



DPC: 23/30480980 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 06 October 2023

Origin: International

Latest date for receipt of comments: 01 November 2023

Project No. 2017/02526

Responsible committee: GEL/65 Measurement and control

Interested committees:

Title: Draft BS EN IEC/IEEE 60802 Time-sensitive networking profile for industrial automation.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 01 November 2023

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



65C/1273/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:

IEC/IEEE 60802 ED1

DATE OF CIRCULATION:

2023-10-06

CLOSING DATE FOR COMMENTS:

2023-12-01

SUPERSEDES DOCUMENTS:

65C/1251/CD, 65C/1264A/CC

IEC SC 65C : INDUSTRIAL NETWORKS

SECRETARIAT:

France

SECRETARY:

Ms Valérie DEMASSIEUX

OF INTEREST TO THE FOLLOWING COMMITTEES:

TC 57

PROPOSED HORIZONTAL STANDARD:

☐

Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.

FUNCTIONS CONCERNED:

☐ EMC

☐ ENVIRONMENT

☐ QUALITY ASSURANCE

☐ SAFETY

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any local regulations or technical reasons that may exist and should be considered should this proposal proceed, recognizing that failure to address such requirements could result in the need for new or existing "In Some Countries" clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

Time-sensitive networking profile for industrial automation

NOTE FROM TC/SC OFFICERS:

This sixth CD of the joint IEC/IEEE 60802 project is circulated in parallel with an IEEE 802.1 initial WG ballot. If your NC submits comments through the IEEE system, please avoid duplication of these comments through the IEC system.

The scope of this document has been updated to include additional types of YANG modules, please provide corresponding comments if you object to this addition.

Copyright © 2023 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

Documents
AA Document Sharing Hub

CONTENTS

FOREWORD	9
INTRODUCTION	11
1 Scope	12
2 Normative References	12
3 Terms, definitions, symbols, abbreviated terms and conventions	15
3.1 General	15
3.2 List of terms, abbreviated terms and definitions given in various standards	15
3.3 Terms defined in this document	18
3.4 Abbreviated terms and acronyms	19
3.5 Conventions	22
3.5.1 Convention for capitalizations	22
3.5.2 Unit conventions	22
3.5.3 Conventions for YANG contents	22
3.5.4 Conventions for YANG selection / Digital Datasheet	22
4 Overview of TSN in industrial automation	23
4.1 Industrial application operation	23
4.2 Industrial applications	24
4.2.1 General	24
4.2.2 Control loop tasks	26
4.2.3 Start of control loop tasks	27
4.3 IA-stations	27
4.4 Ethernet interface	28
4.5 Mechanisms that can be used to meet control loop latency requirements	29
4.6 Translation between middleware and network provisioning	29
4.6.1 Interfaces of type I2vlan	29
4.6.2 PTP Instances	31
4.7 Industrial traffic types	32
4.7.1 General	32
4.7.2 Traffic type characteristics	32
4.7.3 Traffic type categories	33
4.7.4 Traffic types	34
4.8 Security for TSN-IA	36
4.8.1 General	36
4.8.2 Security configuration model	36
4.8.3 NETCONF/YANG processing	37
4.8.4 NETCONF/YANG access control	38
4.8.5 Identity checking	38
4.8.6 Secure device identity	39
5 Conformance	41
5.1 General	41
5.2 Requirements terminology	42
5.3 Profile conformance statement (PCS)	42
5.4 Conformance classes	42
5.5 IA-station requirements	43
5.5.1 IA-station PHY and MAC requirements for external ports	43

48	5.5.2	IA-station topology discovery requirements.....	43
49	5.5.3	IA-station requirements for time synchronization.....	44
50	5.5.4	IA-station requirements for management	44
51	5.6	IA-station options.....	45
52	5.6.1	IA-station PHY and MAC options for external ports	45
53	5.6.2	IA-station options for time synchronization.....	46
54	5.6.3	IA-station options for management	46
55	5.7	Bridge component requirements.....	47
56	5.7.1	Common Bridge component requirements	47
57	5.7.2	ccA Bridge component requirements.....	48
58	5.7.3	ccB Bridge component requirements.....	48
59	5.8	Bridge component options.....	48
60	5.8.1	Common Bridge component options.....	48
61	5.8.2	ccA Bridge component options.....	48
62	5.8.3	ccB Bridge component options.....	49
63	5.9	End station component requirements	49
64	5.9.1	Common end station Component requirements.....	49
65	5.9.2	ccA end station component requirements	50
66	5.9.3	ccB end station component requirements	50
67	5.10	End station component options	50
68	5.10.1	Common end station component options	50
69	5.10.2	ccA end station component options	51
70	5.10.3	ccB end station component options	51
71	5.11	CNC requirements	52
72	5.12	CNC options	52
73	5.13	CUC requirements	52
74	5.14	CUC options	52
75	6	Required functions for an industrial network	52
76	6.1	General.....	52
77	6.2	Synchronization	52
78	6.2.1	General	52
79	6.2.2	PTP Instance requirements.....	52
80	6.2.3	PTP protocol requirements	53
81	6.2.4	Error Generation Limits.....	54
82	6.2.5	Clock states.....	57
83	6.2.6	Grandmaster PTP Instance requirements	57
84	6.2.7	Application framework	57
85	6.2.8	Working Clock domain framework.....	58
86	6.2.9	Global Time domain framework	59
87	6.2.10	IA-station model for clocks.....	59
88	6.2.11	Clock usage for the Ethernet interface	60
89	6.2.12	Error model	60
90	6.2.13	gPTP domains and PTP Instances.....	61
91	6.2.14	Split and combine cases for a PTP domain.....	62
92	6.3	Security model.....	64
93	6.3.1	General	64
94	6.3.2	Security functionality	65
95	6.3.3	IDeVID Profile	68
96	6.3.4	Security setup based on IDeVID.....	72

97	6.3.5	Secure configuration based on LDevID-NETCONF	75
98	6.4	Management	76
99	6.4.1	General	76
100	6.4.2	IA-station management model	76
101	6.4.3	Discovery of IA-station internal structure	81
102	6.4.4	Network engineering model	81
103	6.4.5	Operation	84
104	6.4.6	Engineered time-synchronization spanning tree	90
105	6.4.7	Diagnostics	92
106	6.4.8	Data sheet	95
107	6.4.9	YANG representation of managed objects and nodes	96
108	6.4.10	YANG Data Model	112
109	6.5	Topology discovery and verification	143
110	6.5.1	Topology discovery and verification requirements	143
111	6.5.2	Topology discovery overview	143
112	6.5.3	Topology verification overview	146
113	6.6	CNC	146
114	6.6.1	General	146
115	6.6.2	Stream destination MAC address range	146
116	Annex A (normative)	PCS proforma – Time-sensitive networking profile for industrial	
117		automation	148
118	A.1	General	148
119	A.2	Abbreviations and special symbols	148
120	A.2.1	Status symbols	148
121	A.2.2	General abbreviations	149
122	A.3	Instructions for completing the PCS proforma	149
123	A.3.1	General structure of the PCS proforma	149
124	A.3.2	Additional information	149
125	A.3.3	Exception information	149
126	A.3.4	Conditional status	150
127	A.3.5	Electronic datasheet	151
128	A.4	Common requirements	151
129	A.4.1	Instructions	151
130	A.4.2	Implementation identification	151
131	A.4.3	Profile summary, IEC/IEEE 60802	151
132	A.4.4	Implementation summary	151
133	A.5	IA-station Requirements and Options	152
134	A.5.1	Instructions	152
135	A.5.2	IA-station requirements	152
136	A.5.3	IA-station prohibited management features	152
137	A.5.4	IA-station PHY and MAC options for external ports	153
138	A.5.5	IA-station options for time synchronization	153
139	A.5.6	IA-station secure management exchange options	153
140	A.5.7	CNC Requirements	154
141	A.5.8	CUC Requirements	154
142	A.6	Bridge Component	155
143	A.6.1	Instructions	155
144	A.6.2	Bridge Component Requirements	155
145	A.6.3	Common Bridge Component Options	155

146	A.6.4	ccA Bridge Component Options	155
147	A.6.5	ccB Bridge Component Options	155
148	A.7	End Station Component	157
149	A.7.1	Instructions.....	157
150	A.7.2	Common End Station Component Requirements.....	157
151	A.7.3	Common End Station Component Options	157
152	A.7.4	ccA End Station Component Options	157
153	A.7.5	ccB End Station Component Options	157
154	Annex B (informative)	Representative Configuration Domain	159
155	Annex C (informative)	Description of Clock Control System	160
156	C.1	Clock control system introduction.....	160
157	C.2	Transfer function for control system	161
158	C.3	Frequency response for control system.....	162
159	C.4	Example	167
160	Annex D (informative)	Time Synchronization informative Annex.....	169
161	D.1	Overview	169
162	D.2	Principles of Operation	170
163	D.2.1	General	170
164	D.2.2	Grandmaster PTP Instance Implementation	171
165	D.2.3	Splitting, Joining and Aligning Time Domains.....	172
166	D.2.4	PTP Link Characteristics	173
167	D.3	Notes on Normative Requirements.....	173
168	D.3.1	Oscillator Requirements	173
169	D.3.2	Timestamp Granularity Error.....	173
170	D.3.3	Dynamic Timestamp Error	174
171	D.3.4	Grandmaster PTP Instance Error Generation Requirements	174
172	D.3.5	PTP Relay Instance	174
173	D.3.6	PTP End Instance.....	176
174	D.4	Approach to Testing Normative Requirements	176
175	D.4.1	General	176
176	D.4.2	Testing Grandmaster PTP Instance	177
177	D.4.3	Testing PTP Relay Instance.....	177
178	D.4.4	Testing PTP End Instance	180
179	D.5	Example Algorithms	181
180	D.5.1	General	181
181	D.5.2	Algorithm to Compensate for Errors in measured NRR due to Clock Drift	182
182	D.5.3	Measured NRR Algorithm – Startup Behaviour	183
183	D.5.4	Algorithm for Tracking RR Drift.....	184
184	D.5.5	Algorithm to Compensate for Errors in measured RR due to Clock Drift.....	184
185	D.5.6	Compensate for Errors in measured RR due to Clock Drift at PTP End Instance	186
186	D.5.7	Mean Link Delay Averaging	187
188	Bibliography.....		188
189			
190	Figure 1 – Data flow in a control loop.....		23
191	Figure 2 – IA-station interaction with CNC – Transmit path		25
192	Figure 3 – IA-station interaction with CNC – Receive path		26
193	Figure 4 – IA-station example		

194	Figure 5 – Model for cycles	28
195	Figure 6 – Traffic type translation example	30
196	Figure 7 – IETF Interfaces used for Traffic Type Translation	30
197	Figure 8 – PTP Instance Translation Example.....	31
198	Figure 9 – descriptionDS.userDescription used for PTP Instance Translation.....	32
199	Figure 10 – NETCONF/YANG security processing steps	37
200	Figure 11 – IA-station conformance model	42
201	Figure 12 – Externally controlled ClockSource of a Grandmaster	57
202	Figure 13 – Clock model	58
203	Figure 14 – Example clock usage principles for PTP End Instances	59
204	Figure 15 – Example clock usage principles for Grandmaster PTP Instances.....	60
205	Figure 16 – Error budget scheme	61
206	Figure 17 – Split and combine using BMCA	63
207	Figure 18 – Split and combine using hot standby	64
208	Figure 19 – Generic IEEE 802.1Q YANG Bridge management model.....	76
209	Figure 20 – Internal LAN connection management model.....	77
210	Figure 21 – IA-station example with IETF interfaces	78
211	Figure 22 – VID/FID/MSTID example	79
212	Figure 23 – Structure and interfaces of a CNC.....	82
213	Figure 24 – IA-station structure example.....	83
214	Figure 25 – CNC interaction.....	83
215	Figure 26 – Operational management model.....	84
216	Figure 27 – UNI service model.....	85
217	Figure 28 – CNC southbound.....	85
218	Figure 29 – NETCONF usage in a configuration domain	86
219	Figure 30 – Boundary port model	87
220	Figure 31 – Observer model.....	93
221	Figure 32 – Creation of the digital data sheet of an IA-station	96
222	Figure 33 – Module iecieeee60802-ethernet-interface.....	118
223	Figure 34 – Module iecieeee60802-bridge	119
224	Figure 35 – Module iecieeee60802-dot1-sched-bridge	120
225	Figure 36 – Module iecieeee60802-subscribed-notifications	120
226	Figure 37 – Module iecieeee60802-ia-station.....	120
227	Figure 38 – Usage example of LLDP.....	144
228	Figure 39 – Stream Destination MAC Address	147
229	Figure C.1 – Reference model for clock control system.....	160
230	Figure C.2 – Frequency response for the control system of Figure C.1	163
231	Figure C.3 – Detail of frequency response for the control system of Figure C.1 for	
232	dimensionless frequency in the range 0,1 to 10	164
233	Figure C.4 – Gain peaking (pure fraction) as a function of damping ratio	166
234	Figure C.5 – Gain peaking in dB as a function of damping ratio	167
235	Figure C.6 – Example Frequency response.....	168
236	Figure D.1 – Approach to Testing Normative Requirements for Grandmaster PTP	
237	Instance.....	177

238	Figure D.2 – Approach to Testing Normative Requirements for PTP Relay Instance - 1	178
239	Figure D.3 – Approach to Testing Normative Requirements for PTP Relay Instance - 2	179
240	Figure D.4 – Approach to Testing Normative Requirements for PTP Relay Instance - 3	179
241	Figure D.5 – Approach to Testing Normative Requirements for PTP End Instance	180
242	Figure D.6 – RR Drift Tracking and Error Compensation Calculations – PTP Relay	
243	Instance	185
244	Figure D.7 – RR Drift Tracking and Error Compensation Calculations – PTP End	
245	Instance	186
246	Figure D.8 – Signals and timestamps to measure path delay	187
247		
248	Table 1 – List of terms	16
249	Table 2 – Traffic type characteristics	32
250	Table 3 – IA time-aware stream characteristics	33
251	Table 4 – IA stream characteristics	33
252	Table 5 – IA traffic engineered non-stream characteristics	34
253	Table 6 – IA non-stream characteristics	34
254	Table 7 – Industrial automation traffic types summary	34
255	Table 8 – Example traffic class to traffic type mapping	35
256	Table 9 – Required values	53
257	Table 10 – Protocol settings	53
258	Table 11 – Error generation limits for Grandmaster PTP Instance	54
259	Table 12 – Error generation limits for PTP Relay Instance	55
260	Table 13 – Error generation limits for PTP End Instance	56
261	Table 14 – Error budget	61
262	Table 15 – descriptionDS.userDescription of gPTP Domains	62
263	Table 16 – Summary of the YANG modules	121
264	Table A.1 – Implementation identification template	151
265	Table A.2 – Profile summary template	151
266	Table A.3 – Implementation type	152
267	Table A.4 – IA-station requirements	152
268	Table A.5 – IA-station prohibited management features	152
269	Table A.6 – IA-station PHY and MAC options	153
270	Table A.7 – IA-station time synchronization options	153
271	Table A.8 – IA-station secure management exchange options	153
272	Table A.9 – CNC Requirements	154
273	Table A.10 – CUC Requirements	154
274	Table A.11 – Bridge Component Requirements	155
275	Table A.12 – Common Bridge Component Options	155
276	Table A.13 – ccA Bridge Component Options	155
277	Table A.14 – ccB Bridge Component Options	156
278	Table A.15 – Common End Station Component Requirements	157
279	Table A.16 – Common End Station Component Options	157
280	Table A.17 – ccA End Station Component Options	157
281	Table A.18 – ccB End Station Component Options	158

282	Table D.1 – Time Synchronisation Error Budget.....	169
283	Table D.2 – Protocol configurations & other measures to achieve dTE budget	170
284	Table D.3 – Protocol configurations & other measures to achieve dTE budget	174
285	Table D.4 – Protocol configurations & other measures to achieve dTE budget	174
286	Table D.5 – Protocol configurations & other measures to achieve dTE budget	176
287		
288		
289		

Time-sensitive networking profile for industrial automation

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC document(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation.

