancements for scheduled traffic | IEEE Std 802.1Q-2022, 8.6.8.4 | No | No | Yes (on all ports) | Yes (on all ports) |

**Table 8-4—End Station Time Synchronization Features**

| TSN Feature Description | Reference | Asynchronous Profile | | Synchronous Profile | |
|---|---|---|---|---|---|
| | | Type 1 | Type 2 | Type 1 | Type 2 |
| PTP instances | IEEE Std 802.1AS-2020 | No | No | ≥3 | ≥3 |
| External port configuration | IEEE Std 802.1AS-2020, 5.4.2 item g | No | No | Yes (on all ports) | Yes (on all ports) |
| PTP fault-tolerant timing module | 7.1.2 | No | No | Yes | Yes |
| Enhancements for scheduled traffic | IEEE Std 802.1Q-2022, 5.25 | No | No | Yes | Yes |

## 8.4 Network Redundancy

The functionality required for Bridges and end stations to provide network redundancy (in line with 7.5) are described in the following tables, 8-5 and 8-6.

**Table 8-5—Bridge Network Redundancy Features**

| TSN Feature Description | Reference | Asynchronous Profile | | Synchronous Profile | |
|---|---|---|---|---|---|
| | | Type 1 | Type 2 | Type 1 | Type 2 |
| FRER | IEEE Std 802.1CB-2017, 5.15 | No | Yes | No | Yes |

**Table 8-6—End Station Network Redundancy Features**

| TSN Feature Description | Reference | Asynchronous Profile | | Synchronous Profile | |
|---|---|---|---|---|---|
| | | Type 1 | Type 2 | Type 1 | Type 2 |
| FRER Talker | IEEE Std 802.1CB-2017, 5.6 | No | Yes | No | Yes |
| FRER Listener | IEEE Std 802.1CB-2017, 5.9 | No | Yes | No | Yes |

# Annex A

(normative)

# PICS proforma—IEEE Std 802.1DP Aerospace TSN Networking[10]

*<< Editor’s Note: This Annex has not been worked and is subject to change. Comments on content are not expected but suggestions for content are invited.>>*

## A.1 Introduction

The supplier of a protocol implementation that is claimed to conform to this standard shall complete the following Protocol Implementation Conformance Statement (PICS) proforma.

A completed PICS proforma is the PICS for the implementation in question. The PICS is a statement of which capabilities and options of the protocol have been implemented. The PICS can have a number of uses, including use

a) By the protocol implementer, as a checklist to reduce the risk of failure to conform to the standard through oversight.
b) By the supplier and acquirer—or potential acquirer—of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma.
c) By the user—or potential user—of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSs).
d) By a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

## A.2 Abbreviations and special symbols

### A.2.1 Status symbols

| | |
|---|---|
| M | mandatory |
| O | optional |
| *O.n* | optional, but support of at least one of the group of options labeled by the same numeral n is required |
| X | prohibited |
| pred: | conditional-item symbol, including predicate identification: see A.3.4 |
| ¬ | logical negation, applied to a conditional item’s predicate |

### A.2.2 General abbreviations

| | |
|---|---|
| N/A | not applicable |
| PICS | Protocol Implementation Conformance Statement |

[10] *Copyright release for PICS proformas:* Users of this standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS.

## A.3 Instructions for completing the PICS proforma

### A.3.1 General structure of the PICS proforma

The first part of the PICS proforma, implementation identification and protocol summary, is to be completed as indicated with the information necessary to identify fully both the supplier and the implementation.

The main part of the PICS proforma is a fixed-format questionnaire, divided into several subclauses, each containing a number of individual items. Answers to the questionnaire items are to be provided in the rightmost column, either by simply marking an answer to indicate a restricted choice (usually Yes or No) or by entering a value or a set or range of values. (Note that there are some items where two or more choices from a set of possible answers can apply; all relevant choices are to be marked.)

Each item is identified by an item reference in the first column. The second column contains the question to be answered; the third column records the status of the item—whether support is mandatory, optional, or conditional: see also A.3.4. The fourth column contains the reference or references to the material that specifies the item in the main body of this standard, and the fifth column provides the space for the answers.

A supplier may also provide (or be required to provide) further information, categorized as either Additional Information or Exception Information. When present, each kind of further information is to be provided in a further subclause of items labeled Ai or Xi, respectively, for cross-referencing purposes, where i is any unambiguous identification for the item (e.g., simply a numeral). There are no other restrictions on its format and presentation.

A completed PICS proforma, including any Additional Information and Exception Information, is the Protocol Implementation Conformation Statement for the implementation in question.

NOTE—Where an implementation is capable of being configured in more than one way, a single PICS may be able to describe all such configurations. However, the supplier has the choice of providing more than one PICS, each covering some subset of the implementation’s configuration capabilities, in case that makes for easier and clearer presentation of the information.

### A.3.2 Additional information

Items of Additional Information allow a supplier to provide further information intended to assist the interpretation of the PICS. It is not intended or expected that a large quantity will be supplied, and a PICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations, or information about aspects of the implementation that are outside the scope of this standard but that have a bearing on the answers to some items.