IEEE Standards documents are developed within IEEE Societies and Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of IEEE and serve without compensation. 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 contained in its standards. Use of IEEE Standards documents is wholly voluntary. *IEEE documents are made available for use subject to important notices and legal disclaimers (see <https://standards.ieee.org/ipr/disclaimers.html> for more information).*

IEC collaborates closely with IEEE in accordance with conditions determined by agreement between the two organizations. This Dual Logo International Standard was jointly developed by the IEC and IEEE under the terms of that agreement.

2) The formal decisions of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees. The formal decisions of IEEE on technical matters, once consensus within IEEE Societies and Standards Coordinating Committees has been reached, is determined by a balanced ballot of materially interested parties who indicate interest in reviewing the proposed standard. Final approval of the IEEE standards document is given by the IEEE Standards Association (IEEE SA) Standards Board.

3) IEC/IEEE Publications have the form of recommendations for international use and are accepted by IEC National Committees/IEEE Societies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC/IEEE Publications is accurate, IEC or IEEE cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications (including IEC/IEEE Publications) transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC/IEEE Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC and IEEE do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC and IEEE are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or IEEE or their directors, employees, servants or agents including individual experts and members of technical committees and IEC National Committees, or volunteers of IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board, for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC/IEEE Publication or any other IEC or IEEE Publications.

8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that implementation of this IEC/IEEE Publication may require use of material covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. IEC or IEEE shall not be held responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patent 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.

IEC/IEEE 60802 was prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation, in cooperation with IEEE 802.1: Higher Layer LAN Protocols Working Group of IEEE 802: LAN/MAN Standards Committee of the IEEE computer society, under the IEC/IEEE Dual Logo Agreement between IEC and IEEE. It is an International Standard.

This document is published as an IEC/IEEE Dual Logo standard.

The text of this International Standard is based on the following IEC documents:

Draft	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with the rules given in the ISO/IEC Directives, Part 2, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications/.

The IEC Technical Committee and IEEE Working Group have decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Editor's note: This profile has been drafted per the IEC style guide. The use of introductory boilerplate text, editorial conventions and clause numbering may differ from those outlined in the IEEE style guide.

For the convenience of the reviewer, references to the IEC/IEEE cooperation process and to the IEC organization and style guidelines are listed below:

IEC-IEEE 60802 Joint Project Cooperation Process:

<http://www.ieee802.org/1/files/public/docs2018/admin-IEC-IEEE-JWG-cooperation-process-0118.pdf>

IEC organization:

<http://www.iec.ch/>

Home of the IEC organization of the Joint Project IEC/IEEE 60802 is: IEC 65C/WG18:

https://www.iec.ch/dyn/www/f?p=103:14:506767825234046:::FSP_ORG_ID,FSP_LANG_ID:26299,25Assistance to experts drafting IEC documents:

<http://www.iec.ch/standardsdev/resources/draftingpublications/>

Reference material:

http://www.iec.ch/members_experts/refdocs/

ISO/IEC Directives, Part 2:2021

edition 9.0 (2021-05)

Principles and rules for the structure and drafting of ISO and IEC documents:

https://www.iec.ch/members_experts/refdocs/iec/isoiecdir2%7Bed9.0%7Den.pdf

ISO/IEC Directives, Part 1:2023 + IEC Supplement:2023

https://www.iec.ch/system/files/2023-05/consolidated_iso-iec_part-1_iecsupplement_2023.pdf

Procedures for the technical work - Procedures specific to IEC:

https://www.iec.ch/members_experts/refdocs/iec/isoiecdir1-consolidatedIECsup%7Bed17.0%7Den.pdf

This document defines a Time-Sensitive Networking profile for industrial automation. The profile selects features, options, configurations, defaults, protocols, and procedures of bridges, end stations, and LANs to build industrial automation networks.

The profile meets the industrial automation market objective of converging Operations Technology (OT) and Information Technology (IT) networks by defining a common, standardized network infrastructure. This objective is accomplished by taking advantage of the improvements that Time-Sensitive Networking provides to IEEE 802.1 and IEEE 802.3 standard Ethernet networks by providing guaranteed data transport with bounded low latency, low latency variation, zero congestion loss for critical traffic, and high availability.

The profile helps the convergence of industrial communication networks by referring only to international standards to build the lower layers of the communication stack and their management.

Ethernet extended with Time-Sensitive Networking technology provides the features required in the area of industrial communication networks, such as:

- Meeting low latency and latency variation requirements concerning data transmission.
- Efficient exchange of data records on a frequent time period.
- Reliable communications with calculable downtime.
- High availability meeting application requirements.
- Efficient mechanisms for bandwidth utilization of exchanges of data records, with zero congestion loss.
- Improved clock synchronization mechanisms, including support of multiple gPTP domains.

Time-sensitive networking profile for industrial automation

1 Scope

This document defines time-sensitive networking profiles for industrial automation. The profiles select features, options, configurations, defaults, protocols, and procedures of bridges, end stations, and LANs to build industrial automation networks. This document also specifies YANG modules defining read-only information available online and offline as a digital data sheet. This document also specifies YANG modules for remote procedure calls and actions to address requirements arising from industrial automation networks.

2 Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9594-1:2020 (ITU-T Recommendation X.500), *Information technology: Open systems interconnection – Part 1: The Directory: Overview of concepts, models and services*

ISO/IEC 9594-2:2020 (ITU-T Recommendation X.501), *Information technology: Open systems interconnection Part 2: The Directory: Models*

IEEE Draft Std P1588e¹ (Draft 0.2, March 2022), *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems Amendment: MIB and YANG Data Models*

IEEE Std 802.1AB-2016², *IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery*

IEEE Std 802.1ABcu-2021, *IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery Amendment 1: YANG Data Model*

IEEE Std 802.1AR-2018, *IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identity*

IEEE Std 802.1AS-2020, *IEEE Standard for Local and Metropolitan Area Networks: Timing and Synchronization for Time-Sensitive Applications*

IEEE Draft Std P802.1ASdm (Draft 0.5, January 2022), *IEEE Standard for Local and Metropolitan Area Networks: Timing and Synchronization for Time-Sensitive Applications Amendment: Hot Standby*

IEEE Std 802.1CB-2017, *IEEE Standard for Local and Metropolitan Area Networks: Frame Replication and Elimination for Reliability*

IEEE Std 802.1CBcv-2021, *IEEE Standard for Local and Metropolitan Area Networks: Frame Replication and Elimination for Reliability — Amendment 1: Information Model, YANG Data Model and Management Information Base Module*

IEEE Std 802.1Q-2022, *IEEE Standard for Local and Metropolitan Area Network: Bridges and Bridged Networks*

¹ Numbers preceded by P are IEEE authorized standards projects that were not approved by the IEEE SA Standards Board at the time this publication went to Sponsor ballot/press. For information about obtaining drafts, contact the IEEE.

² The IEEE standards or products referred to in Clause 2 are trademarks of The Institute of Electrical and Electronics Engineers, Incorporated

- 442 IEEE Draft Std P802.1Qcw (Draft 1.3, February 2021), *Draft Standard for Local and*
443 *Metropolitan Area Networks: Bridges and Bridged Networks, Amendment: YANG Data Models*
444 *for Scheduled Traffic, Frame Preemption, and Per-Stream Filtering and Policing*
- 445 IEEE Draft Std P802.1Qdj (Draft 0.3, June 2022), *Draft Standard for Local and Metropolitan*
446 *Area Networks: Bridges and Bridged Networks, Amendment: Configuration Enhancements for*
447 *Time-Sensitive Networking*
- 448 IEEE Draft Std P802.1Qdx, *Draft Standard for Local and Metropolitan Area Networks: Bridges*
449 *and Bridged Networks, Amendment: YANG Data Models for the Credit-Based Shaper*
- 450 IEEE Std 802.3-2022, *IEEE Standard for Ethernet*
- 451 IEEE Std 802.3.2-2019, *IEEE Standard for Ethernet YANG Data Model Definitions*
- 452 IEEE Draft Std P802.3de (Draft 3.0, March 2022), *Draft Standard for Ethernet Amendment 6:*
453 *Enhancements to MAC Merge and Time Synchronization Service Interface for Point-to-Point 10*
454 *Mb/s Single-Pair Ethernet*
- 455 IETF RFC 2131, Droms, R., *Dynamic Host Configuration Protocol*, March 1997, available at
456 <https://www.rfc-editor.org/info/rfc2131>
- 457 IETF RFC 2986, Nystrom, M. and Kaliski, B., *PKCS #10: Certification Request Syntax*
458 *Specification Version 1.7*, November 2000, available at <https://www.rfc-editor.org/info/rfc2986>
- 459 IETF RFC 3986, Berners-Lee, T., Fielding, R., and Masinter, L., *Uniform Resource Identifier*
460 *(URI): Generic Syntax*, January 2005, available at <https://www.rfc-editor.org/info/rfc3986>
- 461 IETF RFC 5246, Dierks, T. and Rescorla, E., *The Transport Layer Security (TLS) Protocol*,
462 August 2008, available at <https://www.rfc-editor.org/info/rfc5246>
- 463 IETF RFC 5277, Chisholm, S. and Trevino, H., *NETCONF Event Notification*, July 2008,
464 available at <https://www.rfc-editor.org/info/rfc5277>
- 465 IETF RFC 5280, Turner, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W.,
466 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)*
467 *Profile*, May 2008, available at <https://www.rfc-editor.org/info/rfc5280>
- 468 IETF RFC 5480, Cooper, S., Brown, D., Yiu., K., Housley, R., and Polk, T., *Elliptic Curve*
469 *Cryptography Subject Public Key Information*, March 2009, available at [https://www.rfc-](https://www.rfc-editor.org/info/rfc5480)
470 [editor.org/info/rfc5480](https://www.rfc-editor.org/info/rfc5480)
- 471 IETF RFC 6022, Scott, M. and Bjorklund, M., *YANG Module for NETCONF Monitoring*, October
472 2010, available at <https://www.rfc-editor.org/info/rfc6022>
- 473 IETF RFC 6024, Reddy, R. and Wallace, C., *Trust Anchor Management Requirements*, October
474 2010, available at <https://www.rfc-editor.org/info/rfc6024>
- 475 IETF RFC 6066, Eastlake, D., *Transport Layer Security (TLS) Extensions: Extension Definitions*,
476 January 2011, available at <https://www.rfc-editor.org/info/rfc6066>
- 477 IETF RFC 6125, Saint-Andre, P. and Hodges, J., *Representation and Verification of Domain-*
478 *Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX)*
479 *Certificates in the Context of Transport Layer Security (TLS)*, March 2011, available at
480 <https://www.rfc-editor.org/info/rfc6125>
- 481 IETF RFC 6241, Enns, R., Bjorklund, M., Schoenwaelder, J. and Bierman, A., *Network*
482 *Configuration Protocol (NETCONF)*, June 2011, available at [editor.org/info/rfc6241](https://www.rfc-
483 <a href=)
- 484 IETF RFC 6242, Wasserman, M., *Using the NETCONF Protocol over Secure Shell (SSH)*, June
485 2011, available at <https://www.rfc-editor.org/info/rfc6242>

- 486 IETF RFC 6961, Pettersen, Y., *The Transport Layer Security (TLS) Multiple Certificate Status*
487 *Request Extension*, June 2013, available at <https://www.rfc-editor.org/info/rfc6961>
- 488 IETF RFC 7317, Bierman, A. and Bjorklund, M., *A YANG Data Model for System Management*,
489 August 2014, available at <https://www.rfc-editor.org/info/rfc7317>
- 490 IETF RFC 7589, Badra, M., Luchuk, A. and Schoenwaelder, J., *Using the NETCONF Protocol*
491 *over Transport Layer Security (TLS) with Mutual X.509 Authentication*, June 2015, available at
492 <https://www.rfc-editor.org/info/rfc7589>
- 493 IETF RFC 7748, Langley, A., Hamburg, M., and Turner, S., *Elliptic Curves for Security*, January
494 2016, available at <https://www.rfc-editor.org/info/rfc7748>
- 495 IETF RFC 7950, Bjorklund, M., *The YANG 1.1 Data Modeling Language*, August 2016, available
496 at <https://www.rfc-editor.org/info/rfc7950>
- 497 IETF RFC 8032, Josefsson, S., and Liusvaara, I., *Edwards-Curve Digital Signature Algorithm*
498 *(EdDSA)*, January 2017, available at <https://www.rfc-editor.org/info/rfc8032>
- 499 IETF RFC 8069, Thomas, A., *URN Namespace for IEEE*, February 2017, available at
500 <https://www.rfc-editor.org/info/rfc8069>
- 501 IETF RFC 8141, Saint-Andre, P., and Klensin, J., *Uniform Resource Names (URNs)*, April 2017,
502 available at <https://www.rfc-editor.org/info/rfc8141>
- 503 IETF RFC 8341, Bierman, A. and Bjorklund, M., *Network Configuration Access Control Model*,
504 March 2018, available at <https://www.rfc-editor.org/info/rfc8341>
- 505 IETF RFC 8342, Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K. and Wilton, R.,
506 *Network Management Datastore Architecture (NMDA)*, March 2018, available at
507 <https://www.rfc-editor.org/info/rfc8342>
- 508 IETF RFC 8343, Bjorklund, M., *YANG Data Model for Interface Management*, March 2018,
509 available at <https://www.rfc-editor.org/info/rfc8343>
- 510 IETF RFC 8348, Bierman, A., Bjorklund, M., Dong, J., and Romascanu, D., *A YANG Data Model*
511 *for Hardware Management*, March 2018, available at <https://www.rfc-editor.org/info/rfc8348>
- 512 IETF RFC 8410, Josefsson, S., and Schaad, J., *Algorithm Identifiers for Ed25519, Ed448,*
513 *X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure*, August 2018,
514 available at <https://www.rfc-editor.org/info/rfc8410>
- 515 IETF RFC 8446, Rescorla, E., *The Transport Layer Security (TLS) Protocol Version 1.3*, August
516 2018, available at <https://www.rfc-editor.org/info/rfc8446>
- 517 IETF RFC 8525, Bierman, A., Bjorklund, M., Schoenwaelder, J., Watsen, K. and Wilton, R.,
518 *YANG Library*, March 2019, available at <https://www.rfc-editor.org/info/rfc8525>
- 519 IETF RFC 8526, Bierman, A., Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K. and
520 Wilton, R., *NETCONF Extensions to Support the Network Management Datastore Architecture*,
521 March 2019, available at <https://www.rfc-editor.org/info/rfc8526>
- 522 IETF RFC 8639, Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and Tripathy, A.,
523 *Subscription to YANG Notifications*, September 2019, available at [https://www.rfc-](https://www.rfc-editor.org/info/rfc8639)
524 [editor.org/info/rfc8639](https://www.rfc-editor.org/info/rfc8639)
- 525 IETF RFC 8640, Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E. and Tripathy, A.,
526 *Dynamic Subscription to YANG Events and Datastores over NETCONF*, September 2019,
527 available at <https://www.rfc-editor.org/info/rfc8640>
- 528 IETF RFC 8641, Clemm, A. and Voit, E., *Subscription to YANG Notifications for Datastore*
529 *Updates*, September 2019, available at <https://www.rfc-editor.org/info/rfc8641>

IETF RFC 9195, Lengyel, B. and Claise, B., *A File Format for YANG Instance Data*, February 2022, available at <https://www.rfc-editor.org/info/rfc9195>

IETF RFC 9196, Lengyel, B., Clemm, A. and Claise, B., *YANG Modules Describing Capabilities for Systems and Datastore Update Notifications*, February 2022, available at <https://www.rfc-editor.org/info/rfc9196>

Editor's note: The „Internet-Draft (I-D)“ will be substituted before IEEE SA ballot and IEC CDV with the IETF RFC numbers, which are not yet known. The reference to the draft will also disappear.

IETF RFC „Internet-Draft (I-D)“, *Updates to Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication* (draft-ietf-netconf-over-tls13-02), Internet Draft, Work in Progress by NETCONF WG, available at <https://datatracker.ietf.org/doc/draft-ietf-netconf-over-tls13/>

IETF RFC „Internet-Draft (I-D)“, *A YANG Data Model for a Truststore* (draft-ietf-netconf-trust-anchors-19), Internet Draft, Work in Progress by NETCONF WG, available at <https://datatracker.ietf.org/doc/draft-ietf-netconf-trust-anchors/19/>

IETF RFC „Internet-Draft (I-D)“, *A YANG Data Model for a Keystore* (draft-ietf-netconf-keystore-26), Internet Draft, Work in Progress by NETCONF WG, available at <https://datatracker.ietf.org/doc/draft-ietf-netconf-keystore/26/>

IETF RFC „Internet-Draft (I-D)“, *YANG Data Types and Groupings for Cryptography* (draft-ietf-netconf-crypto-types-25), Internet Draft, Work in Progress by NETCONF WG, available at <https://datatracker.ietf.org/doc/draft-ietf-netconf-crypto-types/25/>

NIST FIPS 180-4, *Secure Hash Standard (SHS)*, August 2015, available at <https://csrc.nist.gov/publications/detail/fips/180/4/final>

NIST FIPS 186-5, *Digital Signature Standard (DSS)*, February 2023, available at <https://csrc.nist.gov/publications/detail/fips/186/5/final>

NIST SP 800-186, *Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters*, February 2023, available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186.pdf>

Editor's note: Any draft standards will be removed prior to CDV and SA Ballot.

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 General

For the purposes of this document, the terms and definitions given in ITU-T G.8260, IEEE Std 802-2014, IEEE Std 802.3-2022, IEEE Std 802.1Q-2022, IEEE Std 802.1AS-2020, and the following apply:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEEE Standards Dictionary Online: available at <https://dictionary.ieee.org>
- ITU-T Terms and Definitions database: available at https://www.itu.int/br_tsb_terms/#/

NOTE Definitions in IEC 60050 can be found in the Electropedia link above.

3.2 List of terms, abbreviated terms and definitions given in various standards

For the purposes of this document, the terms and definitions given in Table 1 apply.

Editor's note: Any standard referenced in the section title but not referenced in the table will be removed prior to CDV and sponsor ballot.

For ease of understanding, the most important terms used within this document are listed in Table 1 but the definitions are not repeated.

Table 1 – List of terms

Term	Source
BMCA	IEEE Std 802.1AS-2020
Bridge	IEEE Std 802.1Q-2022
Bridge Port	IEEE Std 802.1Q-2022
CFM	IEEE Std 802.1Q-2022
Clock	IEEE Std 802.1AS-2020
ClockTimeTransmitter	IEEE Std 802.1AS-2020
ClockTimeReceiver	IEEE Std 802.1AS-2020
ClockSource	IEEE Std 802.1AS-2020
ClockTarget	IEEE Std 802.1AS-2020
CNC	IEEE Std 802.1Q-2022
constant time error (cTE)	ITU-T G.8260
Customer Virtual Local Area Network (C-VLAN) component	IEEE Std 802.1Q-2022
CUC	IEEE Std 802.1Q-2022
device	IEEE Std 802.1AR-2018
DLL	IEEE Std 802-2014
DTE	IEEE Std 802.3-2022
dynamic time error (dTE)	ITU-T G.8260
end entity (EE)	NIST Special Publication 800-57 Part 2, Revision 1
end station	IEEE Std 802-2014
Ethernet	IEEE Std 802.3-2022
FDB	IEEE Std 802.1Q-2022
FID	IEEE Std 802.1Q-2022
fingerprint	IETF RFC 7589
FQTSS	IEEE Std 802.1Q-2022
fractional frequency offset	IEEE Std 802.1AS-2020
frame	IEEE Std 802.1Q-2022
frame preemption	IEEE Std 802.1Q-2022
FRER	IEEE Std 802.1CB-2017
gating cycle	IEEE Std 802.1Q-2022
gPTP communication path	IEEE Std 802.1AS-2020
gPTP domain	IEEE Std 802.1AS-2020
Grandmaster Clock	IEEE Std 802.1AS-2020
Grandmaster PTP Instance	IEEE Std 802.1AS-2020
Independent Virtual Local Area Network [VLAN] Learning (IVL)	IEEE Std 802.1Q-2022
IST	IEEE Std 802.1Q-2022
LAN	IEEE Std 802-2014
latency	IEEE Std 802.1Q-2022

Term	Source
Listener	IEEE Std 802.1Q-2022
LLDP	IEEE Std 802.1AB-2016
LLDPDU	IEEE Std 802.1AB-2016
local clock	IEEE Std 802.1AS-2020
LocalClock	IEEE Std 802.1AS-2020
logical link	IEEE Std 802-2014
LPI	IEEE Std 802.3-2022
MAC	IEEE Std 802.1Q-2022
MMRP	IEEE Std 802.1Q-2022
MST	IEEE Std 802.1Q-2022
MVRP	IEEE Std 802.1Q-2022
NETCONF	IETF RFC 6241
PCP	IEEE Std 802.1Q-2022
PDU	IEEE Std 802.1Q-2022
PHY	IEEE Std 802.3-2022
PLS	IEEE Std 802.3-2022
Port	IEEE Std 802.1Q-2022
preciseOriginTimestamp	IEEE Std 802.1AS-2020
primary domain	IEEE Draft Std P802.1ASdm
PSFP	IEEE Std 802.1Q-2022
PTP End Instance	IEEE Std 802.1AS-2020
PTP Instance	IEEE Std 802.1AS-2020
PTP Link	IEEE Std 802.1AS-2020
PTP Port	IEEE Std 802.1AS-2020
PTP Relay Instance	IEEE Std 802.1AS-2020
PVID	IEEE Std 802.1Q-2022
redundancy	IEC 60050-192
residence time	IEEE Std 802.1AS-2020
secondary domain	IEEE Draft Std P802.1ASdm
station	IEEE Std 802-2014
stream	IEEE Std 802.1Q-2022
synchronized time	IEEE Std 802.1AS-2020
Talker	IEEE Std 802.1Q-2022
time error	ITU-T G.8260
time-sensitive stream	IEEE Std 802.1Q-2022
traffic class	IEEE Std 802.1Q-2022
TLV	IEEE Std 802.3-2022
Configuration Domain	IEEE P802.1Qdj
UNI	IEEE Std 802.1Q-2022
VID	IEEE Std 802.1Q-2022
VLAN	IEEE Std 802.1Q-2022
YANG	IETF RFC 6020

3.3 Terms defined in this document

3.3.1

application clock

clock used by the application to time events

Note 1 to entry: Events can be periodic or aperiodic.

3.3.2

Bridge component

Customer Virtual Local Area Network (C-VLAN) component as defined in IEEE Std 802.1Q-2022

3.3.3

control latency

time delay between the input to a sensor application and the output from an actuator application

Note 1 to entry: For the purposes of this document, control latency does not include latencies in the sensor, actuator, or the physical system in a process.

3.3.4

deadline

application defined fixed time reference point that represents a time when data is required by the application

3.3.5

digital data sheet

information about the capabilities of an IA-station, for example, states, configurations, and supported features

3.3.6

end station component

end station entity as defined in IEEE Std 802-2014

3.3.7

Global Time

synchronized time, derived from a gPTP domain, that is traceable to the PTP timescale

3.3.8

IA-controller

industrial automation function, consisting of a comparing element and a controlling element, that performs a specified control function

Note 1 to entry: An IA-controller exchanges data with several IA-devices or other IA-controllers for the purpose of control of a system.

Note 2 to entry: The primary categories of IA-controllers are distributed control system (DCS), programmable logic controller (PLC), and programmable automation controller (PAC).

3.3.9

IA-device

industrial automation function, consisting of sensor and/or actuator elements to read and/or write process data

Note 1 to entry: An IA-device exchanges data with an IA-controller or other IA-devices for the purpose of control of a system.

3.3.10

IA-station

material element or assembly of one or more end station components, and zero, one or more bridge components

Note 1 to entry: IA-controllers and IA-devices are industrial automation functions of IA-stations.

Note 2 to entry: An IA-station is often colloquially called an "IA-controller" or "IA-device" based on its primary function, for example, "IA-controller" for an IA-station that includes an IA-controller function and an IA-device function.

3.3.11**imprinting**

<security> equipping IA-stations with an LDevID-NETCONF credential as defined in IEEE Std 802.1AR-2018, corresponding trust anchor as defined in IETF RFC 6024, and certificate-to-name mapping instructions as defined in IETF RFC 7589, Clause 7

3.3.12**management entity**

IA-station function responsible for configuration of Bridge components, end station components and ports

Note 1 to entry: The management entity interacts with remote management.

3.3.13**network diameter**

longest of all the calculated shortest paths between each pair of nodes in the network

Note 1 to entry: The shortest path between 2 nodes is the path between the two nodes that contains the fewest number of logical links.

3.3.14**network provisioning**

process of defining a consistent network configuration, which is applied to all stations

3.3.15**nominal frequency**

ideal frequency with zero uncertainty

Note 1 to entry: The nominal frequency of the PTP timescale is further explained in IEEE Std 1588-2019, 7.2.1, 7.2.2, and Annex B.

3.3.16**ppm**

μHz/Hz

Note 1 to entry: The term "ppm" refers to a pure multiplier of 0,000 001 and is used in the context of this document as an SI unit term to allow readable terms conformant to various rules related to expressions.

3.3.17**Working Clock**

synchronized time, derived from a gPTP domain, that is traceable to the PTP timescale, or to an ARB timescale that is continuous

Note 1 to entry: In general, the Working Clock is traceable to an ARB timescale; however, the Working Clock time can be correlated to a recognized timing standard.

3.4 Abbreviated terms and acronyms

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
ARB	Arbitrary
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BMCA	Best Master Clock Algorithm
CA	Certification Authority
CBC	Cipher Block Chaining
ccA	Conformance Class A
ccB	Conformance Class B
CFM	Connectivity Fault Management
CMLDS	Common Mean Link Delay Service

CMS	Cryptographic Message Syntax
CN	Common Name
CNC	Centralized Network Configuration
CRL	Certificate Revocation List
CRUDX	Create Read Update Delete eXecute
CSR	Certificate Signing Request
CUC	Centralized User Configuration
C-VLAN	Customer VLAN
DAC	Discretionary Access Control
DER	Distinguished Encoding Rules
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DLL	Data Link Layer
DMAC	Destination MAC Address
DNS	Domain Name Service
DSA	Digital Signature Algorithm
DTE	Data Terminal Equipment
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-Curve Digital Signature Algorithm
EE	End Entity
FDB	Filtering Database
FID	Filtering Identifier
FQDN	Fully Qualified Domain Name
FQTSS	Forwarding and Queuing Enhancements for time-sensitive streams
FRER	Frame Replication and Elimination for Reliability
GCM	Galois Counter Mode
gPTP	generalized Precision Time Protocol
HMAC	Keyed-Hashing for Message Authentication Code
HW	HardWare
IA	Industrial Automation
IDevID	Initial Device IDentifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
I-LAN	Internal Local Area Network
ISO	International Organization for Standardization
ISS	Internal Sublayer Service
IST	Internal Spanning Tree
IT	Information Technology
ITU	International Telecommunication Union
IVL	Independent Virtual Local Area Network Learning
LDevID	Locally significant Device IDentifier

LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LPI	Low Power Idle
LRP	Link-local Registration Protocol
MAC	Media Access Control
MD	Media-Dependent
MDI	Media Dependent Interface
MMRP	Multiple MAC Registration Protocol
MST	Multiple Spanning Tree
MVRP	Multiple VLAN Registration Protocol
N/A	Not applicable
NACM	Network configuration Access Control Model
NETCONF	Network Configuration Protocol
NMDA	Network Management Datastore Architecture
NPE	Network Provisioning Entity
NRR	Neighbor Rate Ratio
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OT	Operations Technology
OUI	Organizational Unique Identifier
PCP	Priority Code Point
PCS	Profile Conformance Statement
PDU	Protocol Data Unit
PE	Path Entity
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PHY	Physical Layer devices
PII	Personally Identifiable Information
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PLS	Physical Signaling Sublayer
PPS	Pulse Per Second
PSFP	Per-Stream Filtering and Policing
PTP	Precision Time Protocol
PVID	Port VLAN Identifier
RBAC	Role-Based Access Control
RFC	Request for Comments
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman
RAE	Resource Allocation Entity
SAN	Subject Alternative Name
SHA	Secure Hash Algorithm

STE	Sync Tree Entity
TDE	Topology Discovery Entity
TLS	Transport Layer Security
TLV	Type, Length, Value
TOFU	Trust On First Use
TSN	Time-Sensitive Networking
TSN-IA	Time-Sensitive Networking for Industrial Automation
TTP	Trusted Third Party
UNI	User/Network Interface
URL	Uniform Resource Locator
URN	Uniform Resource Name
VID	VLAN Identifier
VLAN	Virtual Local Area Network
YANG	Yet Another Next Generation data modeling language

3.5 Conventions

3.5.1 Convention for capitalizations

Capitalized terms are either based on the rules given in the ISO/IEC Directives Part 2 or emphasize that these terms have a specific meaning throughout this document.

Throughout this document "bridge" can be used instead of "Bridge", except when

- it occurs at the beginning of a sentence or
- it is being used as (or part of) a specific term such as "VLAN Bridge" rather than being used to identify bridges (potentially of any type) in general. If "VLAN Bridge" is meant where only "Bridge" is written, a change to "VLAN Bridge" would be appropriate.

3.5.2 Unit conventions

This document uses:

- Gb/s for gigabits per second and
- Mb/s for megabits per second.

3.5.3 Conventions for YANG contents

YANG modules and XML instance data for YANG shown in this document use the following style:

Text style `higher-layer-if` text style

Contents of a YANG module use the following style:

```
<ieee802-dot1q-bridge xmlns="urn:ietf:params:xml:ns:yang:ieee802-dot1q-bridge">
  <bridges>
    <bridge> <!-- list -->
      <name>functional-unit-x</name>
      ...
    </bridge>
  </bridges>
</ieee802-dot1q-bridge>
```

YANG modules in which only parent nodes are listed always include all their child leaves.

3.5.4 Conventions for YANG selection / Digital Datasheet

YANG nodes in 6.4 marked with [m], are mandatory nodes in the digital datasheet, nodes marked with [c] are conditional mandatory if the IA-station supports the corresponding optional functionality. Nodes marked with [o], are optional nodes in the digital datasheet.

4 Overview of TSN in industrial automation

4.1 Industrial application operation

Industrial network applications are based on three main types of building blocks, which can be combined in one IA-controller or provided as a combination of an IA-controller and IA-devices interconnected through a suitable communication network.

These basic building blocks are:

- IA-device Sensor subsystems, which provide input signals indicating the value of the parameter or state being monitored, such as temperature, pressure, or discrete input information.
- IA-controller subsystems, which operate on combinations of measurements and external demand settings to develop output requests, such as position corrections in a motion application.
- IA-device Actuator subsystems, which implement output requests that result in physical changes to the process or machine under control, such as a level in a storage tank, the speed of a printing press, or movement of a robot.

NOTE 1 In general, all subsystems have an internal state, based upon initial settings, and derived from execution; therefore, the application inputs are combined with the internal state to develop an updated internal state and associated outputs.

A control loop is formed when the process or machine responds to the actuator output and produces a new measured value at the sensor. The complete loop is shown in Figure 1 where an IA-controller and IA-devices are connected as end stations in the network.