References to items of Additional Information may be entered next to any answer in the questionnaire and may be included in items of Exception Information.

### A.3.3 Exception information

It may occasionally happen that a supplier will wish to answer an item with mandatory status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No preprinted answer will be found in the Support column for this item. Instead, the supplier shall write the missing answer into the Support column, together with an *Xi* reference to an item of Exception Information, and shall provide the appropriate rationale in the Exception item itself.

An implementation for which an Exception item is required in this way does not conform to this standard.

NOTE—A possible reason for the situation described previously is that a defect in this standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

## A.3.4 Conditional status

### A.3.4.1 Conditional items

The PICS proforma contains a number of conditional items. These are items for which both the applicability of the item itself, and its status if it does apply—mandatory or optional—are dependent on whether certain other items are supported.

Where a group of items is subject to the same condition for applicability, a separate preliminary question about the condition appears at the head of the group, with an instruction to skip to a later point in the questionnaire if the "Not Applicable" answer is selected. Otherwise, individual conditional items are indicated by a conditional symbol in the Status column.

A conditional symbol is of the form "**pred:** S" where **pred** is a predicate as described in A.3.4.2 below, and S is a status symbol, M or O.

If the value of the predicate is true (see A.3.4.2), the conditional item is applicable, and its status is indicated by the status symbol following the predicate: The answer column is to be marked in the usual way. If the value of the predicate is false, the "Not Applicable" (N/A) answer is to be marked.

### A.3.4.2 Predicates

A predicate is one of the following:

a) An item-reference for an item in the PICS proforma: The value of the predicate is true if the item is marked as supported and is false otherwise.
b) A predicate-name, for a predicate defined as a boolean expression constructed by combining item-references using the boolean operator OR: The value of the predicate is true if one or more of the items is marked as supported.
c) The logical negation symbol "¬" prefixed to an item-reference or predicate-name: The value of the predicate is true if the value of the predicate formed by omitting the "¬" symbol is false, and vice versa.

Each item whose reference is used in a predicate or predicate definition, or in a preliminary question for grouped conditional items, is indicated by an asterisk in the Item column.

# A.4 PICS proforma—IEEE Std 802.1DP Aerospace TSN Networking

## A.4.1 Implementation identification

| | |
|---|---|
| Supplier | |
| Contact point for queries about the PICS | |
| Implementation Name(s) and Version(s) | |
| Other information necessary for full identification, e.g., name(s) and version(s) of machines and/or operating system names | |
| NOTE 1—Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.<br>NOTE 2—The terms “Name” and “Version” should be interpreted appropriately to correspond with a supplier’s terminology (e.g., Type, Series, Model). | |

## A.4.2 Protocol summary

| | |
|---|---|
| Identification of protocol specification | IEEE Std 802.1DP-<year>, IEEE Standard for Time-Sensitive Networking for Aerospace Ethernet Communications |
| Identification of amendments and corrigenda to the PICS proforma that have been completed as part of the PICS | Amd. : Corr. :<br>Amd. : Corr. : |
| Have any Exception items been required? (See A.3.3: the answer “Yes” means that the implementation is not conformant). | No [ ] Yes [ ] |

| | |
|---|---|
| Date of Statement | |

*<< Editor's Note: This Annex has not been worked and is subject to change. Comments on content are not expected but suggestions for content are invited.>>*

## A.5 Major capabilities

| Item | Feature | Status | References | Support |
|---|---|---|---|---|
| | If the implementation is an end station implementation, mark "N/A" and continue at Annex B. | | | N/A [ ] |
| MAC | Do the implementations of MAC technologies and support of the MAC Internal Sublayer Service (ISS) conform to MAC standards as specified in IEEE Std 802.1AC?<br>(If support of a specific MAC technology is claimed, any PICS proforma(s) required by the standard specifying that technology shall also be completed.) | M | A.6,<br>IEEE<br>Std 802.1AC | Yes [ ] |
| LLC | Is a class of LLC supporting Type 1 operations supported on all Bridge Ports in conformance with ISO/IEC 8802-2? (The PICS proforma required by ISO/IEC 8802-2 shall also be completed.) | M | 8.2, 8.3, 8.1.3, ISO/IEC 8802-2 | Yes [ ] |
| RLY | Does the implementation relay and filter frames as specified? | M | 8.5, 8.6, 8.7, 6.12, 8.8, A.7 | Yes [ ] |
| BFS | Does the implementation maintain the information required to make frame filtering decisions and support Basic Filtering Services? | M | 8.1, 8.5, 8.7, 8.8, A.8 | Yes [ ] |
| ADDR | Does the implementation conform to the provisions for addressing? | M | 8.13, A.9 | Yes [ ] |
| MBRIDGE | Can the Bridge be configured to operate as a VLAN-unaware MAC Bridge | O.2 | 5.14 | Yes [ ] No [ ] |
| TPMR | Can the Bridge be configured to operate as a Two Port MAC Relay? | O.2 | 5.16 | Yes [ ] No [ ] |
| MSP | Is the operation of the MAC Status Propagation Entity (MSPE) supported? | TPMR: M | Clause 23 | Yes [ ] N/A [ ] |
| IMP | Are the required implementation parameters included in this completed PICS? | M | 8.8, A.12 | Yes [ ] |
| PERF | Are the required performance parameters included in this completed PICS?<br>(Operation of the Bridge within the specified parameters shall not violate any of the other conformance provisions of this standard.) | M | 8.5, A.13 | Yes [ ] |
| MGT | Is management of the Bridge supported? | O<br>PBBTE OR<br>TPMR OR<br>SRRM:M | Clause 5, A.14 | Yes [ ] No [ ] |
| RMGT | Is a remote management protocol supported? | MGT:O<br>PBBTE OR<br>TPMR OR<br>SRRM:M | Clause 5, A.15 | Yes [ ] No [ ] |
| MIB | Does the system implementation support management operations using SMIv2 MIB modules? | MGT:O | 8.12, Clause 17 | Yes [ ] No [ ]<br>N/A [ ] |