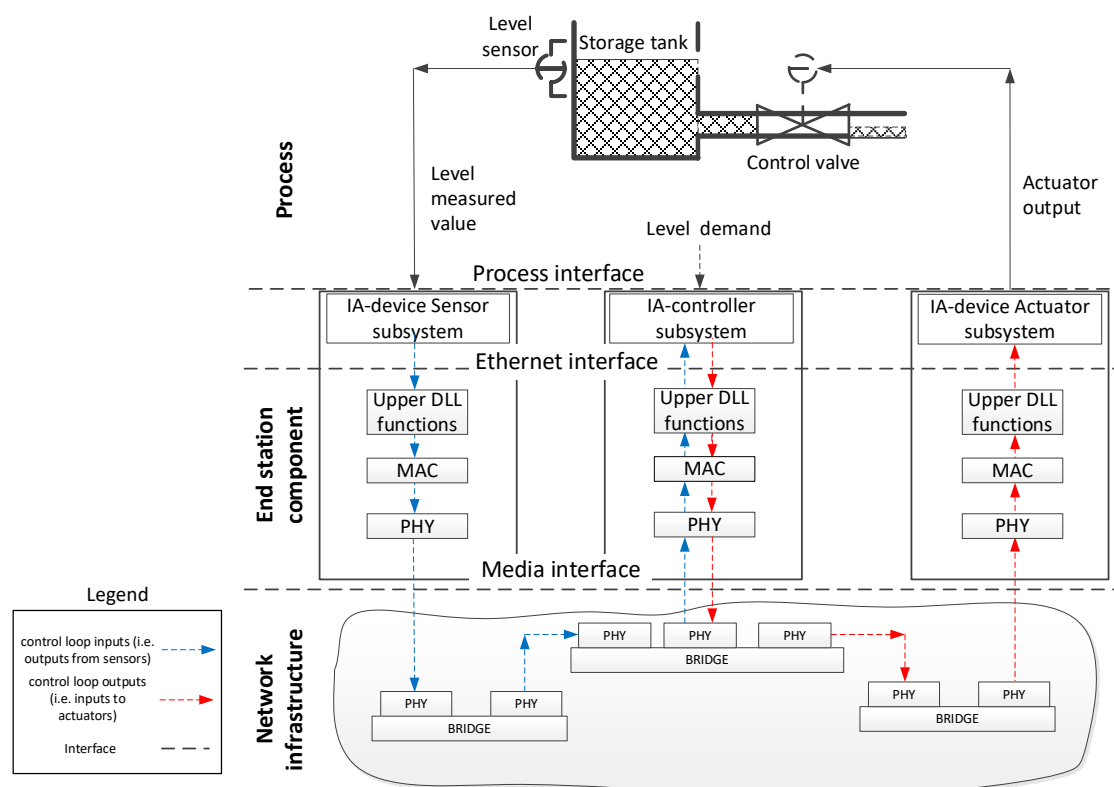


Figure 1 – Data flow in a control loop

In operation, the IA-device Sensor subsystem samples the measured value and the sampled values are transferred through the network as data packets for the IA-controller subsystem to compare with the demand value. After the required computational time, the required output is transferred from the IA-controller subsystem to the IA-device Actuator subsystem for implementation as a change in the external process.

This sequence repeats continuously as a regular operation using a Working Clock. The Working Clock is traceable to an ARB timescale or to the PTP timescale. Traceability to the PTP timescale is not required by all applications. For stability, the time constant of the process response needs to be on the order of five to ten times (or more) the sequence repetition time (i.e., sampling time).

NOTE 2 In common Industrial Network deployments, it has been observed that a ratio of 5 to 10 (or more) provides effective control of the automated process. The actual ratio of the process response time constant to sampling time required for stability depends on the implementation.

Control latency is a critical factor in all types of control and needs to be bounded. Components contributing to the control latency time are shown in Figure 1.

- Application time for sampling, computation, and processing within each IA-controller and IA-device. These are specific to the IA-device and IA-controller and known to the IA-device or IA-controller makers.
- The time for data transfer through the upper DLL functions, MAC and PHY layers within each IA-controller and IA-device. This time depends on the implementation of these components, their situation-dependent load and performance, and configuration elements related to QoS supported by these components.
- End Station and Bridge scheduling and transfer time through the network. These are influenced by the configuration process, which allocates available bandwidth and priorities to various types of application messages.

Offline engineering of the network is possible, including the calculation of the control latency time. During system operation, management services are provided for diagnostics and checking the performance indicators of an installed network.

4.2 Industrial applications

4.2.1 General

Industrial applications can contain multiple tasks. These tasks are executed based upon time or other events. Thus, an industrial application can have multiple tasks executing on different cycles as shown in Figure 2 and Figure 3.

Examples of these tasks include:

- Background tasks, which are executed when no other task is running. There can be zero, one, or more such tasks in an industrial application.
- Main task which executes periodically. The start and execution of this task is often based upon the ARB timescale. There can be zero or one such task, in an industrial application.
- Global Time tasks. The start and execution of these tasks is often based upon Global Time (for example, at noon every day, at noon every Friday, etc). There can be zero, one or more such tasks in an industrial application.
- Process driven tasks which are started by an event (for example, a sensor value reaches a defined point, a process fault occurs, etc.). There can be zero, one or more such tasks in an industrial application.
- Control loop tasks which are bound to Working Clock and started periodically. There can be zero, one or more such tasks in an industrial application.

A user defines the required automation tasks along with the data objects required as output and input for these tasks and the end station which hosts these tasks. Thus, these tasks are bound to data objects, which need to be exchanged between end stations per the user's definition. Many of these tasks have timing requirements, which are added as attributes to the assigned data objects. Examples of these attributes include:

- [DataObject_Update_Interval] an update interval (time between two consecutive updates at the transmitting end station);
- [DataObject_Deadline] a deadline (latest receive time at the end station, relative to the start of the DataObject Update Interval);

- [DataObject_Data_Size] the size of the DataObject;
- Other attributes as needed to form a stream-list request according to IEEE Draft P802.1Qdj, 46.1.5.

NOTE These attributes are provided for illustration purposes. The list is not representative of all industrial applications. These are not network attributes.

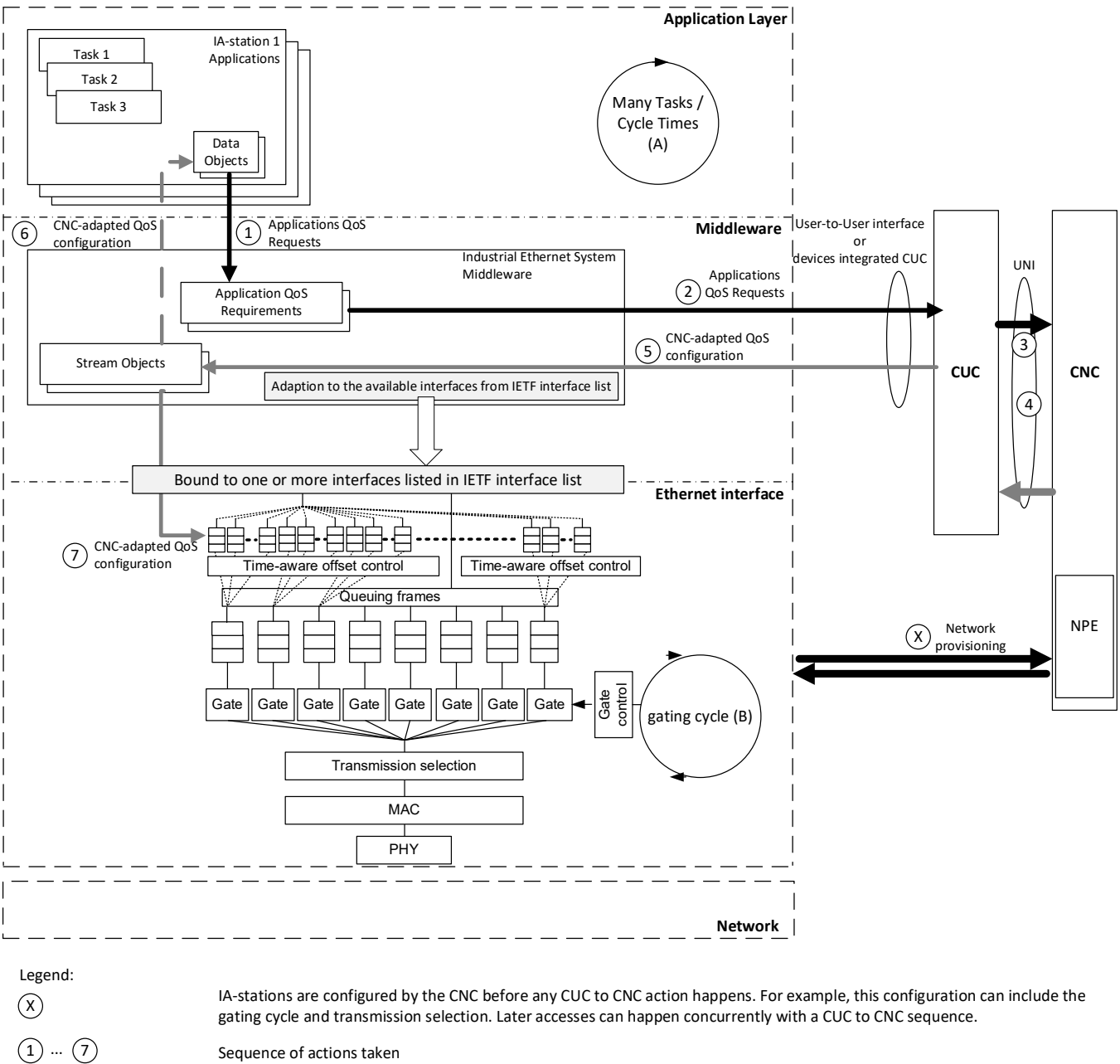


Figure 2 – IA-station interaction with CNC – Transmit path

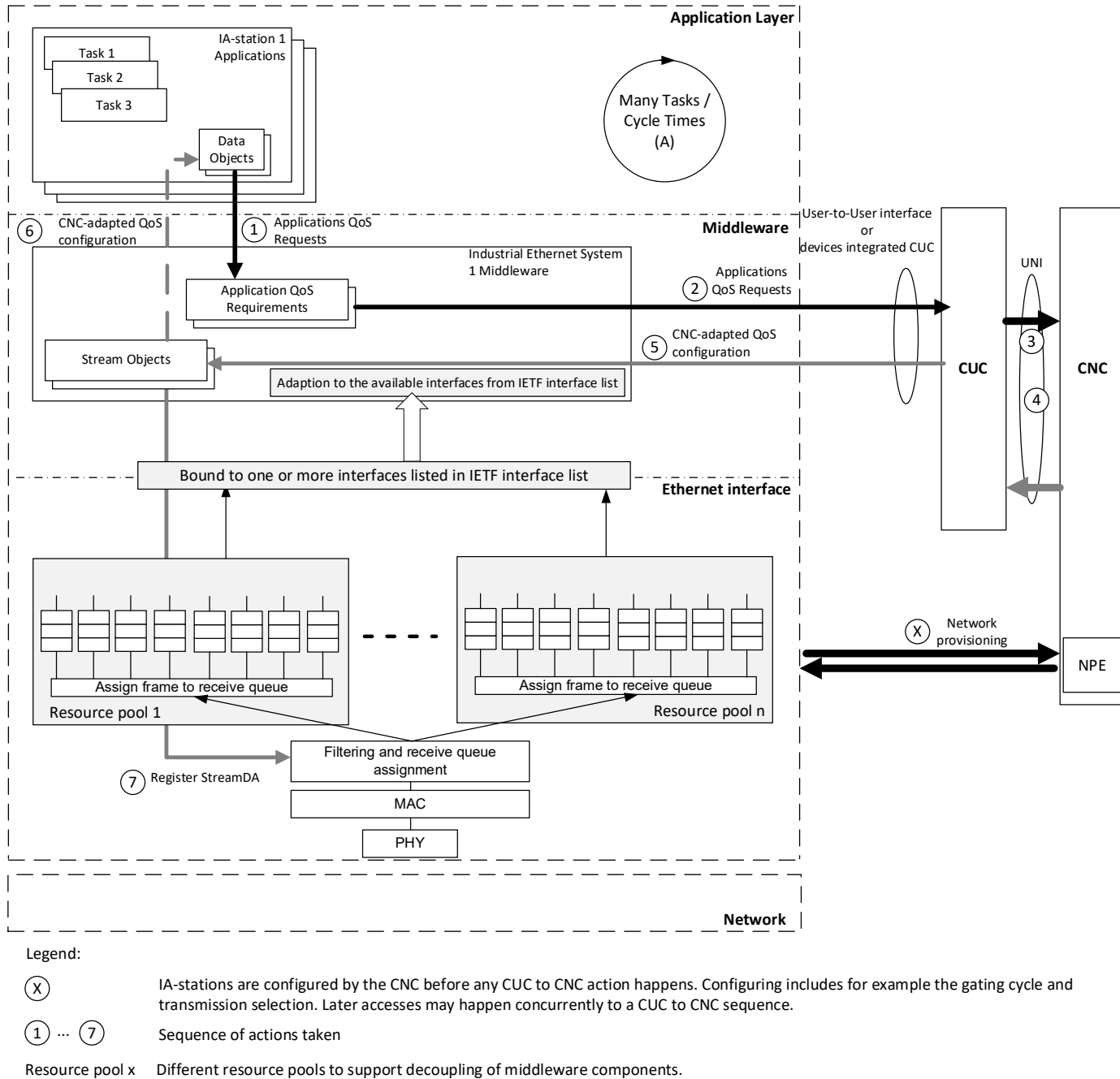


Figure 3 – IA-station interaction with CNC – Receive path

4.2.2 Control loop tasks

Control loops rely on the behavior of synchronized tasks by each of the IA-devices and IA-controllers involved in that control loop. For example, this behavior can be implemented by using a common Working Clock, a common starting point relative to the Working Clock and a common duration for this control loop task at the involved IA-devices and IA-controllers. The data objects associated with the control loop share common values for some attributes (for example, the same values for DataObject_Update_Interval and DataObject_Deadline). Multiple control loop tasks can be implemented and running in parallel at the involved automation devices.

4.2.3 Start of control loop tasks

The calculation of the starting point for a control loop task is independent from the time when the device is powered up or connected to the Configuration Domain. The start of a control loop task, which is based on the Working Clock, can be calculated in the following manner:

Divide the Working Clock value, expressed as an integer, by the duration of the control loop task, expressed as an integer, whenever the Working Clock value increases by one. A remainder of zero provides the basis for the start of the control loop task.

NOTE The units of the Working Clock value and the duration of the control loop task are the same.

Stations in the network associated with the control loop synchronize to a Working Clock using IEEE Std 802.1AS-2020.

4.3 IA-stations

An IA-station can be a simple end station acting as source or destination for control data traffic. In addition, an IA-station can be a combined functional unit that includes an end station component together with a Bridge component in one chassis. IA-stations, incorporating multiple functional units with several end station components and Bridge components within one chassis, can also be found in industrial automation. Within this kind of combined IA-station various components can be connected by internal ports and internal LANs. All components utilize a common management entity as shown in Figure 4.

Figure 4 shows an example IA-station incorporating four functional units in one chassis. Functional unit 1 and functional unit 2 each consist of a Bridge component and an end station component. The end station components are connected by internal ports via internal LANs to the Bridge components. The Bridge components include two external ports each. Functional unit 3 includes only a single end station component with one external port. Functional unit 4 includes a single end station component with two external ports.

IA-controllers and IA-devices as well as the management entity are IA-station functions acting as source of and/or destination for link layer data traffic. Thus, each IA-station incorporates at least one end station component where these functions can be located. Figure 4 shows that IA-station functions can either reside in a single end station component (IA-device 1, IA-controller 1, IA-device 2, IA-controller 2, IA-device 3, IA-controller 3) or in multiple end station components (IA-controller 2, management entity).

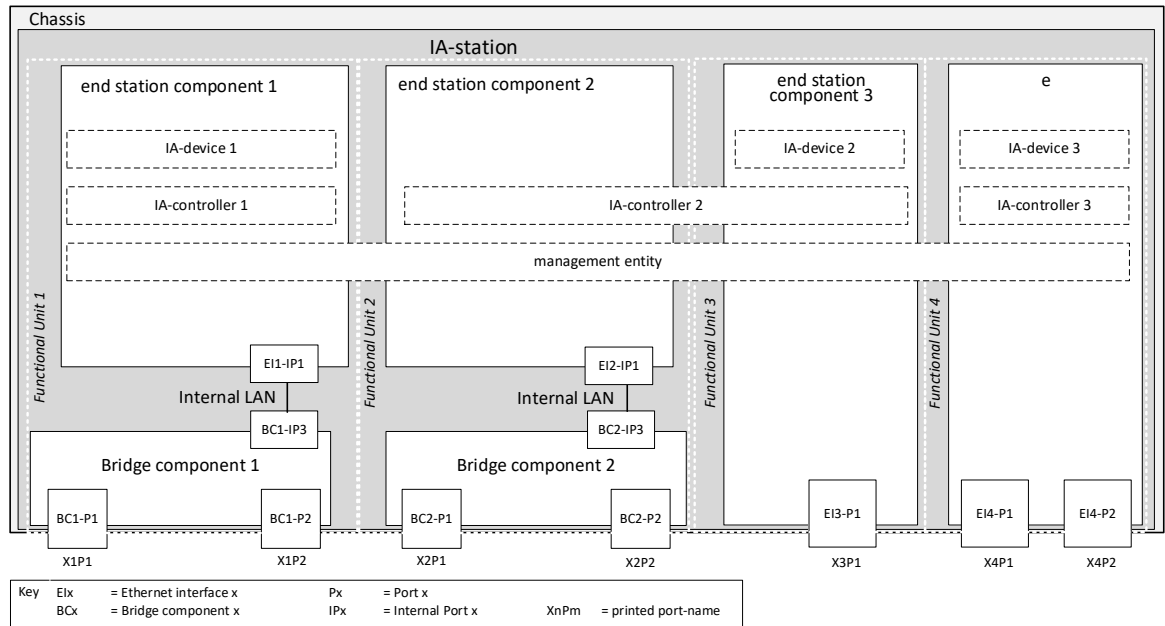


Figure 4 – IA-station example

4.4 Ethernet interface

One or more middleware components act as a layer between applications and the Ethernet interface. Figure 2 and Figure 3 show the relation between applications, middleware, Ethernet interface and the network. Various applications can run in parallel on an automation device. Data objects represent the information exchanged between applications running in different end stations. The application requirements contained in these data objects are translated by the middleware into stream requirements for use by the CUC. This translation can be accomplished in one or both of the following ways:

- The user defines the data objects and translates them into stream requirements and end-station communication-configurations. A user-specific mechanism is used to configure the network components, establish paths, and the time-aware offset control.
- The user defines the data objects and associates them with QoS requirements for each stream (application QoS requirements). These can be forwarded as stream requirement requests by a CUC to a CNC. The CNC responds by providing a stream configuration response. The request and response are specified in IEEE P802.1Qdj. This information is used to configure the time-aware offset control, which utilizes per-stream queues. The CUC can be integrated into the end station or can be accessed via a user-to-user protocol. The middleware uses this information for configuring Talkers and Listeners. This information is also used to add additional timing information to the data objects for application usage.

Time-aware offset control utilizes per-stream queues (see IEEE Std 802.1Q-2022, Figure 34-1) and the traffic specification of the streams, including transmission offsets, provided by the CNC to ensure the order of stream transmission.

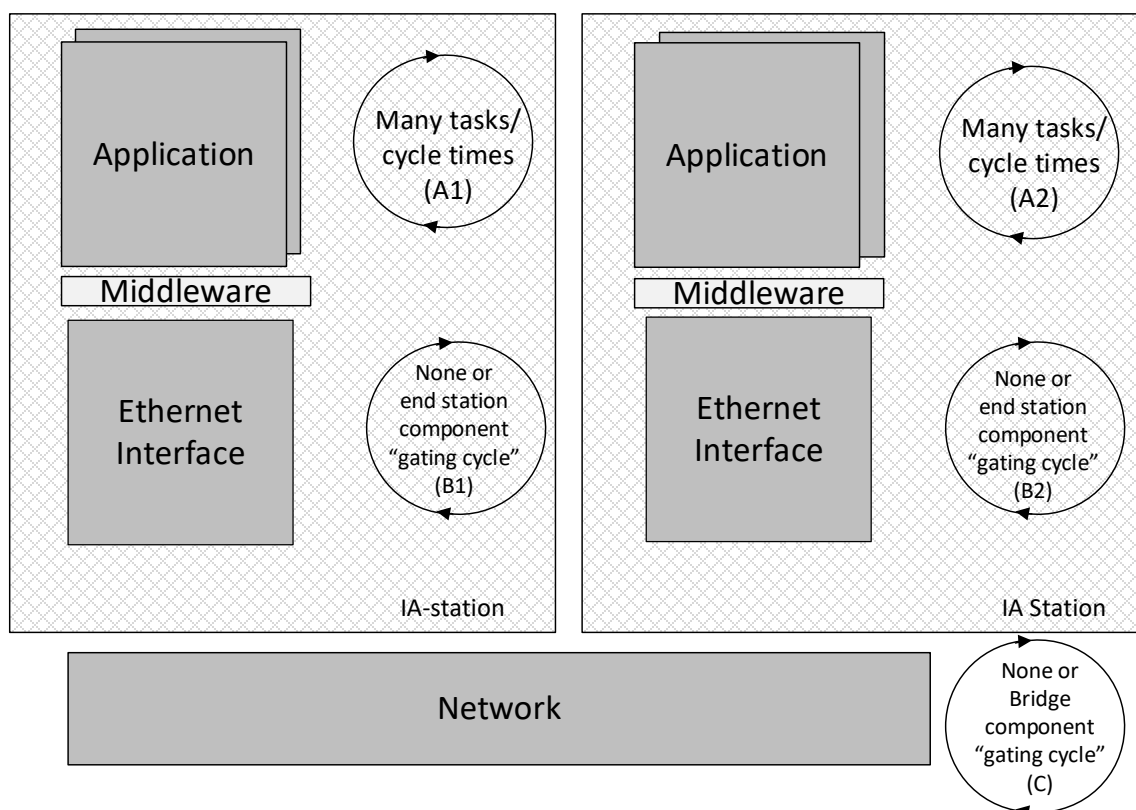


Figure 5 – Model for cycles

These automation systems, which are built from various end stations and connected via bridges, can share a common gating cycle or each station can have its own gating cycle. Alternatively, a bridge or end station can have no gating cycle (expressed as "none" in Figure 5).

4.5 Mechanisms that can be used to meet control loop latency requirements

Meeting latency requirements on a network can be accomplished using one or more combinations of the mechanisms enumerated below. The choice of a mechanism or a subset of the mechanisms listed below depends on the nature of the application(s) and the corresponding latency requirements:

- a) Defining, testing, and simulating all possible application combinations and associated traffic patterns,
- b) Overprovisioning the network,
- c) Providing scheduled time slots for each application to transmit on the network,
- d) Preempting lower priority traffic,
- e) Providing scheduled time slots for certain traffic classes,
- f) Time-aware offset control,
- g) Enforcing deterministic queuing delays in bridges.

NOTE This list is not comprehensive and not all mechanisms mentioned here are part of this specification. For specific mechanisms covered by this document please refer to Clause 5.

Frame preemption is specified in IEEE Std 802.1Q-2022 and IEEE Std 802.3-2022.

Reserving time on the network for certain traffic types can be done through enhancements for scheduled traffic according to IEEE Std 802.1Q-2022, 8.6.8.4. An aligned gating cycle needs to be defined for this method to work. Once a gating cycle is defined, portions of a cycle time can either be allocated to streams or classes of streams.

Multiple Talker/Listener(s) pairs can be used for streams between end stations. Engineered time-triggered transmit can be used to coordinate transmission of all the traffic that shares a network to meet application requirements.

Creating a traffic load model in advance allows analysis of resulting traffic. It can be used to select and implement appropriate mechanisms to achieve latency requirements.

4.6 Translation between middleware and network provisioning

4.6.1 Interfaces of type I2vlan

Application engineering can be done without knowledge of the network provisioning. Since the application is not aware of the network provisioning, it cannot directly map to the network configuration, for example, the use of PCP or VID as configured in the network. This problem is solved by providing a translation table, in the form of a YANG module definition, to the middleware. The IA-station's local YANG datastore contains this information.

Figure 6 and Figure 7 show examples of the translation models.

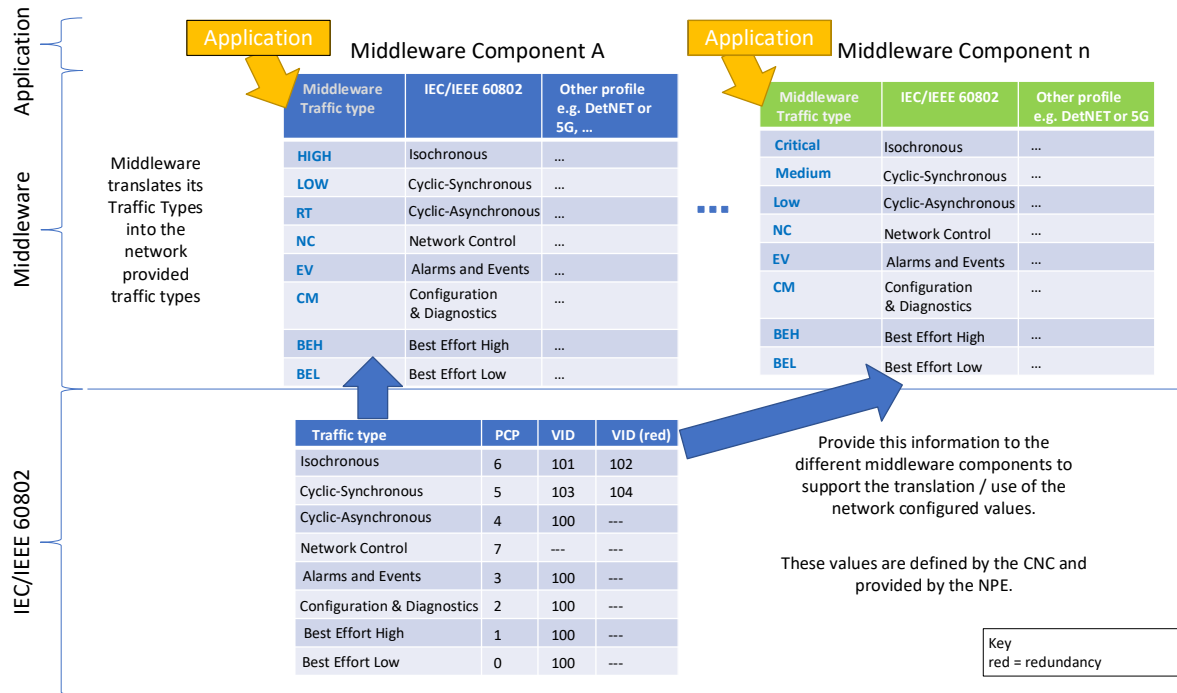


Figure 6 – Traffic type translation example

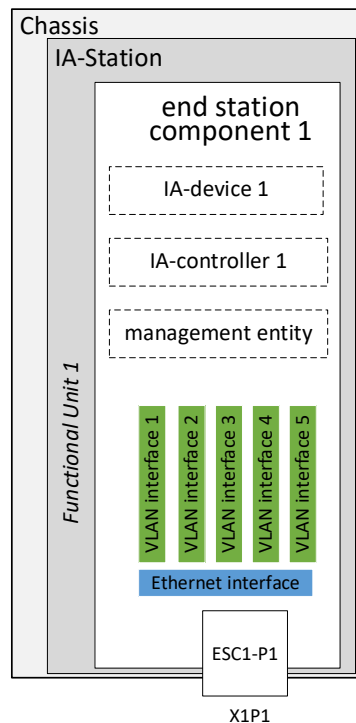


Figure 7 – IETF Interfaces used for Traffic Type Translation

Interfaces of type I2vlan (IETF RFC 7224) can be used to provide the required mapping information to all installed middleware and applications.

The name string of the I2vlan interfaces can provide the vlan-id, the assigned traffic types with their PCP values and redundancy information (see 6.4.2.5).

4.6.2 PTP Instances

PTP domain numbers are also configured during network provisioning. The middleware needs to know which PTP domain is assigned to which target clock. This is done by providing descriptionDS.userDescription names according to IEEE Std 1588-2019, 8.2.5.5 to create a translation table.

descriptionDS.userDescription names allow the support of multiple middleware components at one IA-station using the same PTP Instances (see 6.2.13). An IA-station's local database stores this information.

Figure 8 and Figure 9 show examples of the translation models.

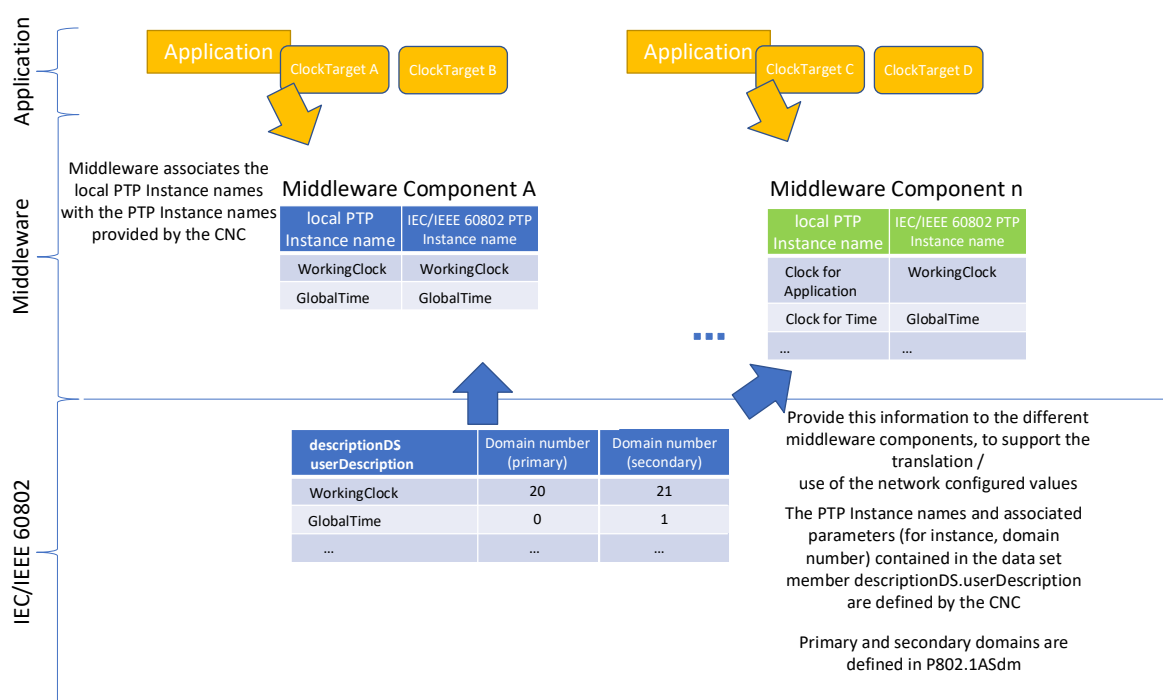


Figure 8 – PTP Instance Translation Example

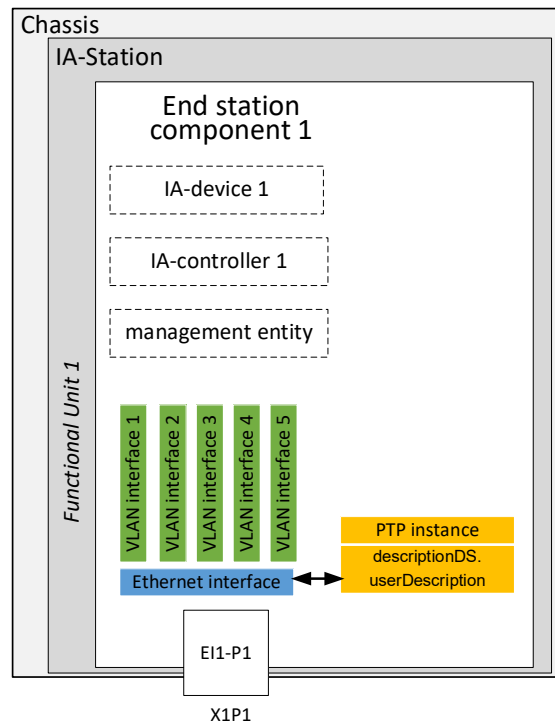


Figure 9 – descriptionDS.userDescription used for PTP Instance Translation

The userDescription contains the clock type (i.e., WorkingClock, GlobalTime, or both). This information is used by the middleware to align to the intended ClockTarget or ClockSource (see 6.2.13).