## A.5 Major capabilities *(continued)*

| Item | Feature | Status | References | Support |
|---|---|---|---|---|
| MVRP | Is automatic configuration and management of VLAN topology using MVRP supported? | ¬(TPMR OR MBRIDGE):M<br>TPMR:X | 5.4, A.21 | Yes [ ] No [ ] |
| MRP | Is the Multiple Registration Protocol (MRP) implemented in support of MRP Applications? | MMRP:M<br>MVRP:M | Clause 10, A.20, A.21, A.22 | Yes [ ] N/A [ ] |
| MSTP | Is MSTP implemented? | ¬TPMR:O.1<br>TPMR:X | Clause 5, Clause 7, 8.4, 8.6.1, 8.8.8, 8.9, 8.10, 8.13.7, 11.2.3.1.2, Clause 13, Clause 14, A.18 | Yes [ ] No [ ] |
| VMGT | Does the implementation support VLAN management operations? | ¬(TPMR OR MBRIDGE) AND MGT:O<br>(MBRIDGE OR TPMR):X | 5.4.1, 12.10.2, 12.10.3 | Yes [ ] No [ ]<br>N/A [ ] |
| CB | Can the Bridge be configured to operate as a C-VLAN Bridge, recognizing and using C-TAGs? | O.2 | 5.9 | Yes [ ] No [ ] |
| PB-2 | State which Ports support the following values for the Provider Bridge Port Type:<br>— PNP<br>— CNP<br>— CEP<br>— RCAP | PB:M | 5.10 | <br><br>Ports: _____<br>Ports: _____<br>Ports: _____<br>Ports: _____ |
| BEB-I | Can the Bridge be configured to operate as a Backbone Edge Bridge with one or more Ports operating as a Provider Instance Port (PIP)? | BEB: O.3 | 5.12 | Yes [ ] No [ ]<br>N/A [ ] |
| BEB-1 | State which Ports support the following values for the Backbone Edge Bridge Port Type:<br>— PIP<br>— CNP<br>— PNP<br>— CBP<br>— CEP<br>— RCAP | BEB: M | 5.11 | <br><br>PIP: _____<br>CNP: _____<br>PNP: _____<br>CBP: _____<br>CEP: _____<br>RCAP: _____ |
| DDCFM | Is management of data-driven and data-dependent connectivity faults implemented? | O | Clause 19, Clause 29 | Yes [ ] No [ ] |
| PBBTE | Can the Bridge be configured by an external agent to provide TESIs? | O | 8.4, 8.9, 25.10 | Yes [ ] No [ ] |

## A.6 Media access control methods

| Item | Feature | Status | References | Support |
|---|---|---|---|---|
| | Which media access control methods are implemented in conformance with the relevant MAC Standards? | | 5.4,<br>IEEE Std 802.1AC | |
| MAC-802.3 | Ethernet, IEEE Std 802.3 | O.2 | IEEE Std 802.1AC | Yes [ ] No [ ] |
| MAC-802.11-PORT | IEEE 802.11 LAN Portal,<br>IEEE Std 802.11 | O.2 | G.4.1,<br>IEEE Std 802.1AC | Yes [ ] No [ ] |
| MAC-PMPN-N | PMPN multiple port, IEEE Std 802.1AC | O.2 | G.4.1,<br>IEEE Std 802.1AC | Yes [ ] No [ ] |
| MAC-PMPN-1 | PMPN single port, IEEE Std 802.1AC | O.2 | G.4.1,<br>IEEE Std 802.1AC | Yes [ ] No [ ] |
| MAC-802.20-WB | IEEE 802.20™ Wideband Mode | O.2 | IEEE Std 802.1AC | Yes [ ] No [ ] |
| MAC-802.20-625 | IEEE 802.20 625k-MC Mode | O.2 | IEEE Std 802.1AC | Yes [ ] No [ ] |
| MAC-1 | Has a PICS been completed for each of the media access control methods implemented as required by the relevant MAC standards? | M | | Yes [ ] |
| MAC-2 | Do all the media access control methods implemented support the MAC ISS as specified? | M | IEEE Std 802.1AC | Yes [ ] |
| MAC-3 | Are the adminPointToPointMAC and operPointToPointMAC parameters implemented on all Ports? | M | IEEE Std 802.1AC | Yes [ ] |
| MAC-4 | Does the implementation support the use of the adminEdgePort and operEdgePort parameters on any Ports? | O | 13.27.1, 13.27.44 | Yes [ ] No [ ] |
| MAC-4a | State which Bridge Ports support the adminEdgePort and operEdgePort parameters. | | | Ports_______ |
| MAC-5 | Is the priority of received frames set to the Default Priority where specified for the MAC? | M | IEEE Std 802.1AC | Yes [ ] |
| MAC-6 | Can the Default Priority be set for each Port? | O | IEEE Std 802.1AC | Yes [ ] No [ ] |
| MAC-7 | Can the Default Priority be set to any of 0–7? | MAC-6:M | IEEE Std 802.1AC | Yes [ ] N/A [ ] |
| MAC-12 | Is the minimum tagged frame length that can be transmitted on IEEE 802.3 Ports less than 68 (but 64 or more) octets? | MAC-802.3:O | IEEE Std 802.1AC | Yes [ ] No [ ]<br>N/A [ ] |