4.7 Industrial traffic types

4.7.1 General

Industrial automation applications make use of different traffic schemes/types for different functionalities (for example, parameterization, control, alarming). The various traffic patterns have different characteristics, and thus impose different requirements on a network. To specify these traffic types, a two-step approach is used:

- First define characteristics of generic traffic types (traffic-type-categories) and
- Second define instances of the generic traffic types, i.e., the traffic types.

4.7.2 Traffic type characteristics

The traffic type characteristics in Table 2 enable the identification of several distinct traffic types that are shared among sets of industrial applications.

Table 2 – Traffic type characteristics

Characteristic	Description
Cyclic	Traffic types consist of frames that can either be transmitted on a reoccurring time period (cyclic) or at no set period (acyclic). Available selections are: - Required: traffic frames are transmitted cyclically - Optional: Implementation of cyclic traffic is at the discretion of the user.

Characteristic	Description
Data delivery requirements	Denotes the delivery constraints for the traffic. Four options are specified: - Frame Latency: data delivery of a frame for a given Talker-Listener pair occurs within a bounded timespan. - Flow Latency: data delivery up to a certain number of frames or data size (including bursts of frames) occurring over a defined period. - Deadline: data delivery of a frame to a given Listener occurs at or before a specific point in time. - No: Denotes the case of traffic types with no special data delivery requirements
Time-triggered transmission	Talker data transmission occurs at a specific point in time based upon the Working Clock. Available selections are: - Required - Optional: Implementation of time-triggered transmission is at the discretion of the user. Enhancements of scheduled traffic is only one means of achieving time-triggered transmission. Other, application-based, methods are possible

4.7.3 Traffic type categories

4.7.3.1 General

The two-step approach described in 4.7.1 allows a clear differentiation between characteristics as seen from the “network” point of view and “application” point of view. Traffic-type-categories allow different IEEE 802 feature selections to achieve the goals of a specific network deployment. Four traffic-type-categories are identified in industrial automation systems:

- a) IA time-aware stream,
- b) IA stream,
- c) IA traffic engineered non-stream,
- d) IA non-stream.

4.7.3.2 IA time-aware stream

The characteristics of this traffic type category are shown in Table 3.

Table 3 – IA time-aware stream characteristics

Characteristics	
Cyclic	Required
Data delivery requirement	Deadline or Frame Latency
Time-triggered transmission	Required

4.7.3.3 IA stream

The characteristics of this traffic type category are shown in Table 4.

Table 4 – IA stream characteristics

Characteristics	
Cyclic	Required
Data delivery requirement	Frame Latency
Time-triggered transmission	Optional

4.7.3.4 IA traffic engineered non-stream

The characteristics of this traffic type category are shown in Table 5.

Table 5 – IA traffic engineered non-stream characteristics

Characteristics	
Cyclic	Optional
Data delivery requirement	Flow Latency
Time-triggered transmission	Optional

4.7.3.5 IA non-stream

The characteristics of this traffic type category are shown in Table 6.

Table 6 – IA non-stream characteristics

Characteristics	
Cyclic	Optional
Data delivery requirement	No
Time-triggered transmission	Optional

4.7.4 Traffic types

4.7.4.1 General

Table 7 summarizes relevant industrial automation traffic types and their associated characteristics. In an industrial automation system, other applications, such as audio or video, utilizes one of these traffic types. Traffic Type codes are needed for the VLAN naming scheme defined in this document. See 6.4.2.4 for more information.

Table 7 – Industrial automation traffic types summary

Traffic type name	Traffic type code	Cyclic	Data delivery requirements	Time-triggered transmission	Traffic-type-category
Isochronous	H	Required	Deadline	Required	IA time-aware-stream
Cyclic-synchronous	G	Required	Frame Latency	Required	IA time-aware-stream
Cyclic-asynchronous	F	Required	Frame Latency	Optional	IA stream
Alarms & Events	E	Optional	Flow Latency	Optional	IA traffic engineered non-stream
Configuration & Diagnostics	D	Optional	Flow Latency	Optional	IA traffic engineered non-stream
Network Control	C	Optional	Flow Latency	Optional	IA traffic engineered non-stream
Best Effort High	B	Optional	No	Optional	IA non-stream
Best Effort Low	A	Optional	No	Optional	IA non-stream

4.7.4.2 Isochronous

A type of IA time-aware stream traffic. This type of traffic is transmitted cyclically using time-triggered transmission. Listeners have individual deadline requirements. Cycle times are typically in the range of microseconds to tens of milliseconds. Frame size is typically below 500 octets. Talker-Listener pairs are synchronized to the Working Clock. The network is configured by the CNC to provide zero congestion loss for this traffic type. This type of traffic is normally used in control loop tasks.

4.7.4.3 Cyclic-synchronous

A type of IA time-aware stream traffic. This type of traffic is transmitted cyclically using time-triggered transmission. Talker-Listener pairs have individual latency requirements. Cycle times are typically in the range of hundreds of microseconds to hundreds of milliseconds. Frame size is unconstrained except as indicated in 5.5.1. Talker-Listener pairs are synchronized to the Working Clock. The network is configured by the CNC to provide zero congestion loss for this traffic type. This type of traffic is normally used in control loop tasks.

4.7.4.4 Cyclic-asynchronous

A type of IA stream traffic. This type of traffic is transmitted cyclically with latency requirements bounded by the interval as defined in IEEE Std 802.1Q-2022, 46.2.3.5.1. Talker-Listener pairs have individual latency requirements. Cycle times are typically in the range of milliseconds to seconds. Frame size is unconstrained except as indicated in 5.5.1. Data exchanges between Talker-Listener pairs are typically not dependent on the Working Clock. This traffic type typically tolerates limited congestion loss. The network is configured by the CNC to handle this traffic type without loss, up to a certain number of frames or data size.

4.7.4.5 Alarms and events

A type of IA traffic engineered non-stream. This type of traffic is transmitted cyclically or acyclically. This traffic expects bounded latency including time for retransmission in the range of milliseconds to hundreds of milliseconds. The source of the alarm or event typically limits the bandwidth allocated to this traffic. Frame size is unconstrained except as indicated in 5.5.1. Congestion loss can occur. Retransmission to mitigate frame loss is expected. The network is configured by the CNC to handle these frames, including bursts of frames, up to a certain number of frames or data size over a defined period.

4.7.4.6 Configuration and diagnostics

A type of IA traffic engineered non-stream. This type of traffic is transmitted cyclically or acyclically. This traffic expects bounded latency, up to seconds, including time for retransmission. The source of configuration or diagnostics frames typically limits the bandwidth allocated to this traffic. Frame size is unconstrained except as indicated in 5.5.1. Congestion loss can occur. Retransmission to mitigate frame loss is expected. The network is configured by the CNC to handle these frames, including bursts of frames, up to a certain number of frames or data size over a defined period.

4.7.4.7 Network control

A type of IA traffic engineered non-stream. This type of traffic can be transmitted cyclically or acyclically. This traffic expects bounded latency including time for retransmission. Frame size is unconstrained except as indicated in 5.5.1. The network is configured by the CNC to handle these frames, including bursts of frames, up to a certain number of frames or data size over a defined period. If these limits are exceeded congestion loss can occur. Network control is comprised of services required to maintain network operation. Examples include time synchronization, loop prevention, and topology detection.

4.7.4.8 Best effort

A type of IA non-stream. The network is configured by the CNC so that these frames do not interfere with other traffic types. These frames are forwarded when resources are available. Congestion loss resulting in frame drop can occur. It is sometimes desirable to have more than one traffic class for best effort traffic (see Table 8).

4.7.4.9 Traffic class to traffic type mapping

Table 8 provides an example for the usage of traffic classes based on the traffic type:

Table 8 – Example traffic class to traffic type mapping

Traffic class	PCP (8 Queues)	PCP (4 Queues)	Traffic Type
7	6	2	Isochronous

6	5	1	Cyclic-Synchronous
5	4	1	Cyclic-Asynchronous
4	7	3	Network Control
3	3	0	Alarms and Events
2	2	0	Configuration & Diagnostics
1	1	0	Best Effort High
0	0	0	Best Effort Low
NOTE An example mapping of PCP and traffic type to an application is provided in Figure 6.			

1019

1020 The traffic-type-categories definition allows different IEEE 802 feature selections to achieve
1021 specified goals. Moreover it helps in identification of the traffic protection mechanisms.
1022 Adherence to this example of a common mapping helps minimize potential conflicts between
1023 traffic types.

1024

1025 4.8 Security for TSN-IA

1026 4.8.1 General

1027 Subclause 4.8 describes selected aspects of TSN-IA security. Protecting the management of
1028 industrial communication is the main objective of TSN-IA security. The protection of
1029 communications that use industrial traffic types is not addressed by this document.

1030

1031 4.8.2 Security configuration model

1032 Security configuration is a part of system engineering and configuration. The security
1033 configuration in this document does not encompass the supply of configuration objects for
1034 middleware and application security. Security configuration settles the prerequisites for
1035 protecting the establishment and management of communications that use industrial traffic
1036 types (see 4.7). It ensures that the security features of IA-stations (including CNCs) can be
1037 used for protecting message exchanges and authorizing the resource accesses during stream
1038 establishment and management. This security configuration supplies deployment-specific
1039 configuration objects to IA-stations. They encompass:

- 1040 • Instructions about cryptographic algorithms,
- 1041 • Credentials and trust anchors,
- 1042 • Instructions to interpret the outcome of peer entity authentication while enforcing resource
- 1043 access controls, and
- 1044 • Access control rules and permissions

1045 This security configuration uses NETCONF/YANG request/response exchanges:

- 1046 • The to-be-configured IA-stations act in NETCONF server role with respect to their security
- 1047 configuration.
- 1048 • A NETCONF client is responsible for setting-up IA-stations for security. This NETCONF
- 1049 client possesses information about the security relationship to be established during security
- 1050 configuration or about the expectations on the IA-stations in a configuration domain. It can
- 1051 be implemented as part of an interactive or automated process (for example an engineering
- 1052 tool, or CNC operation). As an implication, the security configuration includes options for
- 1053 interactive and automated setup, i.e., security configuration is done by human and/or non-
- 1054 human actors.

1055 NOTE NETCONF notifications can also be used to recognize events such as a near-term end-of-life of
1056 certificate objects, especially EE certificate objects (see IETF RFC 4210, 3.1.1).

- 1057 • The security configuration exchanges supply deployment-specific objects (trust anchors,
- 1058 credentials etc.) to IA-stations and manages them. IA-stations that are in factory default
- 1059 state can only possess manufacturer-specific security objects (trust anchors, credentials

etc.) when booting initially. The protected NETCONF/YANG exchanges with IA-stations that are in factory default state are outlined in 4.8.3 to 4.8.6.

4.8.3 NETCONF/YANG processing

Securing NETCONF/YANG resources on NETCONF servers is specified by IETF RFC 6241 (NETCONF). Therefore, message exchange protection between NETCONF clients and servers as well as resource access authorization by NETCONF servers is needed:

- IETF RFC 7589 and IETF draft-ietf-netconf-over-tls13 (NETCONF-over-TLS) specify a solution to protect NETCONF message exchanges by TLS.
- IETF RFC 8341 (NACM) specifies three access control points, covering the request/response and notification model in NETCONF according to IETF RFC 8341, 2.1.

NETCONF servers enforce security as shown in Figure 10. The processing steps are executed upon the current configuration of the NETCONF server's YANG modules.

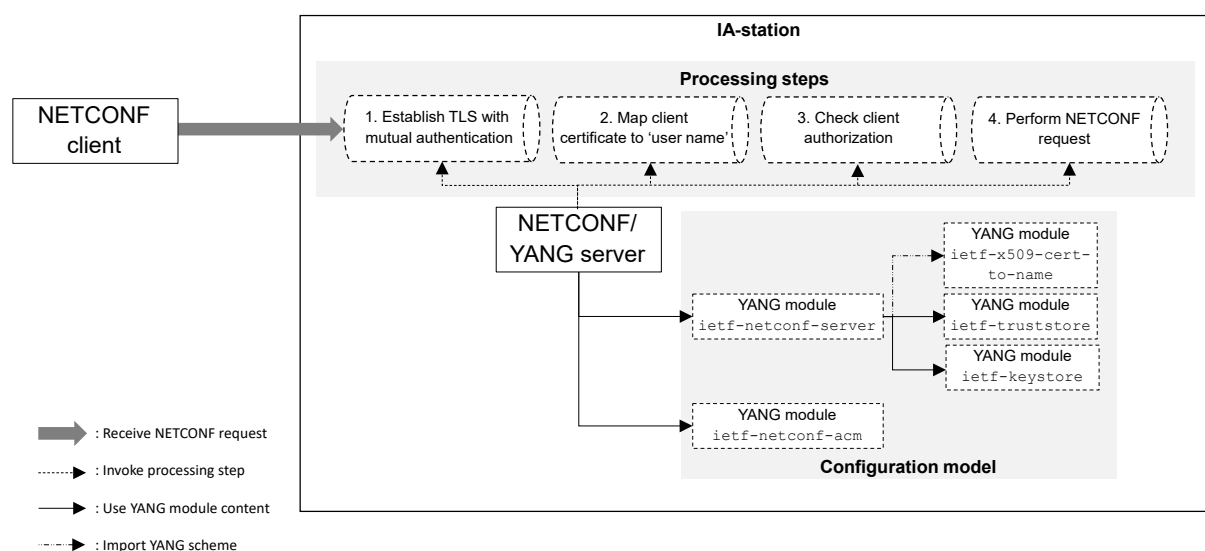


Figure 10 – NETCONF/YANG security processing steps

The processing steps on the side of NETCONF servers are:

- 1) Establish a TLS connection with mutual authentication: The NETCONF server acts as TLS server and awaits connection requests of NETCONF clients (TLS clients). At the beginning of the TLS handshake, the TLS client and server negotiate the TLS protocol version to be used. During the TLS handshake the NETCONF server authenticates itself towards the NETCONF client by a credential from its ietf-keystore YANG module. In addition, the NETCONF server challenges the NETCONF client for authentication and verifies its authentication by trust anchors in its ietf-truststore YANG module according to 6.3.4. A successful mutual authentication is a prerequisite for proceeding to the next step.
- 2) Map the client certificate to a username: The NETCONF server maps the authenticated TLS client certificate to a "NETCONF username"³ by applying an ordered list of mapping instructions. These instructions are provided in its ietf-x509-cert-to-name YANG module. The applicable list item is identified by matching its configured fingerprint (according to IETF RFC 7589, Clause 7) against the certification path that was used for TLS client authentication (an end entity certificate or a CA certificate). According to the map type

³ In this document, 'NETCONF username' values do not represent references to human users – in almost all cases.

of the identified list item, the NETCONF server determines the “NETCONF username”. This can be done by extracting information from the end entity certificate of the NETCONF client. A successful certificate-to-“NETCONF username” mapping is a prerequisite for proceeding to the next step.

- 3) Check client authorization: The NETCONF server checks if the NETCONF client has the permission to access the requested NETCONF/YANG resource based on its “NETCONF username” and the access control rules available in its ietf-netconf-acm YANG module. See 4.8.4 for more information about NETCONF/YANG access control. A successful authorization is a prerequisite for proceeding to the next step.
- 4) Perform NETCONF request: If all preceding steps succeeded, the NETCONF server performs the NETCONF request.

4.8.4 NETCONF/YANG access control

NACM defines a YANG information model for describing permitted/denied access operations. NETCONF servers are responsible for enforcing access control to their resources according to the information in their ietf-netconf-acm YANG modules. NACM allows the description of access-controlled resources in terms of NETCONF protocol operations, nodes in YANG datastores and/or types of notification events. NACM uses character strings to represent the subject actors i.e., NETCONF clients. These character strings are known as “NETCONF username”. The NACM access control information of a NETCONF server is created, updated, and deleted per IA-station. The management of this information happens along the IA-station lifecycle for example, manufacturing, bootstrapping, operation, maintaining, re-owning, destructing. Moreover, the management of the NACM access control information itself is subject to NACM access control.

This document employs multiple YANG data models for fulfilling its purposes. This extends beyond the above identified YANG modules (see 4.8.3). The NETCONF server on an IA-station enforces access control for NETCONF/YANG resources. To meet this objective, the NETCONF server on an IA-station is supplied with access control information for the used NETCONF/YANG resources. NACM is employed for this purpose and profiles default access control information for the NETCONF/YANG resources (see 6.3.2.2). This relieves other organizations or individuals for example, manufacturers, integrators, operators, owners from being responsible to create NACM access control information for the respective NETCONF/YANG resources.

NACM relies on character strings (known as “NETCONF username”) to refer to clients. NACM access control information as specified in this document, populates the “NETCONF username” character strings in NACM with role names specified in 6.3.2.1.4, c). This allows to create default NACM information without knowing actual names of individual entities. A role name can refer to 0, 1 or more individual entities. It is the responsibility of users to assign role names to individual entities. This happens by binding the assigned role names to the credentials of individual entities. The current form to express this binding is a role extension in the identity certificates of end entities defined in this document. These are NETCONF clients, i.e., these role extensions appear in the end entity certificates of LDevID credentials for NETCONF clients.

As initial step NACM maps the NETCONF username to a set of groups. The set of groups determines the set of rules to be applied for access-controlled resources.

4.8.5 Identity checking

IETF RFC 7589 (NETCONF-over-TLS) specifies that NETCONF clients check the identity of NETCONF servers and that NETCONF servers check the identity of NETCONF clients.

The NETCONF server identity check happens inside NETCONF clients. It matches an actual against an expectation:

- The actual server identity is established by the end entity certificate of the NETCONF server (authenticated by means of TLS).
- The expectations on server identity are established by the information that is used to connect to the NETCONF server.

1145 IETF RFC 7589 refers to IETF RFC 6125, Clause 6, for the details of retrieving the actual and
1146 comparing it against the expected.

1147 The NETCONF client identity check happens inside NETCONF servers. It also matches an
1148 actual against an expectation:

- 1149 • The actual client identity is established by the end entity certificate of the NETCONF client
1150 (authenticated by means of TLS).
- 1151 • The expectations on client identity are established by the contents of the YANG modules
1152 ietf-netconf-acm and ietf-x509-cert-to-name.

1153 The details of this check are subject to the requested NETCONF operation. IETF RFC 7589,
1154 Clause 7, specifies the mapping of an authenticated client certificate to a “NETCONF username”
1155 whose permissions are then enforced by IETF RFC 8341 (NACM). More information is provided
1156 in 4.8.3, steps 2 and 3.

1157

1158 **4.8.6 Secure device identity**

1159 **4.8.6.1 Device Identity**

1160 The term ‘device’ originates from IEEE Std 802.1AR-2018. It matches the term IA-station in this
1161 document.

1162 The device identity refers to a set of information items about a device that:

- 1163 • describes a device as a physical or virtual entity in a distributed system (identifier and/or
1164 attribute information);
- 1165 • is used by a device to describe itself as such entity (identifier and/or attribute information);
- 1166 • allows to interact with this device (addressing information i.e., a specific identifier class).

1167 The targeted use case, for example application data exchanges, configuration exchanges,
1168 inventory, or ordering, determines the required amount of identity information about a device.

1169 The device identity of any single IA-station encompasses:

- 1170 • MAC addresses, IP addresses, TCP ports, DNS names.
- 1171 • ietf-hardware YANG module contents (IETF RFC 8348).

1172

1173 **4.8.6.2 Verifiable Device Identity**

1174 Certain aspects of device identity are verified before relying on them during online interactions.
1175 These are examples.

- 1176 • DNS names or IP addresses are used to call the management entity of an IA-station i.e., its
1177 NETCONF/YANG server. Their value represents the caller's expectation on the identity of
1178 their responder in network communications. Verification of the responder's identity helps
1179 defeat DNS spoofing, component impersonation and man-in-the-middle attacks. This is
1180 specified by IETF RFC 7589 and described in IETF RFC 6125, Clause 6. Passing this check
1181 is a prerequisite before NETCONF application exchanges can happen.
- 1182 • mfg-name values in instances of the ietf-hardware YANG module. These values make
1183 claims about the IA-station manufacturer. Their verification is a means to protect against
1184 counterfeiting.

1185 The verification of IA-station identity happens according to a model that is fully specified by this
1186 document. That verification can be done in a manufacturer-agnostic manner. This verification
1187 is important before supplying locally significant credentials especially LDevID-NETCONF to IA-
1188 stations that are in factory-default state.

4.8.6.3 Verification Support Mechanisms

4.8.6.3.1 General

Subclause 4.8.6.3 considers mechanisms that support device identity verification during online interactions with IA-stations.

4.8.6.3.2 Secure Transports

Sending information in plain form over a protected channel, e.g., ietf-hardware YANG module contents via NETCONF-over-TLS protects the transferred information during its transit through the network but does not vouch for the correctness of the received information e.g., the mfg-name value.

4.8.6.3.3 Secure Information

Protecting information objects by means of a cryptographic authentication code or digital signature enables verification of the authenticity and integrity of that information. These cryptographic authentication codes can use symmetric or asymmetric schemes. In case of asymmetric schemes, raw and self-signed public keys need to be distinguished from CA-signed public keys.

Asymmetric schemes with CA-signed public keys are preferable for the verifiable device identity use case: claimants and verifiers share a public key; the claimant possesses the corresponding private key. The establishment and storage of the shared public keys uses public key certificates. For this approach self-signed CA certificates are to be established in an authentic manner. The number of self-signed CA certificates is independent from the number of verifiers (CNCs) as well as claimants (IA-stations).

4.8.6.3.4 IDevID and LDevID Credentials

IDeVID and LDeVID credentials are specified by IEEE Std 802.1AR-2018. These objects are comprised of a certification path and a private key. The certification path encompasses an end entity certificate which contains verifiable device identity in a CA-signed form. The device identity verification happens after validating the certification path (IETF RFC 5280, Clause 6) and checking the proof-of-possession for the private key. The certification path validation demands trust anchors as input arguments (IETF RFC 5280, 6.1.1 input argument (d)).

Two types of credentials are distinguished by IEEE Std 802.1AR-2018:

- IDeVIDs are issued by device manufacturers. They represent an initial identity as it is known at device production-time. The initial device identity is not locally significant: it cannot contain deployment-specific information such as DNS names or IP addresses.
- LDeVIDs are issued by other actors e.g., a device user. They represent a locally significant device identity: they can contain deployment-specific information e.g., DNS names or IP addresses.

IEEE Std 802.1AR-2018, Clause 6, uses signature suites to describe the subject public key and the signature fields in IDeVID and LDeVID certification paths. This notion is different from TLS cipher suites.

NOTE IDeVID and LDeVID credentials also serve purposes beyond secure device identity, for instance the realization of secure transports. This facilitates the use case of NETCONF/YANG security setup from factory default state.

4.8.6.3.5 IDevID Items beyond IEEE Std 802.1AR-2018

IEEE Std 802.1AR allows verification of the following identity items:

- certificate issuer (not necessarily: manufacturer) by issuer field (data type: ASN.1 Name) and
- if present: device instance by serialNumber value (data type: ASN.1 PrintableString).

NOTE 1 IEEE Std 802.1AR-2018 represents the initial device identity as an optional serialNumber attribute (OID 2.5.4.5) in the subject field of the EE certificate. This value is unique within the domain of significance of the EE certificate issuer.

NOTE 2 This verification can happen after certification path validation and the proof-of-possession checking for the private key.

The following bullet points describe options beyond IEEE Std 802.1AR-2018 for verifying the device identity of IA-stations in factory default state. It also identifies informational items needed for the corresponding checks:

- IA-station manufacturer check: using names that identify IA-station manufacturers e.g., mfg-name in ietf-hardware YANG module,
- IA-station type check: using attributes that identify IA-station types e.g., model-name, hw-revision, description in ietf-hardware YANG module, and
- IA-station instance check: using values that identify IA-station instances e.g., serial-num in ietf-hardware YANG module.

The following model described in the bullet points applies to the verification of the initial device identity of IA-stations:

- the set of to-be-conducted checks is determined by IA-station and CNC users,
- an IA-station uses IDevID credentials to prove its device identity. The checking happens by means of online interactions in the operational network. It happens automatically and is done by CNCs. This does not depend on configuration-domain external repositories, and
- other stakeholders e.g., middleware/application consortia or individual manufactures are allowed to additionally express information items in IDevID credentials to reflect their device identity model. CNCs do not assess such additional information.

4.8.6.3.6 Device Identity Representation in IDevID and LDevID Credentials

The best practices for representing verifiable device identity information in IDevID and LDevID credentials (see 6.3.3.2.2 for more information) are:

- Corresponding information (actual values or references to them) appears in EE certificates:
 - IDevID EE certificates bind initial device identity items that are known by the device manufacturer at production time e.g., mfg-name.
 - LDevID EE certificates bind locally significant device identity items that are known by other actors such as device users e.g., DNS names or IP addresses. They can also bind initial device identity information.
- Items that encode device naming information appear in the subjectAltName extension.
NOTE This is specified in IETF RFC 5280, 4.2.1.6. It is further explained in IETF RFC 6125, 2.3.
- A binding can take one of following forms. Multiple forms can appear in one EE certificate:
 - By-value: the verifiable device identity information is represented by its value inside the IDevID resp. LDevID EE certificate. Examples are:
 - the product serialNumber in IDevID credentials (IEEE Std 802.1AR-2018) and,
 - the hostname of the NETCONF/YANG server in LDevID-NETCONF credentials (IETF RFC 6125, Clause 6).
 - By-ref: the verifiable device identity information is represented by a reference inside the IDevID resp. LDevID EE certificate, not by its value:
 - The actual value can be provided by the device itself or by a device-external source, and
 - If it is provided in form of an unprotected information object, then the reference object that is embedded to EE certificates includes a digest value.

5 Conformance

5.1 General

A claim of conformance to this document is a claim that the behavior of an implementation of an IA-station (see 5.5, 5.6) with its Bridge components (see 5.7, 5.8) and end station components (see 5.9, 5.10) meets the mandatory requirements of this document and may support options identified in this document. Furthermore this document includes conformance requirements for CNC and CUC implementations (see 5.11, 5.13).

5.2 Requirements terminology

The verbal forms for required expressions of provisions follow the conventions:

- Requirements terminology is provided in the ISO/IEC Directives Part 2:2021, Clause 7. This document can be found at www.iec.ch/members_experts/refdocs.
- The Profile Conformance Statement (PCS) proformas (see Annex A) reflect the occurrences of the words “shall,” “may,” and “should” within this document.
- This document 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.”

5.3 Profile conformance statement (PCS)⁴

The supplier of an implementation that is claimed to conform to this document shall provide the information necessary to identify both the supplier and the implementation and shall complete a copy of the PCS proforma provided in Annex A.

5.4 Conformance classes

This document includes conformance requirements and options that are related to an entire station, as well as conformance requirements and options that are related to single Bridge or end station components within an IA-station. Figure 11 illustrates this conformance model.

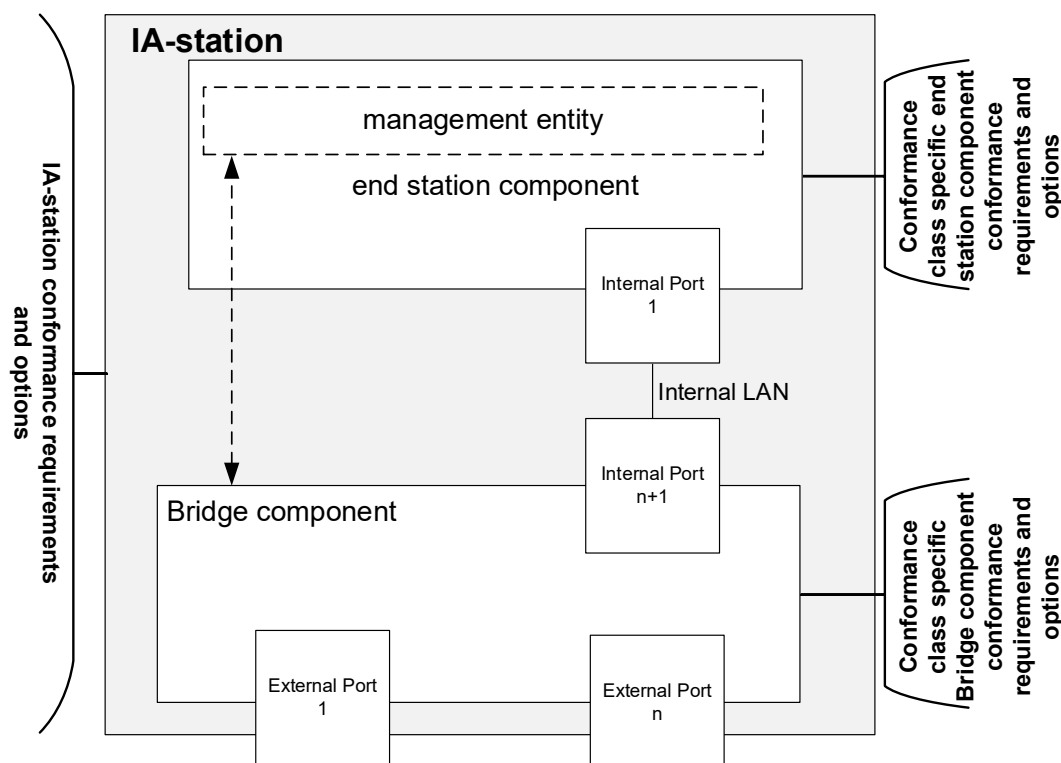


Figure 11 – IA-station conformance model

This document supports a variety of industrial use cases. In some of these use cases, support of certain TSN features might be mandatory, while in others, supporting these features could lead to non-optimal implementations. Therefore, this document defines two conformance

⁴ Copyright release for the PCS: Users of this document may freely reproduce the PCS contained in this document so that they can be used for their intended purpose.

classes that are applicable both to Bridge components and end station components. Conformance Class A (ccA) is feature rich, i.e., tailored to use cases requiring support of many TSN-IA features. Conformance Class B (ccB) targets implementations that are more resource constrained. The details for the conformance classes are specified in 5.7 and 5.8 for Bridge components, and in 5.9 and 5.10 for end station components.

NOTE 1 It is the responsibility of the IA-station manufacturer to carefully consider the implications of mixing ccA and ccB Bridge components and end station components in a single IA-station.

NOTE 2 It is the responsibility of the user to carefully consider the implications of mixing ccA and ccB Bridge components and end station components in a single Configuration Domain.

NOTE 3 Any Bridge compliant to this document is an IA-station. Any IA-station contains a management entity (i.e., an end station component).

5.5 IA-station requirements

5.5.1 IA-station PHY and MAC requirements for external ports

IA-stations for which a claim of conformance to this document is made shall support the following list of requirements for external ports.

- a) Media Access Control (MAC) service specification according to IEEE Std 802.3-2022, Clause 2.
- a) Media Access Control (MAC) frame and packet specifications according to IEEE Std 802.3-2022, Clause 3, especially the MAC Client Data field size according to IEEE Std 802.3-2022, 3.2.7, item c).
- b) Layer Management according to IEEE Std 802.3-2022, 5.2.4.
- c) Implement at least one IEEE Std 802.3-2022 MAC that shall operate in full-duplex mode, and associated IEEE Std 802.3-2022 PHY with a data rate of at least one of speed: 10 Mb/s, 100 Mb/s, 1 000 Mb/s, 2,5 Gb/s, 5 Gb/s, or 10 Gb/s together with the corresponding managed objects:
 - 1) 10BASE-T1L MAU type according to IEEE Std 802.3-2022, Clauses 22 and 146,
 - 2) 100BASE-TX and 100BASE-FX MAU types according to IEEE Std 802.3-2022, Clauses 21, 22, 24, 25, 26, 30, 31 and IEEE Std 802.3-2022, Annexes 23A, 28A, 28B, 28C, 28D, 31A, 31B, 31C, and 31D,
 - 3) 1000BASE-T and 1000BASE-SX MAU types according to IEEE Std 802.3-2022, Clauses 28, 34, 35, 36, 37, 38, and 40,
 - 4) 2.5GBASE-T and 5GBASE-T MAU types according to IEEE Std 802.3-2022, Clauses 28, 125, and 126,
 - 5) 2.5GBASE-T1 and 5GBASE-T1 MAU types according to IEEE Std 802.3-2022, Clause 149,
 - 6) 10GBASE-T and 10GBASE-SR MAU types according to IEEE Std 802.3-2022, Clauses 44, 46, 47, 49, 51, 52, 55, and IEEE Std 802.3-2022, Annexes 48A and 55A,
 - 7) 10GBASE-T1 MAU type according to IEEE Std 802.3-2022, Clause 149,
 - 8) 100BASE-T1 MAU type according to IEEE Std 802.3-2022, Clause 96 and,
 - 9) 1000BASE-T1 MAU type according to IEEE Std 802.3-2022, Clause 97.
- d) Support the YANG features and leaves of the ieee802-ethernet-interface module according to 6.4.9.2.1.
- e) Ethernet support for time synchronization protocols according to IEEE Std 802.3-2022, Clause 90.