# Annex B

(informative)

# Bibliography

*<<Editor’s Note: This list as well as the Normative References (Clause 2) are work in progress, comments on moving documents between them or adding others are invited!>>*

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] Alizadeh, M., B. Atikoglu, A. Kabbani, A. Lakshmikantha, R. Pan, B. Prabhakar, and M. Seaman, “Data Center Transport Mechanisms: Congestion Control Theory and IEEE Standardization,” *Proceedings of The 46th Annual Allerton Conference on Communication, Control and Computing*, Urbana-Champaign, Sept. 2008, Invited paper.

[B2] ARINC Specification 664 part 7,

[B3] Asynchronous Transfer Mode (ATM): A collection of equipment and standards used for telecommunications and data transfer, https://www.itu.int/ITU-T/ and https://www.broadband-forum.org.

[B4] Binary Increase Congestion control—Transmission Control Protocol (BIC-TCP), http://www4.ncsu.edu/~rhee/export/bitcp.pdf.

[B5] Calculating the Delay Added by Qav Stream Queue, http://www.ieee802.org/1/files/public/docs2009/av-fuller-queue-delay-calculation-0809-v02.pdf.

[B6] IEC 62439-3:2016, Industrial communications networks — High availability automation networks — Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).

[B7] IEEE Std 802™-2014, IEEE Standard for Local and metropolitan area networks—Overview and Architecture.[11,12]

[B8] IEEE Std 802.1AB™-2005, IEEE Standard for Local and metropolitan area networks—Station and Media Access Control Connectivity Discovery.

[B9] IEEE Std 802.1AB™-2009, IEEE Standard for Local and metropolitan area networks—Station and Media Access Control Connectivity Discovery.

[B10] IEEE Std 802.1AC™-2016, IEEE Standard for Local and Metropolitan area networks—Media Access Control (MAC) Service Definition.

[B11] IEEE Std 802.1AS™-2020, IEEE Standard for Local and Metropolitan Area Networks—Timing and Synchronization for Time-Sensitive Applications

[B12] IEEE Std 802.1BA™, IEEE Standard for Local and metropolitan area networks—Audio Video Bridging (AVB) Systems.

[B13] IEEE Std 802.1D™, 1993 Edition [ISO/IEC 10038:1993], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local area networks—Media Access Control (MAC) bridges.

[11] IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://standards.ieee.org/).
[12] The IEEE standards or products referred to in this annex are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

[B14] IEEE Std 802.1D™, 1998 Edition [ISO/IEC 15802-3:1998], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 3: Media Access Control (MAC) Bridges.

[B15] IEEE Std 802.1D™-2004, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Bridges.

[B16] IEEE Std 802.1Q™-2022, IEEE Standard for Local and metropolitan area networks—Bridges and Bridged Networks

[B17] IEEE Std 802.3™-2018, IEEE Standard for Ethernet.

[B18] IEEE Std 802.11™-2016, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[B19] IEEE Std 1588-2019, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurements and Control Systems.

[B20] IEEE Std 1722™, IEEE Standard for Layer 2 Transport Protocol for Time Sensitive Applications in Bridged Local Area Networks.

NOTE—See Figure 5.3 for the ABTP common stream data header format. Also see IEC 61883-6, Consumer audio/video equipment—Digital Interface—Part 6: Audio and music data transmission protocol, Second edition, 2005-10, and IEC 61883-4, Consumer audio/video equipment—Digital Interface—Part 4: MPEG2-TS data transmission, Second edition, 2004-08.

[B21] IETF RFC 791, Internet Protocol—DARPA Internet Program Protocol Specification, Sept. 1981.[13]

[B22] IETF RFC 793 (STD0007), Transmission Control Protocol, Sept. 1981, https://tools.ietf.org/html/rfc793.

[B23] IETF RFC 1321, The MD5 Message-Digest Algorithm, Apr. 1992, https://tools.ietf.org/html/rfc2321.

[B24] IETF RFC 1633, Integrated Services in the Internet Architecture: An Overview, June 1994, https://tools.ietf.org/html/rfc1633.

[B25] IETF RFC 2210, The Use of RSVP with IETF Integrated Services, Sept. 1997, https://tools.ietf.org/html/rfc2210.

[B26] IETF RFC 2211, Specification of the Controlled-Load Network Element Service, Sept. 1997, https://tools.ietf.org/html/rfc2211.

[B27] IETF RFC 2212, Specification of Guaranteed Quality of Service, Sept. 1997, https://tools.ietf.org/html/rfc2212.

[B28] IETF RFC 2215, General Characterization Parameters for Integrated Service Network Elements, Sept. 1997, https://tools.ietf.org/html/rfc2215.

[B29] IETF RFC 2475, An Architecture for Differentiated Services, Dec. 1998, https://tools.ietf.org/html/rfc2475.

[B30] IETF RFC 2597, Assured Forwarding PHB Group, June 1999, https://tools.ietf.org/html/rfc2597.

[B31] IETF RFC 2814, SBM (Subnet Bandwidth Manager): A Protocol for Admission Control over IEEE 802-style Networks, May 2000, https://tools.ietf.org/html/rfc2814.

[13] IETF documents (i.e., RFCs) are available from the Internet Engineering Task Force (https://www.rfc-editor.org/).

[B32] IETF RFC 2815, Integrated Service Mappings on IEEE 802 Networks, May 2000, https://tools.ietf.org/html/rfc2815.

[B33] IETF RFC 2816, A Framework for Providing Integrated Services Over Shared and Switched LAN Technologies, May 2000, https://tools.ietf.org/html/rfc2816.

[B34] IETF RFC 2863, The Interfaces Group MIB, June 2000, https://tools.ietf.org/html/rfc2863.

[B35] IETF RFC 3031 (Proposed standard), Multiprotocol Label Switching Architecture; The Internet Society, https://tools.ietf.org/html/rfc3031.

[B36] IETF RFC 3246, An Expedited Forwarding PHB (Per-Hop Behavior), Mar. 2002, https://tools.ietf.org/html/rfc3246.

[B37] IETF RFC 3270, Multi-Protocol Label Switching (MPLS) Support of Differentiated Services, May 2002, https://tools.ietf.org/html/rfc3270.

[B38] IETF RFC 4655, A Path Computation Element (PCE)-Based Architecture (Informational RFC), Aug. 2006, https://tools.ietf.org/html/rfc4655.

[B39] IETF RFC 4663, Transferring MIB Work from IETF Bridge MIB WG to IEEE 802.1, Sept. 2006, https://tools.ietf.org/html/rfc4663.

[B40] IETF RFC 4960, Stream Control Transmission Protocol, Sept. 2007, https://tools.ietf.org/html/rfc4960.

[B41] IETF RFC 5306, Restart Signalling for IS-IS, Oct. 2008, https://tools.ietf.org/html/rfc5306.

[B42] IETF RFC 5681, TCP Congestion Control, Sept. 2009, https://tools.ietf.org/html/rfc5681.

[B43] IETF RFC 6087, Guidelines for Authors and Reviewers of YANG Data Model Documents, January 2011.

[B44] IETF RFC 6241, Network Configuration Protocol (NETCONF), June 2011.

[B45] IETF RFC 6242, Using the NETCONF Protocol over Secure Shell (SSH), June 2011.

[B46] IETF RFC 6328, IANA Considerations for Network Layer Protocol Identifiers, July 2011, https://tools.ietf.org/html/rfc6328.

[B47] IETF RFC 6329, IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging, Apr. 2012, https://tools.ietf.org/html/rfc6329.

[B48] IETF RFC 6536, Network Configuration Protocol (NETCONF) Access Control Model, March 2012.

[B49] IETF RFC 6762, Multicast DNS, Feb. 2013.

[B50] IETF RFC 6991, Common YANG Data Types, July 2013.

[B51] IETF RFC 7223, A YANG Data Model for Interface Management, May 2014.

[B52] IETF RFC 7224, IANA Interface Type YANG Module, May 2014.

[B53] IETF RFC 7317, A YANG Data Model for System Management, August 2014.

[B54] IETF RFC 7319, IANA Considerations for Connectivity Fault Management (CFM) Code Points, July 2014, https://tools.ietf.org/html/rfc7319.

[B55] IETF RFC 7813, IS-IS Path Control and Reservation, 2016, https://tools.ietf.org/html/rfc7813.

[B56] IETF RFC 7950, The YANG 1.1 Data Modeling Language, August 2016.

[B57] IETF RFC 8040, RESTCONF Protocol, January 2017.

[B58] IETF RFC 8069, URN Namespace for IEEE, February 2017.

[B59] IETF RFC 8200, Internet Protocol, Version 6 (IPv6) Specification, July 2017, https://tools.ietf.org/html/rfc8200.

[B60] ISO 6937-2, Information technology—Coded graphic character set for text communication—Latin alphabet.[14]

[B61] ISO/IEC TR 11802-1:1997, Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Technical Reports and Guidelines—Part 1. The Structure and Coding of Logical Link Control Addresses in Local Area Networks.[15]

[B62] ITU-T Recommendation G.806, Characteristics of transport equipment — Description methodology and generic functionality.[16]

[B63] ITU-T Recommendation G.8031/Y.1342, Ethernet linear protection switching.

[B64] ITU-T Recommendation I.610 (02/1999), B-ISDN operation and maintenance principles and functions.

[B65] ITU-T Recommendation X.25 (10/1996), Public Data Networks: Interfaces—Interfaces between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit.

[B66] MEF Technical Specification 4 (MEF 4), Metro Ethernet Network Architecture Framework—Part 1: Generic Framework, May 2004.[17]

[B67] MEF Technical Specification 16 (MEF 16), Ethernet Local Management Interface (E-LMI).

[B68] MEF Technical Specification 26 (MEF 26), External Network Network Interface (ENNI)—Phase 1.

[B69] MEF 35.1, Service OAM Performance Monitoring Agreement

[B70] MoCA MAC/PHY Specification Extensions v1.1, MoCA-M/P-SPEC-V1.1-06162009, Multimedia over Coax Alliance (MoCA), June 16, 2009.[18]

[B71] MoCA MAC/PHY Specification v2.0, MoCA_Specification_v2-131121, Nov. 2013.

[B72] Multiprotocol Label Switching (MPLS): A standard for label-based forwarding in an IP network. The standard is specified in several RFCs, (see https://datatracker.ietf.org/doc/charter-ietf-mpls/) and ITU-T recommendations (see https://www.itu.int/ITU-T/).

[B73] OMG Unified Modeling Language (OMG UML), Version 2.5, March 2015.

[B74] Peristaltic Shaper: updates, multiple speeds, Michael Johas Teener, 23 Jan. 2014, https://www.ieee802.org/1/files/public/docs2014/new-tsn-mjt-peristaltic-shaper-0114.pdf.

[14] ISO publications are available from the International Organization for Standardization (https://www.iso.org/).

[15] ISO/IEC publications are available from the International Organization for Standardization (https://www.iso.org/). ISO/IEC publications are also available in the United States from Global Engineering Documents (https://global.ihs.com/). Electronic copies are available in the United States from the American National Standards Institute (https://www.ansi.org/).

[16] ITU-T publications are available from the International Telecommunications Union (https://www.itu.int/).

[17] MEF standards are available from the MEF Forum (https://www.mef.net/).

[18] MoCa publications are available from the Multimedia over Coax Alliance (http://mocalliance.org).

[B75] Seaman, Mick, *Preemption and MACsec replay protection,* Nov. 2014, https://www.ieee802.org/1/files/public/docs2014/ae-seaman-preemption-1114-v04.pdf.

[B76] SMPTE 259M-2008, SMPTE Standard for Television—SDTV Digital Signal/Data—Serial Digital Interface, 2008. See section 8.[19]

[B77] SMPTE 292M-2008, SMPTE Standard 1.5 Gb/s Signal/Data Serial Interface, 2008. See sub 4.3.

[B78] SMPTE 424M-2008, SMPTE Standard for Television—3 Gb/s Signal/Data Serial Interface, 2008. See sub 4.3.

[B79] Specht, J., and S. Samii, "Urgency-Based Scheduler for Time-Sensitive Switched Ethernet Networks," *28th Euromicro Conference on Real-Time Systems (ECRTS)*, pp. 75–85, 2016.

[B80] Jabbar-et-al, Aerospace Traffic Characterization, https://www.ieee802.org/1/files/public/docs2021/dp-Jabbar-et-all-Aerospace-Traffic-Characterization-0421-v02.pdf.

[B81] RTCA DO-178C,

[19] SMPTE publications are available from the Society of Motion Picture and Television Engineers (https://www.smpte.org).

# Annex C

(informative)

# Example Aerospace Configuration

*<< Editor's Note: This Annex is work in progress and subject to change. Comments on content are invited.>>*

## C.1 Introduction

In the highly regulated aerospace industry, the generation of complex network configurations is required to be traceable to system level requirements to ensure that the system behavior is that which was intended and that unintended behavior is eliminated. TSN network configurations are no exception to this and system integrators will often rely on tooling to develop the configurations used in the equipment that makes up the system for which TSN is being used.

aerospace applications use a fully centralized configuration model to define an engineered static network topology. This profile for TSN aerospace communications does not specify the process by which configurations are loaded into the network but leaves that to the integrator to define. This Annex is intended to provide an example for how this might be achieved in a typical commercial aerospace application.

An example for an aerospace configuration model is provided in Figure C-1 and explained below.

In the example provided here it is expected that some form of modeling tool is used to design the network topology and streams required by the application. Depending upon the complexity of the required system and on the expectation for through-life support and modification, this could be as simple as a series of spreadsheets or a sophisticated model-based engineering tool capable of supporting complex analysis plug-ins. The main point being that the configuration process can be maintained for the life of the system controlled

TSN standards make no mention of how a system might be configured to perform a specified user function but instead provide the building blocks from which a variety of systems can be built. It is then up to users and integrators to decide how these standards are combined to implement the desired functionality. In an aerospace application it is expected that system level requirements will be defined to support safety assessments and that these will require consistency and performance checks to be made on the output of the configuration step.

Whilst TSN configurations will use YANG configuration models, 7.6.2, aerospace equipment is expected to use vendor-specific binary configurations that are generated from the YANG models. Vendor supplied configuration tools are therefore expected to be supplied with equipment that performs translation from YANG models to vendor-specific binary data and that performs verification on the output to show that it matches the configuration requirements described in the YANG model. The expectation would then be that the configuration tool and verifier are qualified tools following guidance provided by DO-178C [B81].

Once the vendor-specific binary configuration data has been generated, this data can then be loaded into equipment that makes up the system to configure the Bridges and end stations that constitute the time-sensitive network. Aerospace norms suggest here that ARINC specifications are used to define how this is performed, in particular with data provided as loadable software according to ARINC 665 and loaded using an ARINC 615-A compliant data loader (Bibliography additions needed).

The topology and configurations are developed from requirements that represent the required system behavior. A design modeling tool is used to generate all input to centralized configuration models (CUC & CNC) from which individual device configurations are derived. Consistent with aerospace practice, no direct communications occur between the CUC/CNC and Bridges or end stations. Instead, individual file-based device configurations are created and loaded into equipment during manufacture or at major service events. Aerospace qualified tools are used at each stage of configuration development to verify that configurations are accurate representations of the user requirements with configuration control maintained for individually identifiable items. Figure 7-1 depicts the configuration model specified by the aerospace profile.

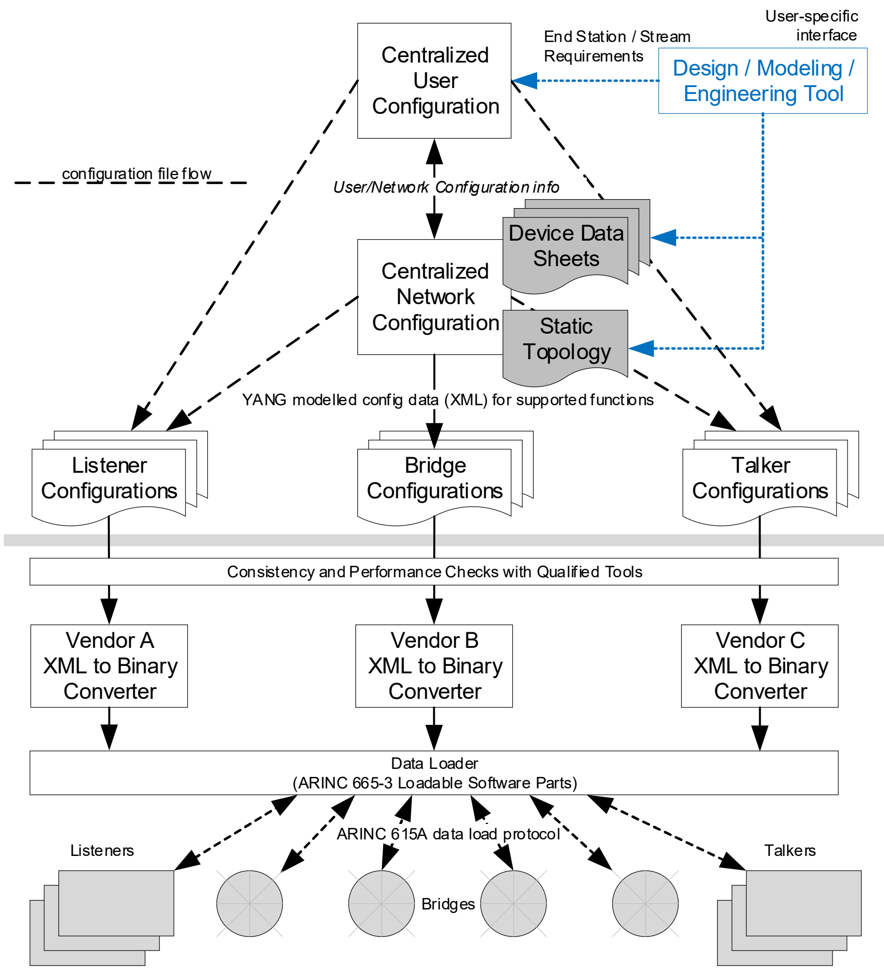


**Figure C-1—Aerospace Configuration Model Example**

# Annex D

(informative)

# Time Synchronization for Aerospace Systems

*<< Editor's Note: This Annex is work in progress and subject to change. Comments on content are invited.>>*

## D.1 Introduction

This Annex provides example patterns for time synchronization in aerospace systems.

Synchronous aerospace systems, i.e. those conforming the synchronous TSN Aerospace profile, are expected to tolerate multiple (typically 2) simultaneous arbitrary faults in end stations, Bridges, links, and GMs to maintain availability and integrity of time synchronization,

Fault-tolerance, or availability, and integrity address the reliable and accurate transmission of time values and the associated sync and follow-up messages in the presence of arbitrary faults in the network (link, Bridge, end station, and GM). Thus, under fault conditions, a correctly operating end station is expected to maintain a target maximum time error relative to the correctly operating GM. If unable to maintain the max time error, the correctly operating end station will detect an erroneous time sync state. To support this, it is expected that multiple clock domains, introduced in [B11], are configured and managed in the network.

## D.2 Clock Domain Management

As described in 7.1, clock domains can be considered dependent or independent. Independent clock domains, where clock sources are independent, are expected to present problems to the integrator because, at the time of writing, commercially available devices cannot be relied upon to support multiple independent PTP Instances at a single port. This makes it problematic to bridge synchronized traffic between domains. In Figure D-1, two clock domains D1 and D2 are shown overlapping at Bridges B2 and B3 with streams S1 and S2 sharing a common output port, P4, on B2. If the two clock domains are synchronized, Bridges B2 and B3 will synchronize to the common domain time and will be able to forward both of the streams to the downstream end stations. If however the two clock domains are not synchronized then a conflict can occur on the shared output port of B2. such that it must either maintain two PTP Instances on the shared output port, and widen the output windows to accommodate a potential conflict, or must forward one of the streams in an unsynchronized manner.

It is not possible for a device to support multiple unsynchronized gate schedules on a single output port, and aerospace networks using multiple PTP domains should therefore ensure that the clock domains are either dependent on a common clock source or are synchronized to each other by some other means.

Management of multiple PTP instances using a fault-tolerant timing module (FTTM) is discussed in 7.1.2.

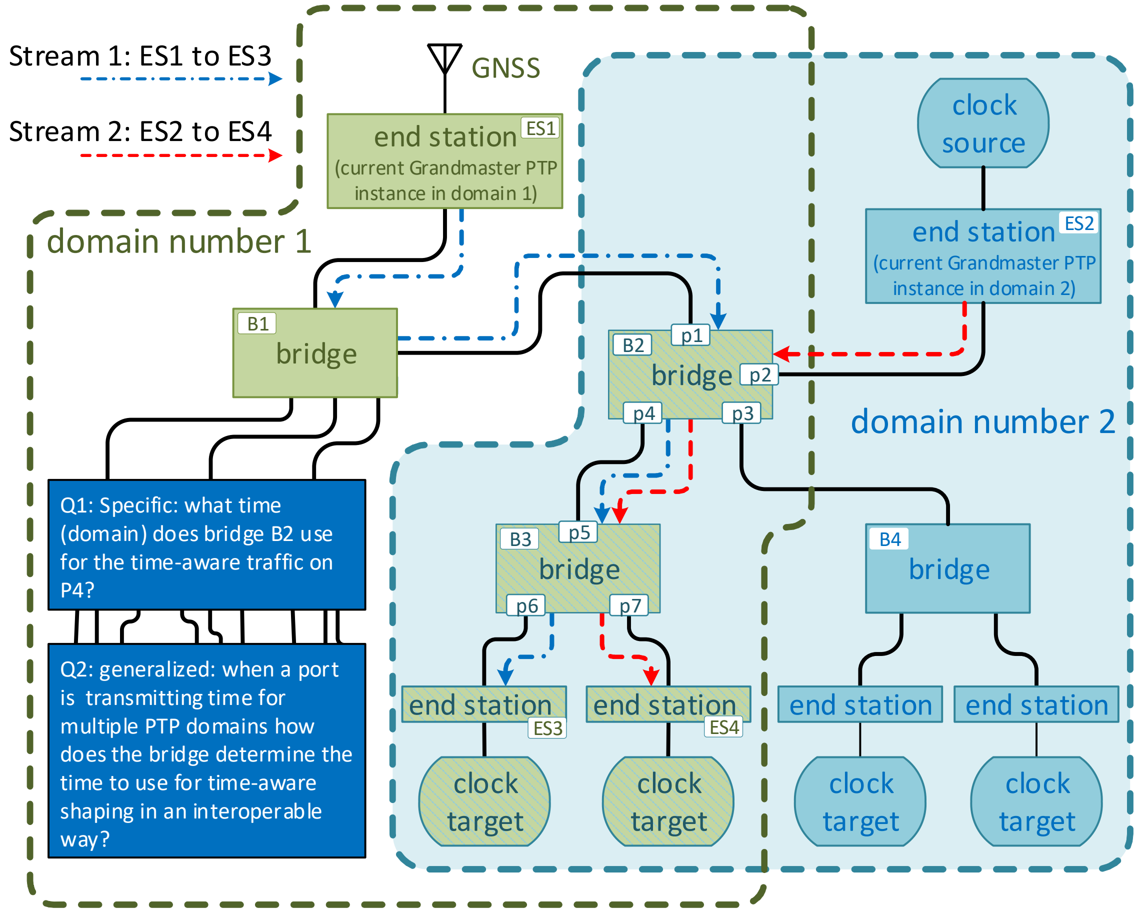


**Figure D-1—Multiple gPTP Domains with Shared Port**

## D.3 Time agreement generation examples

*<< Editor’s Note: Content for this subclause is expected to be provided in a future draft of this standard.>>*

## D.4 FTTM operation in example network topologies

*<< Editor’s Note: Content for this subclause is expected to be provided in a future draft of this standard.>>*

# Annex E

(informative)

# Security for Aerospace TSN Systems

*<< Editor's Note: This Annex is work in progress and subject to change. Comments on content are invited.>>*

## E.1 Introduction

This Annex provides example patterns for security in aerospace systems using time-sensitive networks.

.I

**Figure E-3— TBD Example**