NOTE Clauses and subclauses not mentioned can be implemented but are not part of a conformity assessment.

5.5.2 IA-station topology discovery requirements

IA-stations for which a claim of conformance to this document is made shall support the following list of requirements.

- a) The required capabilities according to IEEE Std 802.1AB-2016, 5.3 and IEEE Std 802.1ABcu-2021, 5.3.
- b) Topology discovery and verification according to 6.5.
- c) The YANG features and leaves of the ieee802-dot1ab-ldp module according to 6.4.9.2.2.

5.5.3 IA-station requirements for time synchronization

These requirements are related to the entire IA-station with all its PTP Instances and PTP Ports. IA-stations for which a claim of conformance to this document is made shall support the following list of requirements.

- a) PTP Instance requirements according to IEEE Std 802.1AS-2020, 5.4.1 items a) through i).
NOTE A gPTP domain in a PTP End Instance can be used for Global Time, Working Clock, or both.
- b) Timing and synchronization management according to IEEE Std 802.1AS-2020, 5.4.2 items j) and k).
- c) PTP Instance requirements according to 6.2.2.
- d) PTP Protocol requirements according to 6.2.3.
- e) Error generation limits according to 6.2.4.
- f) PtpInstanceSyncStatus state machine according to 6.2.5.
- g) The transmission of the Drift_Tracking TLV according to IEEE P802.1ASdm, 5.4.2 item n).
- h) The PtpInstanceSyncStatus according to 6.2.5.
- i) External port configuration capability according to IEEE Std 802.1AS-2020, 5.4.2 item g).
- j) MAC-specific timing and synchronization methods for IEEE Std 802.3 full-duplex links according to IEEE Std 802.1AS-2020, 5.5 items a) through d) and item h).
- k) The YANG features and leaves of the:
 - i) ieee1588-ptp module according to 6.4.9.2.3.1,
 - ii) ieee802-dot1as-ptp module according to 6.4.9.2.3.2, and
 - iii) ieee802-dot1as-hs module according to 6.4.9.2.3.3.
- l) The message timestamp point according to IEEE802.1AS-2020, 11.3.9.
- m) The Common Mean Link Delay Service (CMLDS) according to IEEE802.1AS-2020, 11.2.17.
- n) The descriptionDS according to IEEE Std 1588-2019, 8.2.5.

5.5.4 IA-station requirements for management

5.5.4.1 General

These requirements are related to the secured management of an entire IA-station independent of the internal component structure.

5.5.4.2 Secure management exchanges

IA-stations for which a claim of conformance to this document is made shall support the following list of requirements.

- a) NETCONF server functionality according to IETF RFC 6241 including:
 - 1) Candidate configuration capability as described in IETF RFC 6241, 8.3,
 - 2) Rollback-on-Error capability as described in IETF RFC 6241, 8.5, and
 - 3) Validate capability as described in IETF RFC 6241, 8.6.

NOTE The SSH transport protocol, which is mandatory in IETF RFC 6241, 2.3, is not used by IA-stations conformant to this document.

- b) NETCONF-over-TLS server supporting TLS version 1.2, according to IETF RFC 7589, with the cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, based on the

signature algorithm ECDSA with SHA-256 and Curve P-256 (NIST FIPS 186-5 and NIST SP 800-186, 3.2.1.3), according to 6.3.2.1 and 6.3.4.

c) Secure Device Identity according to 6.3.3 and IEEE Std 802.1AR-2018, 5.3 a) using the signature suite in IEEE Std 802.1AR-2018 9.2, 5.3 d), and 5.3 i).

d) PKIX (IETF RFC 5280) according to 6.3.2.1.4 and IETF RFC 5280, 4.1, 4.2.1.1-3, 4.2.1.6, 6.1, 6.2.

e) NACM (IETF RFC 8341) supporting six different roles according to 6.3.2.1.4 c).

f) The YANG features and leaves of the:

1) [draft-ietf-keystore module according to 6.4.9.2.4.1,

2) ietf-netconf-acm module according to 6.4.9.2.4.2 and,

3) [draft-ietf-truststore according to 6.4.9.2.4.3.

g) NETCONF Event Notifications according to IETF RFC 5277 including operations according to IETF RFC 5277, Clause 2.

h) Dynamic Subscription to YANG Events and Datastores over NETCONF as described in IETF RFC 8640.

i) NETCONF Extensions to Support the Network Management Datastore Architecture (NMDA) as described in IETF RFC 8526.

j) DHCP client according to IETF RFC 2131, 4.1, 4.2, and 4.4.

5.5.4.3 IA-station management YANG modules

IA-stations for which a claim of conformance to this document is made shall support the YANG features and leaves for IA-station management of the:

a) ietf-system-capabilities module according to 6.4.9.2.5.1,

b) ietf-yang-library module as according to 6.4.9.2.5.2,

c) ietf-yang-push module according to and 6.4.9.2.5.3,

d) ietf-notification-capabilities module according to 6.4.9.2.5.4,

e) ietf-subscribed-notifications module according to 6.4.9.2.5.5,

f) Diagnostics using YANG-Push subscriptions according to 6.4.7,

g) ietf-netconf-monitoring module according to 6.4.9.2.5.6,

h) ietf-system module according to 6.4.9.2.5.7,

i) ietf-hardware module according to 6.4.9.2.5.8,

j) ietf-interfaces module according to 6.4.9.2.5.9,

k) ieee802-dot1q-bridge module according to 6.4.9.2.5.10,

l) ieciee60802-ethernet-interface module according to 6.4.9.2.5.11 and,

m) ietf-netconf-server according to 6.4.9.2.5.12.

5.5.4.4 Digital data sheet

IA-stations for which a claim of conformance to this document is made shall provide a 60802 instance data file according to 6.4.8. The instance data file shall contain at least the YANG nodes of 6.4.9 that are marked with [m] or [c].

NOTE It is the users responsibility to ensure that the filename is unique by using a standardized mechanism (for example, GUID, URL, or ReverseDomainName).

5.6 IA-station options

5.6.1 IA-station PHY and MAC options for external ports

IA-stations for which a claim of conformance to this document is made may support the following list of requirements.

- a) Power over Ethernet (PoE) over 2 Pairs according to IEEE Std 802.3-2022, Clause 33.
- b) Power Interfaces according to IEEE Std 802.3-2022, Clause 104.
- c) Power over Ethernet according to IEEE Std 802.3-2022 Clause 145.

5.6.2 IA-station options for time synchronization

IA-stations for which a claim of conformance to this document is made may support the following list of requirements.

- a) The media-independent master capability according to IEEE Std 802.1AS-2020, 5.4.2 item b).
- b) Grandmaster PTP Instance capability according to IEEE Std 802.1AS-2020, 5.4.2 item c).
- c) More than one PTP port as a PTP Relay Instance according to IEEE Std 802.1AS-2020, 5.4.2 item d).
- d) Transmit of the Signaling message according to IEEE Std 802.1AS-2020, 5.4.2 item e).
- e) support more than 1 PTP Instance according to IEEE Std 802.1AS-2020, 5.4.2 item f).
- f) The SyncIntervalSetting state machine according to IEEE Std 802.1AS-2020, 5.4.2 item h),
- g) One or more application interfaces according to IEEE Std 802.1AS-2020, 5.4.2 item i).
- h) Hot standby redundancy requirements according to P802.1ASdm, 5.4.2, item m).

5.6.3 IA-station options for management

IA-stations for which a claim of conformance to this document is made may support the following list of requirements.

- a) Writable-Running capability according to IETF RFC 6241, 8.2.
- b) Confirmed Commit capability according to IETF RFC 6241, 8.4.
- c) Distinct Startup capability according to IETF RFC 6241, 8.7.
- d) URL capability according to IETF RFC 6241, 8.8.
- e) XPath capability according to IETF RFC 6241, 8.9.
- f) NETCONF-over-TLS server supporting TLS version 1.2, according to IETF RFC 7589, with one or more of the following cipher suites.
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 according to IETF RFC 5289, 3.2, Clause 5, and
 - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 according to IETF RFC 7905, 2 and Clause 3.

and based on one or more of the following signature algorithms:

 - ECDSA with SHA-512 and Curve P-521 according to NIST FIPS 186-5 and NIST SP 800-186, 3.2.1.5,
 - Ed25519 according to IETF RFC IETF RFC 8032, 5.1, and
 - Ed448 according to IETF RFC 8032, 5.2.
- g) NETCONF-over-TLS server supporting TLS version 1.3, according to IETF RFC 7589 and IETF draft-ietf-netconf-over-tls13, with one or more of the following cipher suites according to IETF RFC 8446, 9.1.
 - TLS_AES_128_GCM_SHA256,
 - TLS_AES_256_GCM_SHA384, and
 - TLS_CHACHA20_POLY1305_SHA256.

and one or more of the following signature schemes:

 - ecdsa_secp256r1_sha256 according to NIST FIPS 186-5 and NIST SP 800-186, 3.2.1.3,

- ecdsa_secp521r1_sha512 according to NIST FIPS 186-5 and NIST SP 800-186, 3.2.1.5,
 - ed25519 according to IETF RFC 8032, 5.1, and
 - ed448 according to IETF RFC 8032, 5.2.
- h) Support the YANG features and leaves of the ietf-keystore (IETF RFC “Internet-Draft (I-D) “ A YANG Data Model for a Keystore - draft-ietf-netconf-keystore) with component-internal or component-external generation of asymmetric key pairs according to 6.3.4.3.
- i) PKIX according to IETF RFC 5280, 4.2.1.13, Clause 5, and 6.3.
- IA-stations for which a claim of conformance to this document is made should support Internal key generation according to 6.3.4.3.2.

5.7 Bridge component requirements

5.7.1 Common Bridge component requirements

A Bridge component implementation of any conformance class for which a claim of conformance to this document is made shall support the following list of requirements.

- a) C-VLAN component requirements according to IEEE Std 802.1Q-2022, 5.5 and 5.4 except item o) in IEEE Std 802.1Q-2022, 5.4.
 - b) The use of Customer VLAN Identifiers (C-VID).
 - c) FDB to contain Static and Dynamic VLAN Registration Entries for a minimum of 10 VIDs, up to a maximum of 4 094 VIDs, according to IEEE Std 802.1Q-2022, 8.8.
- NOTE 1 An example use case for 8 VIDs: 2 VIDs for IA time-aware stream or IA stream traffic, 2 VIDs for IA time-aware stream or IA stream redundancy, 4 VIDs for IA traffic engineered non-stream or IA non-stream traffic, 1 isolation VID, and 1 default VID (see 6.4.5.2).
- d) Translation of VIDs through support of the VID Translation Table or through support of both the VID Translation Table and Egress VID translation table on one or more Bridge Ports according to IEEE Std 802.1Q-2022, 6.9.
 - e) 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.
 - f) The capability to disable Priority-based flow control if it is implemented according to IEEE Std 802.1Q-2022, Clause 36.
 - g) The Priority Regeneration requirements according to IEEE Std 802.1Q-2022, 5.4.1, item o).
 - h) MST according to IEEE Std 802.1Q-2018, 5.4.1.1 a) to i) and k) to o) and 6.4.2.4.
 - i) TE-MSTID according to IEEE Std 802.1Q-2022, 8.6. and 8.8 and IEEE Std 802.1Q-2022, 5.5.2.
 - j) Spanning tree, VLAN, and TE-MSTID configuration according to 6.4.2.4.
 - k) The I2vlan interface types per 6.4.2.5.
 - l) Flow meters including support of at least 3 flow meters per port, according to IEEE Std 802.1Q-2022 8.6.5.3 items a), b), and f) and 8.6.5.5 items a) through c). A flow meter should set following IEEE Std 802.1Q-2022, 8.6.5.5 parameters to values:
 - Item d) Excess Information Rate (EIR) = 0,
 - Item e) Excess burst size (EBS) = 0, and
 - Item g) Color mode (CM) = color_blind.

NOTE 2 When CM = color_blind, DropOnYellow (IEEE Std 802.1Q-2022, 8.6.5.1.3, item h), MarkAllFramesRed (IEEE Std 802.1Q-2022, 8.6.5.1.3, item j), and MarkAllFramesRedEnable (IEEE Std 802.1Q-2022, 8.6.5.1.3, item i) are not used.

NOTE 3 For example, an implementation could contain one flow meter for broadcast traffic, one flow meter for multicast traffic and one flow meter for unicast traffic.

5.7.2 ccA Bridge component requirements

A Bridge component implementation for which a claim of conformance to ccA of this document is made shall support the following list of requirements.

- a) Common Bridge component requirements according to 5.7.1.
 - b) At least 2 PTP Instances according to 5.5.3.
 - c) Eight queues according to IEEE Std 802.1Q-2022, 8.6.6.
 - d) Enhancements for scheduled traffic for data rates of 100 Mb/s and 1 Gb/s according to IEEE Std 802.1Q-2022, 5.4.1 items ab) and ac) including:
 - 1) a tick granularity of less than or equal to 10 ns according to IEEE Std 802.1Q-2022, 8.6.8.4,
 - 2) The allowable error budget between the transmission selection timing point and the on-the-wire timing point, less any error budget for the PHY (IEEE Std 802.1Q-2022, Figure 12.6), of less than or equal to 10 ns, and
- NOTE Transmission selection timing points have a granularity of 1 ns; however, operation is determined by the precision of the "tick" event.
- 3) Support the YANG features and leaves of the `ieee802-dot1q-sched` module according to 6.4.9.3.2.
 - e) Frame preemption according to IEEE Std 802.1Q-2022, 5.4.1 item ad), for data rates of 100 Mb/s and 1 Gb/s, including:
 - 1) Support of Interspersing Express Traffic with preemptable traffic according to IEEE Std 802.3-2022, Clause 99, including support of the Additional Ethernet Capabilities for TLV in an LLDPDU to indicate supported functions of frame preemption according to IEEE Std 802.3-2022, 79.3.7, and
 - 2) Support of the YANG features and leaves of the `ieee802-dot1q-preemption` module according to 6.4.9.3.4.

5.7.3 ccB Bridge component requirements

A Bridge component implementation for which a claim of conformance to ccB of this document is made shall support the following list of requirements.

- a) Common Bridge component requirements according to 5.7.1.
- b) At least 1 PTP Instance according to 5.5.3.
- c) At least four queues according to IEEE Std 802.1Q-2022, 8.6.6.

5.8 Bridge component options

5.8.1 Common Bridge component options

A Bridge component implementation of any conformance class for which a claim of conformance to this document is made may support the operation of the credit-based shaper algorithm according to 802.1Q, 8.6.8.2 on all Ports as the transmission selection algorithm for at least 4 traffic classes including support of the YANG features and leaves of the `<ieee-cbs>` module according to 6.4.9.3.5.

5.8.2 ccA Bridge component options

A Bridge component implementation for which a claim of conformance to ccA of this document is made may support the following list of requirements.

- a) Any or none of the common Bridge component options according to 5.8.1.
- b) More than 2 PTP Instances according to 5.5.3.
- c) Enhancements for scheduled traffic for data rates of 10 Mb/s, 2,5 Gb/s, 5 Gb/s, and 10 Gb/s according to IEEE Std 802.1Q-2022, 5.4.1 items ab) and ac) including: