



HARMONISED EUROPEAN STANDARD

Cyber Security (CYBER); Cyber Resilience Act (CRA); Cybersecurity requirements for physical and virtual network interfaces

Exercising one of the **Principles of International Standardization – Openness** – and taking them to a different level, ETSI CYBER-EUSR has conducted open consultations on the vertical standards in support of the Cyber-Resilience Act, at a much earlier stage than it is usual in the standardization world. In this context, please keep in mind that the present document is an INTERIM draft, which expectably will be subject to substantial changes before their target publication date in the second semester of 2026.

ETSI CRA vertical standards v1.1.1 are being finalized and undergoing Public Enquiry via the National Standardization Organizations (NSO). Therefore, starting from 16 April 2026, ETSI CYBER-EUSR may only be able to address your comments in a future revision of the standard. **To enable ETSI CYBER-EUSR to address your comments before the first publication of the standards, you should cumulatively submit to your NSO any comments submitted here from 16 April 2026 onwards.** If you don't know how to do this, email us at cybersupport@etsi.org and we will guide you in the process.

Disclaimer: The INTERIM DRAFTS available for download in this page are provided for information and are for future development work within the ETSI Technical Committee CYBER EUSR Working Group (CYBER-EUSR) only. ETSI and its Members accept no liability for any further use/implementation of these specifications. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at <http://www.etsi.org/standards-search>

Commenting guidelines: Your comments to improve this early draft are very welcomed. To ensure the effectiveness of your contribution, please make sure to include the following elements in your comment:

1. Clear identification of the section of the draft your comment is referring to.
2. Objective proposal to delete content, add content or substitute content.
3. Concrete contribution (exact content you suggest including in the draft as an addition to, or in substitution of, existing content).
4. Brief rationale to justify the proposal (e.g. why the suggested content should be added an/or the existing content should be deleted or substituted).

Please note that comments without concrete contributions will be noted but not acted upon by ETSI CYBER-EUSR. We trust and value your expertise and therefore expect you to take this opportunity to proactively contribute to solving the issues you find while analysing this early draft.

Use of Artificial Intelligence (AI): Please do not use large language models to generate your comments. Inclusion of language generated by “AI” creates a potential for intellectual property conflicts and liability for ETSI, which is not acceptable.

How to comment: To comment or provide feedback on the present interim draft please visit: [STAN4CRA / EN 304 631 Smart home assistants · GitLab](#) and submit your comments as “issues” following the guidelines provided on this site. Alternatively, you may also send your comments to: cybersupport@etsi.org using the “[ETSI Commenting Format for Open Consultation.xlsx](#)” available in <https://docbox.etsi.org/CYBER/EUSR/Open>

Feedback on your comments: The resolutions made in **Consensus** by ETSI CYBER-EUSR members, on each comment received through these Open Consultations will be published at the ETSI Open Area and ETSI Lab, assuring full **Transparency**.

Reference

< TC/WI-Number >

Keywords

< CRA, Cybersecurity, Interfaces >

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

0

1 **Contents**

2	Intellectual Property Rights	8
3	Foreword.....	8
4	Modal verbs terminology	8
5	Executive summary	9
6	1 Scope	10
7	1.1 General.....	10
8	1.2 Products in scope	10
9	2 References	10
10	2.1 Normative references.....	10
11	2.2 Informative references	11
12	3 Definition of terms, symbols and abbreviations.....	11
13	3.1 Terms.....	11
14	3.2 Abbreviations.....	12
15	4 Product context.....	14
16	4.1 Intended purpose and reasonably foreseeable use	14
17	4.2 Product functions	14
18	4.2.1 Physical network interface product functions	14
19	4.2.2 Device driver product functions	14
20	4.2.3 Virtual network interface product functions.....	14
21	4.3 Product architecture.....	14
22	4.3.1 Overview	14
23	4.3.2 Types of network interface.....	15
24	4.3.3 Device drivers for network interfaces	17
25	4.4 Operational Environment.....	18
26	4.5 Distribution of security functions	18
27	4.5.1 General.....	18
28	4.5.2 Security functions provided outside the product.....	18
29	4.5.3 Security functions provided to other components	18
30	4.6 Users	19
31	4.7 Use cases.....	19
32	4.7.1 Wired network interface use cases	19
33	4.7.2 Wireless network interface use cases	21
34	4.7.3 Virtual network interface use cases.....	22
35	5 Cybersecurity requirement specifications	23
36	5.1 Notes on the structure of cybersecurity requirements.....	23
37	5.2 Technical cybersecurity requirements specifications.....	23
38	5.2.1 General.....	23
39	5.2.1 ER-NKEV: No known exploitable vulnerabilities at first use.....	24
40	5.2.1.1 Cybersecurity requirement	24
41	5.2.1.2 MI-KEVD: Documentation for secure update before or during first use	24
42	5.2.1.3 MI-KEVA: Automatic secure update before or during first use.....	24
43	5.2.1.4 MI-KEVM: Documentation of mitigation of known exploitable vulnerabilities	25
44	5.2.1.5 MI-KEVT: Testing for known exploitable vulnerabilities	25
45	5.2.1.6 MI-SCAN: No easily scannable known exploitable vulnerabilities	25
46	5.2.1.7 Mapping of mitigations to risk factors and security profiles	26
47	5.2.2 ER-SSDD: Secure design and development.....	26
48	5.2.2.1 Cybersecurity requirement	26
49	5.2.2.2 MI-SSCA: Static source code analysis for memory errors.....	26
50	5.2.2.3 MI-FZ95 Runtime code coverage checking with memory access error detection.....	27
51	5.2.2.4 MI-IMSL Implement in a memory-safe language	27
52	5.2.2.5 MI-BTIN Boundary testing of inputs that may cause memory errors	27
53	5.2.2.6 MI-SCFS: Secure compilation flags.....	28

54	5.2.2.7	Mapping of mitigations to risk factors and security profiles	28
55	5.2.2.8	MI-MSAF-1: Stack exhaustion detection	28
56	5.2.2.9	MI-MSAF-2: Stack linear buffer overflow detection	28
57	5.2.2.10	MI-MSAF-3: Array bounds checking	28
58	5.2.2.11	MI-MZRO-1: Stack memory initializing.....	29
59	5.2.2.12	MI-MZRO-2: Heap memory initializing.....	29
60	5.2.3	ER-LMII: Limit incident impact	29
61	5.2.3.1	Cybersecurity requirement	29
62	5.2.4	ER-MINI: Minimize impact on other devices and services	29
63	5.2.4.1	Cybersecurity requirement	29
64	5.2.4.2	MI-MDOC: Document transfer of risk of minimizing impact to operating environment	29
65	5.2.4.3	MI-MPHY: Prevent denial of service at physical layer.....	30
66	5.2.4.4	Mapping of mitigations to risk factors and security profiles	30
67	5.2.5	ER-SDEF: Secure by default configuration	30
68	5.2.5.1	Cybersecurity requirement	30
69	5.2.5.2	MI-ADEF: Authorization required by default to access security-relevant assets.....	30
70	5.2.5.3	MI-DPAH: Documentation of product assets accessible from host	31
71	5.2.5.4	MI-PDDI-1: Document how to protect access to debug/management interfaces.....	31
72	5.2.5.5	MI-PDDI-2: Protect or disable physical access to debug/management interfaces	31
73	5.2.5.6	MI-PDDI-3: Protect or disable local software access to debug/management interfaces	32
74	5.2.5.7	MI-PDDI-4: Protect or disable network access to debug/management interfaces.....	32
75	5.2.5.8	Mapping of mitigations to risk factors and security profiles	33
76	5.2.6	ER-SCUD: Secure updates.....	33
77	5.2.6.1	Cybersecurity requirement	33
78	5.2.6.2	MI-SUDC: Documentation of secure update.....	33
79	5.2.6.3	MI-SUVP: Secure update via product	33
80	5.2.6.4	MI-SUAP: Automatic secure update via product.....	33
81	5.2.6.5	MI-SUOE: Secure update provided by operational environment.....	34
82	5.2.6.6	MI-SUAO: Automatic secure update provided by operational environment	34
83	5.2.6.7	Mapping of mitigations to risk factors and security profiles	34
84	5.2.7	ER-AUTH: Authentication and access control	34
85	5.2.7	ER-CDST: Confidentiality of data stored on the product	35
86	5.2.7.1	Cybersecurity requirement	35
87	5.2.7.2	MI-CDST: Protect confidentiality of data stored on the product.....	35
88	5.2.7.3	Mapping of mitigations to risk factors and security profiles	35
89	5.2.8	ER-CDTX: Confidentiality of data transmitted by product	35
90	5.2.8.1	Cybersecurity Requirement	35
91	5.2.8.2	MI-CDTX: Protect confidentiality of data transmitted by product.....	35
92	5.2.8.3	MI-DOCC: Document transfer of risk of confidentiality of data transmitted by product	36
93	5.2.8.4	Mapping of mitigations to risk factors and security profiles	36
94	5.2.9	ER-CRYP: Encryption.....	36
95	5.2.10	ER-IDST: Integrity of data stored on the product	36
96	5.2.10.1	Cybersecurity requirement	36
97	5.2.10.2	MI-IDST: Protect integrity of data stored on the product.....	36
98	5.2.10.3	MI-DCST: Detect corruption of data stored.....	37
99	5.2.10.4	Mapping of mitigations to risk factors and security profiles	37
100	5.2.11	ER-IDTX: Integrity of data transmitted by the product	37
101	5.2.11.1	Cybersecurity requirement	37
102	5.2.11.2	MI-DCTX: Detect corruption of data transmitted by the product	37
103	5.2.11.3	Mapping of mitigations to risk factors and security profiles	38
104	5.2.12	ER-DMIN: Data Minimization	38
105	5.2.12.1	Cybersecurity requirement	38
106	5.2.12.2	MI-DJST: Document and justify processed data.....	38
107	5.2.12.3	Mapping of mitigations to risk factors and security profiles	38
108	5.2.13	ER-AVAI: Availability	38
109	5.2.13.1	Cybersecurity requirement	38
110	5.2.13.2	MI-WDOG: Watchdog and self-initiated reset.....	39
111	5.2.13.3	MI-NTFY: Watchdog and notification of host.....	39
112	5.2.13.4	MI-FDRP: Fast packet drop	39
113	5.2.13.5	MI-LMEM: Limit memory usage	39
114	5.2.13.6	MI-FAIR: Fair resource usage and prioritisation	39
115	5.2.13.7	MI-DOST: Document risk transfer to operational environment for denial of service.....	40

116	5.2.14	ER-LMAS: Minimize exposed interfaces	40
117	5.2.14.1	Cybersecurity requirement	40
118	5.2.14.2	MI-JSTY: Document and justify exposed interfaces.....	40
119	5.2.14.3	Mapping of mitigations to risk factors and security profiles	40
120	5.2.15	ER-LOGG: Logging and monitoring	40
121	5.2.15.1	Cybersecurity requirement	40
122	5.2.15.2	MI-LOGG: Logging	40
123	5.2.16	ER-SCDL: Secure deletion	41
124	5.2.16.1	Cybersecurity requirement	41
125	5.2.16.2	MI-RSET: Secure deletion via reset	41
126	5.2.16.3	MI-INST: Secure deletion via reinstallation.....	41
127	5.2.16.4	MI-DELE: Secure deletion via secure deletion function.....	42
128	5.2.16.5	Mapping of mitigations to risk factors and security profiles	42
129	5.2.17	ER-SDTR: Secure data read and transfer.....	42
130	5.2.17.1	Cybersecurity requirement	42
131	5.2.17.2	MI-SDRF: Secure data read from product.....	42
132	5.2.17.3	MI-SDTR: Secure data transfer to another product.....	43
133	5.2.17.4	Mapping of mitigations to risk factors and security profiles	43
134	5.2.18	ER-VULH: Vulnerability handling	43
135	5.2.18.1	Cybersecurity requirement	43
136	5.2.18.2	MI-VULH: Vulnerability handling.....	43
137	5.3	Risk Mitigation Sets.....	43
138	5.3.1	Introduction	43
139	5.3.1	Wired network interface risk mitigation sets.....	43
140	5.3.1.1	SP-WD-1 required mitigations	43
141	5.3.1.2	SP-WD-2 required mitigations	44
142	5.3.1.3	SP-WD-3 required mitigations	44
143	5.3.1.4	SP-WD-4 required mitigations	45
144	5.3.2	Wireless network interface risk mitigation sets.....	46
145	5.3.2.1	SP-WL-1 required mitigations.....	46
146	5.3.2.2	SP-WL-2 required mitigations.....	47
147	5.3.2.3	SP-WL-3 required mitigations.....	48
148	5.3.3	Virtual network interface risk mitigation sets	49
149	5.3.3.1	SP-VI-1 required mitigations.....	49
150	5.3.3.2	SP-VI-2 required mitigations.....	49
151	6	Conformity Assessment	50
152	6.1	General.....	50
153	6.2.13.4	MI-FDRP assessment.....	50
154	Activities	50	
155	Verdict	51	
156	Supporting evidence	51	
157	6.2.13.5	MI-LMEM assessment.....	51
158	Activities	51	
159	Verdict	51	
160	Supporting evidence	52	
161	6.2.13.6	MI-FAIR assessment.....	52
162	Activities	52	
163	Verdict	52	
164	Supporting evidence	52	
165	6.2.13.7	MI-DOST assessment	52
166	Activities	52	
167	Verdict	53	
168	Supporting evidence	53	
169	Annex A (informative): Mapping between the present document and CRA essential requirements.....		54
170	Annex B (informative): Relationship between the present document and any related ETSI standards (if		
171	any).....		55
172	Annex C (informative): Risk identification and assessment methodology		56
173	C.1	Assets.....	56
174	C.1.1	Data 56	

175	C.1.1.1 Physical network interfaces.....	56
176	C.1.1.2 Virtual network interfaces or device drivers	56
177	C.1.2 Product functions	56
178	C.1.2.1 Physical network interface essential functions.....	56
179	C.1.2.2 Device driver essential functions	57
180	C.1.2.3 Virtual network interface essential functions.....	57
181	C.2 Risk factors	57
182	C.2.1 List of risk factors	57
183	C.3 Assumptions	60
184	C.3.1 Proper host system	60
185	C.3.2 Proper administrator.....	60
186	C.3.3 Attacker has limited physical access to product.....	60
187	C.3.4 Attacker has limited resources	60
188	C.4 Threats and risk assessment of threats	60
189	C.4.1 General60	
190	C.4.2 Risk assessment methodology.....	61
191	C.4.3 List of threats, risk assessments, and mitigations.....	61
192	C.4.3.1 TH-UEVU: Unknown exploitable vulnerabilities.....	61
193	C.4.3.2 TH-KEVU: Known exploitable vulnerabilities.....	62
194	C.4.3.3 TH-PHYS: Access to data via acquisition of used product.....	62
195	C.4.3.4 TH-CONF: Access to assets via configuration errors	62
196	C.4.3.5 TH-UADT: Unauthorized access to confidential data transmitted.....	63
197	C.4.3.6 TH-AVAI: Denial of service attack on product via exploitation of vulnerabilities	63
198	C.4.3.7 TH-PDOS: Denial of service attack on product functions via system or network access.....	64
199	C.4.3.8 TH-DDOS: Denial of service attack on other products via exploitation of vulnerabilities	64
200	C.4.3.9 TH-MQSE: Masquerading authorized server.....	64
201	C.4.3.10 TH-AHHS: Harm to host system via unauthorized access through the network	65
202	C.5.2 Mapping of use cases to risk factors and security profiles	66
203	C.5.2.1 Wired network interface use cases	66
204	C.5.2.2 Wireless network interface use cases	66
205	C.5.2.3 Virtual network interface use cases.....	66
206	C.6 Security profiles.....	66
207	C.6.1 General66	
208	C.6.2 Mapping of security profile to risk factors.....	66
209	C.6.2.1 Wired network interface security profiles	66
210	C.6.2.2 Wireless network interface security profiles	67
211	C.6.2.3 Virtual network interface security profiles.....	67
212	C.7 How to add new security profiles	67
213	Annex D (informative): Risk evaluation guidance.....	68
214	D.1 Explanation of Risk Modeling Approach	68
215	D.2 Mapping of risks to cybersecurity requirements.....	68
216	D.3 Risk acceptance criteria	69
217	D.4 Risks not treated by the cybersecurity requirements.....	69
218	Annex E: Explanation of the present document (informative only).....	70
219	E.1 Introduction.....	70
220	E.2 How to understand a vertical standard.....	70
221	E.2.1 General 70	
222	E.2.2 TL;DR 70	
223	E.3 Standard basics	70
224	E.3.1 Normative and informative text.....	70
225	E.3.2 Cybersecurity requirements describe default configuration only	70
226	E.4 CRA vertical standard specifics.....	71
227	E.4.1 Vertical standards are optional	71
228	E.4.2 Manufacturer declares intended purpose/use case.....	71
229	E.4.3 Intended purpose/use case and capabilities determines how to satisfy cybersecurity requirements.....	71
230	E.4.4 Each cybersecurity requirement can be satisfied by one or more mitigations.....	71
231	E.4.5 Risk factors determine which mitigations are necessary	71
232	E.4.6 Use cases are grouped into security profiles	71
233	E.4.7 New use cases and security profiles may be contributed	71
234	E.4.8 Manufacturer may use any CRA-conformant risk assessment methodology	71

235	Annex F (informative): Change history.....	72
236	History	73
237		
238		

239 Intellectual Property Rights

240 Essential patents

241 IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations
 242 pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be
 243 found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to*
 244 *ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the
 245 [ETSI IPR online database](#).

246 Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs,
 247 including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not
 248 referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become,
 249 essential to the present document.

250 Trademarks

251 The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners.
 252 ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no
 253 right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does
 254 not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

255 **DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its
 256 Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of
 257 the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members
 258 and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM
 259 Association.

260 **BLUETOOTH®** is a trademark registered and owned by Bluetooth SIG, Inc.

261 Foreword

262 DRAFT FOREWORD - DO NOT CONSIDER THE CONTENT

263 The present document has been prepared under the Commission's standardisation request C(2025) 618 [
 264 i.3] final to provide one voluntary means of conforming to the requirements of Regulation (EU) No
 265 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal
 266 cybersecurity requirements for products with digital elements and amending Regulations (EU) No
 267 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)[i.1].

268

269 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
 270 with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the
 271 present document, a presumption of conformity with the corresponding essential requirements of that Regulation and
 272 associated EFTA regulations.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	18 months after doa

273

274 The Technical Body should advise the ETSI Secretariat if the above default national transposition dates are
 275 inappropriate for the particular standard.

276 Modal verbs terminology

277 In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and
 278 "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of
 279 provisions).

280 "**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

281 **Executive summary**

282 **Before commenting, please read Annex E for an informative explanation of the use and function of the present**
283 **document.**

284

285 1 Scope

286 1.1 General

287 The present document specifies cybersecurity requirements and related assessment criteria for physical and virtual
288 network interfaces.

289 1.2 Products in scope

290 Products in scope include products whose purpose is to serve as a virtual or physical network interface intended to
291 enable the connection of a computing device to a network. A network interface provides connectivity via a device driver
292 API operating at the data link layer.

293 Physical network interfaces are products that directly connect a device to a network via an application programming
294 interface (API) provided by device drivers. This connection may be wired or wireless and feature hardware adapters to
295 transmission media with corresponding firmware, typically physical network interfaces operate at the physical and data
296 link layer. Products that are connected to a host system by a communications bus, such as PCIe or USB are physical
297 network interfaces, though they may use a wide variety of technologies to enable this connection including both direct
298 physical connections and wireless connections. The category of physical network interfaces is broad and composed of
299 wired and wireless network interface cards, controllers and adapters, and network interface hardware modules, such as
300 for Wi-Fi™, Ethernet, cellular modems, IrDA, USB, Bluetooth®, NearLink, Zigbee®, Fieldbus, or Infiniband.

301 Virtual network interfaces are products that directly or indirectly connect a device to a network via an API that emulates
302 that of device drivers or physical network interfaces, typically operating at the data link layer. These virtual network
303 interfaces consist of software running on a host system, and communicate via the device driver interface of that host. As
304 purely virtual, standalone products, a virtual network interface remains a product whose core function is that of a
305 network interface and that provides a remote management interface for the network interface or the host system.
306 Examples of virtual network interfaces also include: container network interfaces, VPN interfaces, and loopback
307 interfaces.

308 For the purposes of the present document, network interfaces will be split up into the following groups, due to their
309 distinct threat models:

- 310 • Wired network interfaces
- 311 • Wireless network interfaces
- 312 • Virtual network interfaces

313 Network interfaces are closely related to what is commonly called a "modem", but this general term is used for two
314 different kinds of products:

- 315 1. "Modem interface": A single network interface that connects a physical transmission adapter to a system bus,
316 as for example a 5G modem interface or Power Line Communication device
- 317 2. "Standalone modem": A device with two or more network interfaces that routes network data between two
318 different networks, relaying data from one type of physical transmission media to another, such as a cable
319 modem

320 "Modem interfaces" are included in the present document. "Standalone modems" are excluded from the present
321 document, but may be found in the vertical CRA standard for Routers Modems & Switches [i.7]

322 2 References

323 2.1 Normative references

324 The following referenced documents are necessary for the application of the present document.

- 325 [1] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability
326 Handling", (produced by CEN).

327 2.2 Informative references

328 References are either specific (identified by date of publication and/or edition number or version number) or
 329 nonspecific. For specific references, only the cited version applies. For non-specific references, the latest version of the
 330 referenced document (including any amendments) applies.

331 NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee
 332 their long-term validity.

333 The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's
 334 understanding but are not required for conformance to the present document.

335 [i.1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on
 336 horizontal cybersecurity requirements for products with digital elements and amending
 337 Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber
 338 Resilience Act)

339 [i.2] EN 18031-1 (2024): "Common security requirements for radio equipment - Part 1: Internet
 340 connected radio equipment", , (produced by CEN).

341 [i.3] C(2025)618 – Standardisation request M/606: Commission Implementing decision of 3.2.2025 on
 342 a standardisation request to the European Committee for Standardisation (CEN), the European
 343 Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications
 344 Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU)
 345 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal
 346 cybersecurity requirements for products with digital elements and amending Regulations (EU) No
 347 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

348 [i.6] CEN/CLC JTC13: "Cybersecurity and Data Protection".

349 [i.5] ETSI TS 103 732 "Consumer Mobile Device Protection Profile".

350 [i.6] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements – Vocabulary",
 351 (produced by CEN).

352 [i.7] ETSI EN 304 627 "Essential cybersecurity requirements for routers, modems intended for the
 353 connection to the internet, and switches".

354 3 Definition of terms, symbols and abbreviations

355 3.1 Terms

356 For the purposes of the present document, the following terms apply:

357 NOTE: This clause provides terms and definitions based on CEN/CLC JTC13 WG09's [i.6] work on terms and
 358 definitions, terms and definitions provided by ETSI TS 103 701 [i.5], prEN 40000-1-1 [i.6], and by CEN/CLC EN
 359 18031 [i.2] series. **Cybersecurity requirement:** A requirement described within this standard to conform to the
 360 "Essential requirements" of the Cyber Resilience Act [i.1]

361 **device driver:** piece of software or firmware running on the host that enables communication on the network via the
 362 network interface

363 **Essential requirement:** A requirement described within the Cyber Resilience Act, primarily those listed in its Annex
 364 I [i.1]

365 **firmware:** software stored within a device's non-volatile memory, such as ROM or flash memory, and executed by
 366 different types of hardware which can include the physical network interface and the host

367 **host:** any equipment to which the network interface part provides additional functionality, mainly network connectivity,
 368 and to which connection is necessary for the network interface to operate

369 **modem interface:** A single network interface that connects a physical transmission adapter to a system bus

- 370 **Network Interface (NI):** virtual or physical network interface
- 371 **Network Device Driver Interface (NDDI):** standardized interface provided by the host operating system or software
372 framework that abstracts the underlying network hardware or virtualized network devices
- 373 **physical network interface:** hardware device that directly connects to a network using a hardware adapter to the
374 transmission media and is connected to a host system by a communications bus
- 375 **physical transmission media adapter:** physical adapter on a network interface that transmits and receives data on the
376 medium
- 377 **physical transmission medium:** physical instantiation of a network, which can be wired or wireless
- 378 **standalone modem:** device with two or more network interfaces that routes network data between two different
379 networks, relaying data from one type of physical transmission media to another
- 380 **system bus:** data transmission bus also connecting one or more physical network interfaces to a host
- 381 **Virtual Network Interface (VNI):** software-based network interface that simulates the functionality of a physical
382 network interface
- 383 **wired network interface:** physical network interface which transmits data through a fixed, specific medium such as
384 Ethernet cable, fibre optic cable, coaxial cable or power lines
- 385 **wireless network interface:** physical network interface which transmits data in a manner that does not require a
386 specific medium, such as radiofrequency waves or visible light communication through the air

387 3.2 Abbreviations

388 For the purposes of the present document, the following abbreviations apply:

389	ADEF	Authorization Required by Default
390	ADM	Availability and Skill of Administration
391	API	Application Programming Interface
392	AHHS	Harm to Host System Via Unauthorized Access Through the Network
393	AS	Assumption
394	AUTH	Authentication
395	AVAI	Availability
396	BTIN	Boundry Testing of Inputs
397	CDST	Confidentiality of Stored Data
398	CDTX	Confidentiality of Transmitted Data
399	CEN	Comité Européen de Normalisation
400	COM	Complexity of Product Functions
401	CONF	Configuration (Errors)
402	CRA	Cyber Resilience Act
403	CYRP	Encryption
404	DCTX	Detect Corruption of Transmitted Data
405	DCST	Detect Corruption of Storedd Data
406	DDOS	Denial of Service (Attack)
407	DELE	Secure Deletion Via Secure Delete Function
408	DJST	Document and Justify Processed Data
409	DMIN	Data Minimization
410	DOCC	Documentation of Risk of Confidential Data Transfer
411	DOST	Documentation of Risk Transfer to Operational Environment
412	DPAH	Documentation of Product Assets Accessible from Host
413	ER	Essential Security Requirement
414	FAIR	Fair Resource Usage and Prioritization
415	FDRP	Fast PAcKet Drop
416	FUN	Sensitivity of Functions
417	IDST	Integrity of Stored Data
418	IDTX	Integrity of Transmitted Data
419	IMSL	Implement in Memory Safe Language
420	INST	Secure Deletion Via Reinstallation
421	INT	Integration in Host System

422	IoT	Internet of Things
423	ISP	Internet Service Provider
424	IrDA	Infrared Data Association
425	IT	Information Technology
426	IXP	Internet Exchange Point
427	JSTY	Document and Justify Exposed Interfaces
428	KEV	Known Exploitable Vulnerability
429	KEVU	Known Exploitable Vulnerability
430	LIS	Ease of Reading From Transmission Media of Directly Attached Network by Unauthorized Agents
431	LMAS	Minimize Exposed Interfaces
432	LMEM	Limited Memory Usage
433	LMII	Limit Incident Impact
434	LOGG	Logging and Monitoring
435	MDOC	Document Transfer of Risk Minimizing Impact on Operational Environment
436	MI	Mitigation
437	MINI	Minimization of Impact on Other Devices
438	MPHY	Preventing Attack at Physical Layer
439	MQSE	Masquerading Authorized Server (Attack)
440	MSA	Market Surveillance Authority
441	MSAF	Memory Safety
442	MZRO	Memory Stack Zeroing
443	NDDI	Network Device Driver Interface
444	NET	Degree of Public Access to Attached Network
445	NI	Network Interface
446	NKEV	No Known Exploitable Vulnerabilities
447	NTFY	Watchdog and Notification of Host
448	OS	Operating System
449	OT	Operational Technology
450	PCIe	Peripheral Component Interconnect Express
451	PDDI	Protect, Document, or Disable Interface
452	PDOS	Denial of Service Attack on Product Functions
453	PHY	Physical Layer
454	PHYS	Acquisition of Physical Product
455	PII	Personally Identifiable Information
456	PXE	Preboot Execution Environment
457	ROM	Read Only Memory
458	RSET	Secure Deletion Via Reset
459	RTOS	Real Time Operating System
460	SCAN	No Easily Scannable Vulnerabilities
461	SCDL	Secure Deletion
462	SCFS	Secure Completion Flags
463	SCUD	SEcure Updates
464	SDEF	Secure Default Configuration
465	SDS	Sensitivity of Data Stored
466	SDRF	Secure Data Read From Product
467	SDT	Sensitivity of Data Transferred
468	SDTR	Secure Data Read and Transfer
469	SFT	Sensitivity of Data Stored
470	SSCA	Static Source Code Analysis
471	SSDD	Secure Design and Development
472	SUAP	Automatic Secure Update Via Product
473	SUAO	Automatic Secure Update Provided by Operational Environment
474	SUDC	Documentation of Secure Update
475	SUOE	Secure Update Provided by Operational Environment
476	SUVP	Secure Update Via Product
477	SP	Security Profile
478	SYS	Impact of Access to Host System Assets
479	TH	Threat
480	TV	Television
481	UADT	Unauthorised access to confidential data transmitted
482	UC	Use Case
483	UEVU	Unknown Exploitable Vulnerabilities

484	USB	Universal Serial Bus
485	VI	Virtual Interface
486	VNI	Virtual Network Interface
487	VPN	Virtual Private Network
488	VULH	Vulnerability Handling
489	WD	Wired Interface
490	WDOG	Watchdog and Self-initiated Reset
491	WL	Wireless Interface
492	WPA2	Wi-Fi Protected Access 2

493 4 Product context

494 4.1 Intended purpose and reasonably foreseeable use

495 The intended purpose and reasonably foreseeable use of this product is to provide communication between computer
496 systems over a network, whether physical or virtual.

497 4.2 Product functions

498 4.2.1 Physical network interface product functions

499 A physical network interface is the link between the physical transmission media and the host system. The product's
500 essential function is to transfer data between the network and the host.

501 The product supports configuration of itself by the host. The host system may configure settings related to transmitting
502 data, encryption, or features like waking the host after a packet arrives at the network interface.

503 The product may keep and report statistics about network traffic or its internal functions.

504 The product may update or load its own firmware. The host system may be able to update or load firmware to the
505 product.

506 The product may be able to take actions that affect the entire host system, such as power cycling or reading any part of
507 memory.

508 4.2.2 Device driver product functions

509 A device driver manages the network interface on behalf of the host system, often presenting a standardized network
510 device driver interface to the host operating system. It manages the transfer of data from the network interface to and
511 from host memory. It carries out requests by the host software, such as configuration or loading firmware. It may keep
512 and report statistics about network traffic.

513 4.2.3 Virtual network interface product functions

514 A virtual network interface presents a network device driver interface to the rest of the host software. It may encrypt,
515 filter, transform, route, discard, or otherwise modify network traffic entering the interface. The network traffic may then
516 be directed to another virtual network interface on the same host, to another executable on the host, or to a physical
517 network interface.

518 4.3 Product architecture

519 4.3.1 Overview

520 For the purposes of this standard, a physical network interface consists of:

- 521 • A local bus interface to connect to the host via a communications bus
- 522 • A hardware transceiver to communicate on the network
- 523 • Hardware and firmware to process incoming signals and host commands

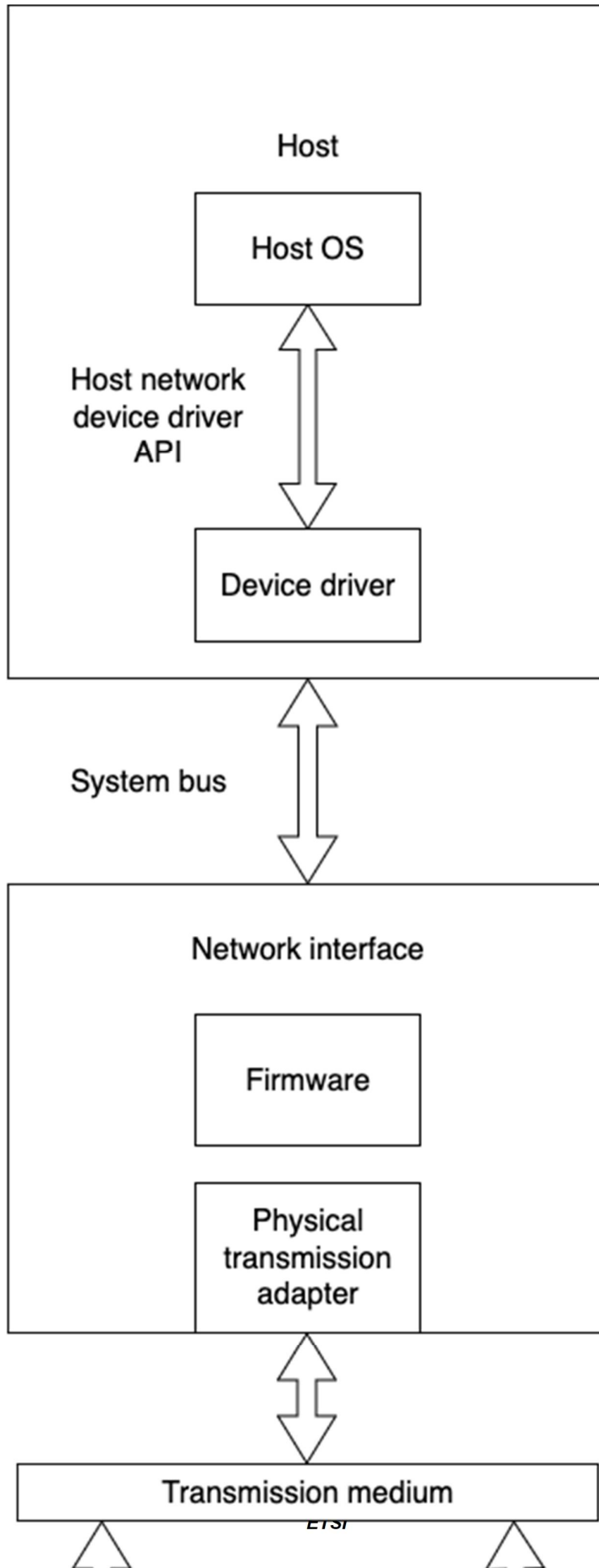
524 Physical network interfaces may also include the following parts:

- 525 • Device driver
- 526 • Removable/changeable antenna
- 527 • Daughter boards/add-on hardware modules

528 A virtual network interface consists of a device driver only.

529 4.3.2 Types of network interface

530 A network interface connects via a communications bus to the host. The host transmits to and receives data from the
531 network by means of a device driver interface provided by the device driver for the network interface. A network
532 interface might read and write the host memory directly and raise interrupts. It sometimes has more advanced features
533 that allow it to power cycle the entire system, download files using simple protocols, and act as a simple boot loader.



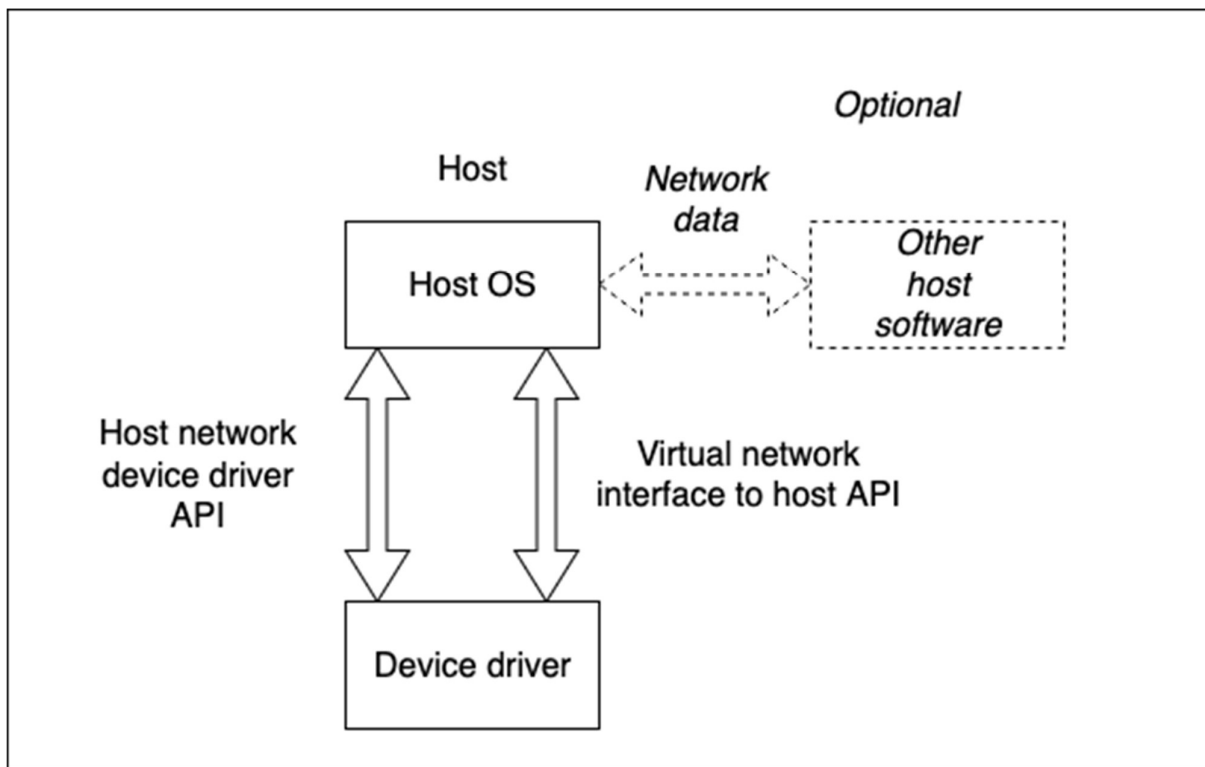
535

Figure 4.3.2-1: Physical network device architecture

536 A wired network interface transmits data via a specific physical medium such as Ethernet cable, fibre optic cable,
 537 coaxial cable or power lines. A wireless network interface transmits data in a manner that does not require a specific
 538 medium, such as radiofrequency waves or visible light communication through the air. A virtual network interface
 539 transmits data through software within the memory of a host system, sometimes across a software-defined network
 540 fabric.

541 Wireless network interfaces often have an independent real-time operating system on the network interface itself.
 542 Wireless medium access often requires real-time response to manage the radio frequency transmissions properly. The
 543 network interface may also need to prevent improper settings of radio frequency transmission parameters, which is
 544 often implemented by having the internal firmware set the parameters, rather than exposing them to the host. The
 545 complexity of this firmware may increase the risk of a wireless interface.

546 A virtual network interface emulates the device driver interface of a network interface to a host's device driver API.
 547 Instead of a physical network interface, it may send and receive packets to a hypervisor, a container, another device
 548 driver, another part of the network stack, an application, or other software.



549

550

Figure 4.3.2-2: Virtual network device architecture

551 4.3.3 Device drivers for network interfaces

552 The device driver communicates with the host software or firmware by means of a network device driver API. This API
 553 abstracts the implementation details of the underlying network interface. Such network device driver API is typically

554 defined by the host operating system or other software and is used by the host network stack to send or receive data
555 through the network interface.

556 Physical network interfaces require device drivers to make use of the physical hardware through a device driver
557 interface. Virtual network interfaces are effectively device drivers only, since they are made of software only without
558 underlying hardware.

559 The device driver often needs elevated privileges to read and write memory. Device drivers for physical network
560 interfaces often must have access also to the network interface control registers, directly or via host memory address
561 space mapped to them; sometimes device drivers must as well enable or disable interrupts or other host hardware
562 functions. This usually requires that the device driver has a high level of privilege on the host system.

563 4.4 Operational Environment

564 A network interface operates in the context of a host system and a network which may include other products. If the
565 device driver is not included with the product, it will be provided by the operating system or other part of the system.

566 4.5 Distribution of security functions

567 4.5.1 General

568 For each cybersecurity requirement, a product may:

- 569 1. Provide all necessary security functions itself
- 570 2. Require security functions be provided by some other part of its context
- 571 3. Provide security functions for the use of other components

572 For example, most individual hardware components do not have a built-in method of securely updating any firmware in
573 the product. Usually this requires a full-featured system running an operating system which can check for firmware
574 updates, download and verify them, and carry out the process of updating the firmware.

575 4.5.2 Security functions provided outside the product

576 The following security functionalities are frequently handled by the operating system or other external component:

- 577 • Secure by default configuration
- 578 • Secure configuration changes
- 579 • Secure update of firmware and/or device driver
- 580 • Authentication of users
- 581 • Authorization of users
- 582 • Deletion and transfer of user data
- 583 • Provision of cryptographic keys to network interface

584 4.5.3 Security functions provided to other components

585 The network interface provides the following security functions to other parts of the system:

- 586 • Reporting of network-related statistics

587 Optional features the product may implement, with hardware offloading or features built into the driver. Availability
588 and implementation style is often tied to the protocol. These features can be, but are not limited to:

- 589 • Integrity protection via data link layer error detection and correction
- 590 • Confidential communication channel when providing encryption at the data link layer (WPA2, MACSEC)

- 591 • Availability protection via packet processing offload features

592 4.6 Users

593 While users of almost every product with digital elements are also indirectly using a network interface, the users for the
594 purpose of the present document are restricted to those removing, installing, administering, or otherwise directly
595 interacting with the network interface as an individual product.

596 Users of network interfaces include:

- 597 • System integrators
- 598 • Internet equipment manufacturers
- 599 • Home computer users
- 600 • Mobile phone users
- 601 • Home IoT users
- 602 • Professional IT administrators
- 603 • Professional OT administrators
- 604 • Computer hobbyists

605 4.7 Use cases

606 The following use cases are provided to assist manufacturers in selecting risk factors and security levels. This is not
607 intended to be an exhaustive or complete list of all possible use cases.

608 The examples given in each use case are for a finished product that includes the network interface. They are examples
609 of a products which at least one of the core functionalities is to operate as a network interface.

610 4.7.1 Wired network interface use cases

- 611 • UC-WD-1 Wired stationary home IoT device
 - 612 ○ E.g. thermostat, fridge
 - 613 ○ Behind home gateway firewall
 - 614 ○ Host access limited to people within the home
 - 615 ○ Simple, low-feature network interface implementation
 - 616 ○ Non-professional administration
- 617 • UC-WD-2 Wired professional device in isolated internal infrastructure
 - 618 ○ E.g. Data centre for internal job processing, smart meter in an isolated private network
 - 619 ○ Behind a firewall/gateway, no direct route to internet
 - 620 ○ Users are administrators and approved (predefined, fixed) applications
 - 621 ○ Network interface implements performance optimizations
 - 622 ○ Professional administration
- 623 • UC-WD-3 Wired professional internal infrastructure device
 - 624 ○ E.g. switches behind edge firewall devices
 - 625 ○ Behind a firewall, routing filtered internet traffic

- 626
 - Users are administrators
- 627
 - Network interface implements performance optimizations
- 628
 - Professional administration
- 629
 - UC-WD-4 Wired professional edge device or internet infrastructure
- 630
 - E.g. firewalls, VPN servers, switches in IXPs and ISPs, smart meter gateways and data concentrators
- 631
 - in a smart metering system
- 632
 - Exposed to entire internet on the public network side
- 633
 - Users are administrators and approved applications
- 634
 - Network interface implements performance optimizations
- 635
 - Professional administration
- 636
 - UC-WD-5 Wired stationary home gateway
- 637
 - E.g. ISP-managed access point
- 638
 - Exposed to the entire internet, with potentially some ISP filtering
- 639
 - Host access limited to trusted users/systems
- 640
 - Network interface implements performance optimizations
- 641
 - Mix of professional and non-professional administration
- 642
 - UC-WD-6 Wired professional worker device on internal network
- 643
 - E.g. stationary personal computer, registration terminal, cash register
- 644
 - Behind a corporate firewall
- 645
 - Users are company employees
- 646
 - Network interface implements performance optimizations
- 647
 - Professional administration
- 648
 - UC-WD-7 Wired stationary home device
- 649
 - E.g. stationary personal computer, IoT hub, thermostat, TV
- 650
 - Behind home gateway firewall
- 651
 - Host access limited to people within the home
- 652
 - Network interface implements performance optimizations
- 653
 - Non-professional administration
- 654
 - UC-WD-8 Wired mobile device
- 655
 - E.g. laptop
- 656
 - Exposed to entire internet, physically nearby attackers
- 657
 - Users limited to owner and a limited number of people they trust
- 658
 - Network interface implements performance optimizations
- 659
 - Non-professional administration
- 660
 - UC-WD-9 Wired stationary public server

- 661 ○ E.g. shared webhosting
- 662 ○ Behind some firewall
- 663 ○ Can be used by anyone who can open an account
- 664 ○ Network interface implements performance optimizations
- 665 ○ Professional administration
- 666 ● UC-WD-10 Wired stationary device for public use
 - 667 ○ E.g. public library computer, vending machine
 - 668 ○ Behind some firewall, network accessible by physically nearby attackers
 - 669 ○ Can be used by anybody
 - 670 ○ Network interface implements performance optimizations
 - 671 ○ Professionally administered but likely under-resourced

672 4.7.2 Wireless network interface use cases

- 673 ● UC-WL-1 Wireless professional device in isolated internal infrastructure
 - 674 ○ E.g. Data centre for internal job processing, smart meter in an isolated private network
 - 675 ○ Behind a firewall/gateway, no direct route to internet
 - 676 ○ Users are administrators and approved (predefined, fixed) applications
 - 677 ○ Interface implements radio control and encryption
 - 678 ○ Professional administration
- 679 ● UC-WL-2 Wireless stationary home IoT device
 - 680 ○ E.g. IoT lightbulb, smart oven, stationary personal computer
 - 681 ○ Behind home gateway firewall, network accessible by physically nearby attackers
 - 682 ○ Host access limited to people within the home
 - 683 ○ Interface implements radio control and encryption
 - 684 ○ Non-professional administration
- 685 ● UC-WL-3 Wireless professional edge device or internet infrastructure
 - 686 ○ E.g. firewalls, VPN servers, switches in IXPs and ISPs, smart meter gateways and data concentrators
 - 687 in a smart metering system
 - 688 ○ Exposed to entire internet on the public network side
 - 689 ○ Users are administrators and approved applications
 - 690 ○ Interface implements radio control and encryption
 - 691 ○ Professional administration
- 692 ● UC-WL-4 Wireless mobile enterprise worker device
 - 693 ○ E.g. company laptop, phone, tablet
 - 694 ○ Exposed to entire internet via any access point
 - 695 ○ Users are company employees

- 696 ○ Interface implements radio control and encryption
- 697 ○ Professional administration
- 698 • UC-WL-5 Wireless stationary home computer
- 699 ○ E.g. stationary personal computer
- 700 ○ Behind home gateway firewall, network accessible by physically nearby attackers
- 701 ○ Host access limited to people within the home
- 702 ○ Interface implements radio control and encryption
- 703 ○ Non-professional administration
- 704 • UC-WL-6 Wireless mobile personal device
- 705 ○ E.g. laptop, phone, tablet, watch
- 706 ○ Exposed to entire internet, physically nearby attackers
- 707 ○ Users limited to owner and a few people they trust
- 708 ○ Interface implements radio control and encryption
- 709 ○ Non-professional administration
- 710 • UC-WL-7 Wireless stationary device for public use
- 711 ○ E.g. public library computer, vending machine
- 712 ○ Behind some firewall, network accessible by physically nearby attackers
- 713 ○ Can be used by literally anybody
- 714 ○ Interface implements radio control and encryption
- 715 ○ Professional administration but likely under-resourced

716 4.7.3 Virtual network interface use cases

- 717 • UC-VI-1 Virtual network interface for internal use on private or professional device
- 718 ○ E.g. loopback, containers, tunnel to local application
- 719 ○ Packets only from other applications/users on host
- 720 ○ Users limited to owner and who they trust
- 721 ○ Very simple device driver
- 722 ○ Professional administration
- 723 • UC-VI-2 Virtual network interface for external use on private device
- 724 ○ Virtio on hypervisors, VPN interfaces, tunnel interfaces
- 725 ○ Exposed to entire internet
- 726 ○ Users limited to owner and who they trust
- 727 ○ Highly complex packet filtering, processing, encryption, etc.
- 728 ○ Non-professional administration
- 729 • UC-VI-3 Virtual network interface for external use on enterprise device

- 730 ○ Virtio on hypervisors, VPN interfaces, tunnel interfaces
- 731 ○ Exposed to entire internet
- 732 ○ Users are company employees
- 733 ○ Highly complex packet filtering, processing, encryption, etc.
- 734 ○ Professional administration
- 735 ● UC-VI-4 Virtual network interface for external use on public server
 - 736 ○ Virtio on hypervisors, VPN interfaces, tunnel interfaces
 - 737 ○ Exposed to entire internet
 - 738 ○ Users are untrusted
 - 739 ○ Highly complex packet filtering, processing, encryption, etc.
 - 740 ○ Professional administration

741 5 Cybersecurity requirement specifications

742 5.1 Notes on the structure of cybersecurity requirements

743 A Cybersecurity requirement is a security or other functional element that a product must have to comply with this
 744 standard. An ideal cybersecurity requirement is technical, meaning it is objectively testable on an instance of the
 745 product. If a cybersecurity requirement cannot be tested on the product itself, it is a cybersecurity documentation
 746 requirement, where the manufacturer documents the steps they have taken to implement it. Any documentation required
 747 to meet the cybersecurity requirements of this standard must be detailed (including materials such as configuration files
 748 or written policies used by employees), and will ideally be sufficient to replicate the manufacturer's tests. Limited
 749 documentation, such as that indicating only that a test was completed, do not meet the cybersecurity requirements of
 750 this standard.

751 Mitigations are how a technical cybersecurity requirement can be satisfied. Mitigations provided in this standard are
 752 tailored to the use case and take into account the user's sophistication and the operational environment.

753 While risks may not be transferred to the user, some risks may be treated partially or fully by other, connected elements
 754 of the system. When that is the case, mitigations that allow a risk to be treated externally are included as an option to
 755 fulfill a technical cybersecurity requirement, depending on the use case and risk factors.

756 **IMPORTANT:** Not all cybersecurity requirements are necessary for all products. The mapping tables at the end of
 757 each cybersecurity requirement shows which risk factors and use cases determine which cybersecurity requirements are
 758 necessary for the product.

759 **See Annex C for more information.**

760 5.2 Technical cybersecurity requirements specifications

761 5.2.1 General

762 This clause is a list of technical cybersecurity requirements necessary to satisfy the CRA essential requirements. Each
 763 technical cybersecurity requirement can be satisfied by one or more potential mitigations. Each mitigation may or may
 764 not be appropriate for an individual use case. The following clause will define which mitigations will be required,
 765 depending on risk factors and/or a use case.

766 **See Annex C for more information.**

767 5.2.1 ER-NKEV: No known exploitable vulnerabilities at first use

768 5.2.1.1 Cybersecurity requirement

769 Recognizing that there may be vulnerabilities discovered between the time that a product is placed on the market and
770 the time of that product's first use, and that the product should be free from known vulnerabilities both when first made
771 available and when first used by a consumer, the product shall be able to be updated at the time of first use to address all
772 known exploited vulnerabilities which were discovered after the product's placement on the market and before that first
773 use.

774 5.2.1.2 MI-KEVD: Documentation for secure update before or during first use

775 The product shall be accompanied by documentation describing how the product may be securely updated, including
776 how to update the product prior to, or as part of, first use.

- 777 • Applicability: Product expected use is long enough to require updates and the product has firmware update
778 capability
- 779 • Reference: ER-NKEV
- 780 • Objective: Prevent exploitation of known exploited vulnerabilities at first use
- 781 • Preparation: Examine public or private vulnerability information sources and select a representative sample of
782 recently fixed vulnerabilities for the product and for its dependencies
- 783 • Activities: On a new product, carry out the initial secure update, scan the product to see if a recently fixed
784 vulnerabilities has been fixed on the product, and examine the documentation for the required info
- 785 • Verdict: The secure update completes successfully, the sample set of vulnerabilities is fixed, and the
786 documentation includes all the required information => PASS, otherwise FAIL
- 787 • Evidence: Documentation of vulnerability handling, documentation of how to securely update the product, the
788 report for the selected vulnerabilities, description of how to scan for the vulnerabilities, log of vulnerability
789 scan results

790 5.2.1.3 MI-KEVA: Automatic secure update before or during first use

791 The product shall implement automatic secure update by default before or during first use.

- 792 • Applicability: Product expected use is long enough to require updates and the product has firmware update
793 capability
- 794 • Reference: ER-NKEV
- 795 • Objective: Prevent exploitation of known exploited vulnerabilities at first use
- 796 • Preparation: Examine public or private vulnerability information sources and select a representative sample of
797 recently fixed vulnerabilities for the product and for its dependencies
- 798 • Activities: Follow the instructions to install and use the product for the first time, scan the product to see if a
799 recently fixed vulnerabilities has been fixed on the product, and examine the documentation for the required
800 info
- 801 • Verdict: The secure update completes successfully, the sample set of vulnerabilities is fixed, and the
802 documentation includes all the required information => PASS, otherwise FAIL
- 803 • Evidence: Documentation of vulnerability handling, documentation of how to securely update the product, the
804 report for the selected vulnerabilities, description of how to scan for the vulnerabilities, log of vulnerability
805 scan results

806 5.2.1.4 MI-KEVM: Documentation of mitigation of known exploitable vulnerabilities

807 The product's development and release process shall include a process to document known exploitable vulnerabilities in
808 the product and their fixes or mitigations. The documentation for this process shall be compliant with the process
809 described in prEN 40000-1-3 [3]. The product shall be compliant with this cybersecurity requirement if it:

- 810 1. has no known exploitable vulnerabilities
- 811 2. has known exploitable vulnerabilities whose age is consistent with the specification of how long vulnerabilities
812 may go unfixed after public disclosure, as described in the vulnerability handling procedure for the product
- 813 3. for each detected vulnerability, has documentation of how the risk has been mitigated
 - 814 • Reference: ER-NKEV
 - 815 • Objective: Prevent exploitation of known exploited vulnerabilities at first use
 - 816 • Preparation: Compile a list of known exploitable vulnerabilities in the product and its components
 - 817 • Activities: Compare the generated list of known exploitable vulnerabilities with the documentation of the
818 known exploitable vulnerabilities that have been fixed or mitigated in the product
 - 819 • Verdict: No vulnerabilities found, or all reported vulnerabilities satisfy either the age or documentation
820 cybersecurity requirement => PASS, otherwise FAIL
 - 821 • Evidence: Documented vulnerability handling policy, list of vulnerabilities, documentation of mitigations or
822 age of vulnerability, correlation of list of vulnerabilities with documentation of mitigations or age of
823 vulnerability

824 5.2.1.5 MI-KEVT: Testing for known exploitable vulnerabilities

825 The product shall be tested for all known exploitable vulnerabilities to demonstrate that each has been mitigated. The
826 product shall be compliant with this cybersecurity requirement if it:

- 827 1. has no known exploitable vulnerabilities
- 828 2. has known exploitable vulnerabilities whose age is consistent with the specification of how long vulnerabilities
829 may go unfixed after public disclosure, as described in the vulnerability handling procedure for the product
- 830 3. for each tested vulnerability, the test result shows that the vulnerability has been mitigated
 - 831 • Reference: ER-NKEV
 - 832 • Objective: Prevent exploitation of known exploited vulnerabilities at first use
 - 833 • Preparation: Compile a list of known exploitable vulnerabilities in the product and its components, compile a
834 list of known exploitable vulnerabilities that will be tested, collect tests for each one
 - 835 • Activities: On a new product, carry out a secure update, run the tests, and compare the results with the
836 generated list of known exploitable vulnerabilities
 - 837 • Verdict: No vulnerabilities found, or all reported vulnerabilities satisfy either the age or mitigation
838 cybersecurity requirement => PASS, otherwise FAIL
 - 839 • Evidence: Documented vulnerability handling policy, list of vulnerabilities, test results for each vulnerability
840 or documentation of age of vulnerability, correlation of list of vulnerabilities with test results or documentation
841 of age of vulnerability

842 5.2.1.6 MI-SCAN: No easily scannable known exploitable vulnerabilities

843 If automatable and freely-usable vulnerability scanners are available for the product, then the product shall satisfy the
844 following with respect to the three (or fewer, if fewer than three are available) most comprehensive of such scanners:

- 845 1. has no vulnerabilities discovered by scans

- 846 2. has discoverable exploitable vulnerabilities whose age is consistent with the specification of how long
 847 vulnerabilities may go unfixed after public disclosure, as described in the vulnerability handling procedure for
 848 the product
- 849 3. for each detected vulnerability, has publicly available documentation explaining how the risk has been
 850 mitigated
- 851 • Reference: ER-NKEV
 - 852 • Objective: Prevent exploitation of known vulnerabilities at first use
 - 853 • Preparation: Select a set of tools meeting the cybersecurity requirements
 - 854 • Activities: On a new product, carry out a secure update, run the tools on the product, and examine the
 855 documentation for any reported vulnerabilities
 - 856 • Verdict: No vulnerabilities found, or all reported vulnerabilities satisfy either the age or documentation
 857 cybersecurity requirement => PASS, otherwise FAIL
 - 858 • Evidence: Documented vulnerability handling policy, list of vulnerability scanners selected, reports from each
 859 scanner, correlation of reports of discovered vulnerabilities with documentation of mitigations

860 5.2.1.7 Mapping of mitigations to risk factors and security profiles

861 See clause 5.3 for which mitigations are necessary for which security profiles and clause C.4 for the rationale.

862 5.2.2 ER-SSDD: Secure design and development

863 5.2.2.1 Cybersecurity requirement

864 The product shall be designed and developed in a secure manner as defined in CRA Essential Requirement 1 in Annex
 865 I. This section defines what additional measures needs to be taken which are not fit under other essential requirements.

866 5.2.2.2 MI-SSCA: Static source code analysis for memory errors

867 All security-relevant parts of the product shall be checked for memory errors using a source code analysis tool that
 868 detects code that may produce common memory errors, such as:

- 869 • buffer overflow
- 870 • out-of-bounds
- 871 • use after free
- 872 • double free
- 873 • use of uninitialized variables
- 874 • dereference of invalid pointer

875 The sufficiency of the source code analysis tool and the selected manner of running it shall be documented.

876 All warnings, annotations, or other method of suppressing warnings from the analysis tool shall be documented with a
 877 rationale for why it does not constitute an unacceptable risk.

- 878 • Reference: ER-SSDD
- 879 • Objective: Prevent unauthorized memory access
- 880 • Preparation: None
- 881 • Activities: Review the documentation on why the source code analysis tool is sufficient, how it is run, the
 882 source code for the product, the output of the source code analysis tool, and the documentation for any
 883 warnings or suppression of warnings

884 • Verdict: Sufficiency documentation is acceptable, the method of running the tool is consistent with rationale,
 885 the output of source code analysis tool is consistent with the source code, all warnings or suppression of
 886 warnings have convincing documentation for why they are an acceptable risk => PASS, otherwise FAIL

887 • Evidence: The documentation on why the source code analysis tool is sufficient, how it is run, the source code
 888 for the product, the output of the source code analysis tool, and the documentation for any warnings or
 889 suppression of warnings

890 5.2.2.3 MI-FZ95 Runtime code coverage checking with memory access error 891 detection

892 The product shall be checked for memory errors by running a tool that exercises the functions of the product in an
 893 environment that permits measuring code coverage and detecting memory access errors. All memory errors detected
 894 shall be documented with a rationale for why it does not constitute an unacceptable risk.

895 • Reference: ER-SSDD

896 • Objective: Prevent unauthorized memory access

897 • Preparation: None

898 • Activities: Run the tool while measuring code coverage and monitoring for memory access errors until 95%
 899 code coverage has been reached

900 • Verdict: Code coverage was at least 95%, all reported memory errors are documented and justified => PASS,
 901 otherwise FAIL

902 • Evidence: Logs of code coverage tool, memory error report, documentation of any memory errors

903 5.2.2.4 MI-IMSL Implement in a memory-safe language

904 The product's firmware and/or software shall be implemented in a memory-safe language. Any use of unsafe memory
 905 features shall be documented to explain why they are necessary and do not present a security risk.

906 • Reference: ER-SSDD, ER-MSAF

907 • Objective: Prevent unauthorized memory access

908 • Preparation: None

909 • Activities: Review source code to determine its language and what exceptions to memory safety exist

910 • Verdict: Source code is in a memory-safe language and the documentation of all uses of unsafe memory
 911 features convincingly demonstrates that each one of them does not present a security risk => PASS, otherwise
 912 FAIL

913 • Evidence: Source code, documentation of unsafe memory features

914 5.2.2.5 MI-BTIN Boundary testing of inputs that may cause memory errors

915 The input fields of the product that may produce memory errors in the firmware or device driver shall be identified. The
 916 product shall be boundary tested for all such inputs while monitoring for memory errors. All memory errors detected
 917 shall be documented with a rationale for why it does not constitute an unacceptable risk.

918 • Reference: ER-SSDD, ER-MSAF

919 • Objective: Prevent unauthorized memory access

920 • Preparation: Identify input fields in the product that may produce memory errors

921 • Activities: Run a tool that tests the boundaries of the input values (minimum valid, maximum valid, minimum
 922 possible, maximum possible, off-by-one, etc.) while monitoring for memory errors

923 • Verdict: All boundary values tested and all memory errors detected are documented and justified => PASS,
 924 otherwise FAIL

- 925 • Evidence: Logs of boundary testing tool, memory error report, documentation of any memory errors

926 5.2.2.6 MI-SCFS: Secure compilation flags

927 All security-relevant firmware and software shall be compiled with secure compilation flags and options appropriate to
928 the target platform and language. All compilation flags used shall be documented as to their rationale, along with any
929 exceptions or limitations. Any exceptions to the flags or warnings shall be documented as to why they do not create an
930 unacceptable risk.

- 931 • Applicability: Product implemented in a compiled language
- 932 • Reference: ER-SSDD
- 933 • Objective: Secure design and development
- 934 • Preparation: Document which flags should be used
- 935 • Activities: Review compilation flags, warnings, and documentation for exceptions
- 936 • Verdict: Documentation of flags exists, all warnings and exceptions are documented => PASS, otherwise
937 FAIL
- 938 • Evidence: Documentation of flags, build system files, documentation of warnings and exceptions

939 5.2.2.7 Mapping of mitigations to risk factors and security profiles

940 See clause 5.3 for which mitigations are necessary for which security profiles and clause C.4 for the rationale.

941 5.2.2.8 MI-MSAF-1: Stack exhaustion detection

942 The product shall reject writes beyond the end of the stack.

- 943 • Reference: ER-SSDD
- 944 • Objective: Prevent thread from writing beyond end of stack
- 945 • Activities: Write beyond the end of the stack
- 946 • Verdict: each involved thread fails to read or write the target data and takes a segmentation fault, has error
947 handling code executed, or is terminated in all tests => PASS, otherwise FAIL
- 948 • Evidence: error messages, log message, or the product reboots or halts

949 Guidance: Two methods of exhausting stack memory include allocating a very large object on the stack, and performing
950 an unbounded recursive function call.

951 5.2.2.9 MI-MSAF-2: Stack linear buffer overflow detection

952 The product shall reject stack buffer writes that go beyond the end of the stack frame.

- 953 • Reference: ER-SSDD
- 954 • Objective: Prevent thread from writing beyond end of stack
- 955 • Activities: Write beyond the end of the stack frame
- 956 • Verdict: each involved thread fails to read or write the target data and takes a segmentation fault, has error
957 handling code executed, or is terminated in all tests => PASS, otherwise FAIL
- 958 • Evidence: error messages, log message, or the product reboots or halts

959 5.2.2.10 MI-MSAF-3: Array bounds checking

960 The product shall reject writes to fixed-size arrays that are beyond the end of the array.

- 961 • Reference: ER-SSDD

- 962 • Objective: Prevent thread from writing beyond the end of a fixed-size array
- 963 • Activities: Write beyond the end of a fixed-size array
- 964 • Verdict: each involved thread fails to read or write the target data and takes a segmentation fault, has error
965 handling code executed, or is terminated in all tests => PASS, otherwise FAIL
- 966 • Evidence: error messages, log message, or the product reboots or halts

967 5.2.2.11 MI-MZRO-1: Stack memory initializing

968 The product shall initialize all stack memory before use.

- 969 • Reference: ER-SSDD
- 970 • Objective: Prevent attacker from exploiting erroneous use of uninitialized stack memory
- 971 • Preparation: Define initialization value to be zero or one
- 972 • Activities: Sequentially call 2 functions that allocate the same amount of memory, fill the first with
973 non-initialization values and return, and during second function call, read the stack contents back
- 974 • Verdict: Stack contents are all set to initialization value on second call => PASS, otherwise FAIL
- 975 • Evidence: Contents of stack before the first function return, contents of stack during the second function call

976 5.2.2.12 MI-MZRO-2: Heap memory initializing

977 The product shall initialize all heap memory before use.

- 978 • Reference: ER-SSDD
- 979 • Objective: Prevent attacker from exploiting erroneous use of uninitialized heap memory
- 980 • Preparation: Define initialization value to be zero or one
- 981 • Activities: Allocate heap memory, fill with a non-initialization value, free it, allocate it again in a deterministic
982 way to get the same heap region, and read back the contents
- 983 • Verdict: Memory contents are all initialization value on second call => PASS, otherwise FAIL
- 984 • Evidence: Contents of allocated memory before the free, contents of allocated memory after second allocation

985 5.2.3 ER-LMII: Limit incident impact

986 5.2.3.1 Cybersecurity requirement

987 The product shall implement appropriate mitigations to limit incident impact.

988 This subsection is empty after HAS comment changes.

989 5.2.4 ER-MINI: Minimize impact on other devices and services

990 5.2.4.1 Cybersecurity requirement

991 The product shall implement appropriate mitigations to minimize impact on other devices and services.

992 5.2.4.2 MI-MDOC: Document transfer of risk of minimizing impact to operating 993 environment

994 The product shall be accompanied by documentation informing the user of the transfer of risk for minimizing impact on
995 other devices and services.

- 996 • Reference: ER-MINI

- 997 • Objective: Minimize impact on other devices and services
- 998 • Activities: Examine the documentation
- 999 • Verdict: Transfer of risk documented in a manner appropriate to the user => PASS, otherwise FAIL
- 1000 • Evidence: Documentation, analysis of documentation
- 1001 **5.2.4.3 MI-MPHY: Prevent denial of service at physical layer**
- 1002 The product shall implement methods of detecting and mitigating denial of service attacks on other devices resulting
1003 from exploitation of vulnerabilities on the product via network or host system access.
- 1004 • Reference: ER-MINI
- 1005 • Objective: Minimize impact on other devices and services
- 1006 • Preparation: List known attack methods that generate output on the transmission medium originating in the
1007 product itself that negatively impact other devices and services
- 1008 • Activities: Use a tool to simulate these attacks and observe whether the product notifies the host or mitigates
1009 the negative impact itself
- 1010 • Verdict: Product notifies host or mitigates the negative impact itself => PASS, otherwise FAIL
- 1011 • Evidence: List of attack methods, list of negative behaviours tested, log messages of product behaviour, log on
1012 host system
- 1013 **5.2.4.4 Mapping of mitigations to risk factors and security profiles**
- 1014 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.
- 1015 **5.2.5 ER-SDEF: Secure by default configuration**
- 1016 **5.2.5.1 Cybersecurity requirement**
- 1017 The product shall operate in a secure configuration by default.
- 1018 **5.2.5.2 MI-ADEF: Authorization required by default to access security-relevant
1019 assets**
- 1020 TODO: This is a blanket mitigation that is too vague and high-level. Public
1021 comment or delegate activity is needed to contribute more detailed and specific
1022 mitigations.
- 1023 The product shall require appropriate authorization by default to access security-relevant assets, such as product
1024 firmware, security-relevant configuration, sensitive data, and sensitive functions.
- 1025 Guidance: Appropriate authorization depends on the use case and the asset. For example, if the product's intended
1026 purpose is for integration into another product, then authorization is generally not necessary to access assets since the
1027 integrator will implement appropriate authorization. Another example would be encryption keys; these should not be
1028 readable without authorization such as password-based or pre-shared credentials/secrets from either the host or the
1029 network.
- 1030 • Reference: ER-SDEF
- 1031 • Objective: Find any unauthorized access to security relevant assets in default configuration
- 1032 • Preparation: List all interfaces allowing access to security-relevant assets
- 1033 • Activities: For each interface, attempt to access security-relevant assets without appropriate authorization and
1034 record whether access was allowed or not
- 1035 • Verdict: If every interface does not allow access without appropriate authorization => PASS, otherwise =>
1036 FAIL

- 1037 • Evidence: List of interfaces allowing access to security-relevant assets, record of activities used to attempt
1038 unauthorized access to security-relevant assets, log of results of attempts

1039 5.2.5.3 MI-DPAH: Documentation of product assets accessible from host

1040 The product shall be accompanied by documentation for all interfaces for the product that can be accessed by the host,
1041 describing what product assets are accessible from the interface and what type of access is appropriate for representative
1042 use cases or risk profiles.

1043 Guidance: This cybersecurity requirement gives the user or integrator of the product the necessary information they
1044 need to implement an appropriate level of access control in the host system. This cybersecurity requirement does not
1045 specify how the host implements access control.

- 1046 • Applicability: Physical network interface
- 1047 • Reference: ER-SDEF
- 1048 • Objective: Secure by default
- 1049 • Preparation: Define a method that can be used to find all interfaces on the product accessible from the host
- 1050 • Activities: For each interface, review the documentation to see if it is listed and provides the necessary
1051 information
- 1052 • Verdict: If every interface discovered is listed in the documentation and has the required information => PASS,
1053 otherwise => FAIL
- 1054 • Evidence: Method to list all interfaces accessible from the host, list of interfaces discovered, documentation of
1055 assets

1056 5.2.5.4 MI-PDDI-1: Document how to protect access to debug/management 1057 interfaces

1058 All debug/management interfaces on the product shall be documented as to how to protect or disable them.

1059 Guidance: This is for the use case of selling to an integrator.

- 1060 • Applicability: Physical network interface
- 1061 • Reference: ER-SDEF
- 1062 • Objective: Secure by default
- 1063 • Preparation: Examine the documentation for how to protect or disable the debug/management interfaces of the
1064 product
- 1065 • Activities: Examine the product for undocumented debug/management interfaces, then follow the instructions
1066 in the documentation to disable or protect each documented interface, then attempt to access the interface
1067 without authorization
- 1068 • Verdict: All debug/management interfaces are documented as to how to disable or protect them, and no
1069 interfaces are accessible without authorization after following the documentation to protect or disable them =>
1070 PASS, otherwise => FAIL
- 1071 • Evidence: Pictures of the product, list of discovered interfaces, comparison with documentation, notes as to
1072 which are documented how to disable/protect, logs of protect/disable actions, logs of attempts to access
1073 interfaces after protected or disabled

1074 5.2.5.5 MI-PDDI-2: Protect or disable physical access to debug/management 1075 interfaces

1076 All debug/management interfaces accessible to someone with physical access to the product shall be protected or
1077 disabled by default, unless necessary for backward compatibility and use by an appropriately sophisticated user who has
1078 been sufficiently informed of the risk and how to mitigate it.

1079 Guidance: This is for the use case of an end user in use cases where physical access is possible for a threat actor.

1080 • Applicability: Physical network interface

1081 • Reference: ER-SDEF

1082 • Objective: Secure by default

1083 • Preparation: Examine the documentation to find the physically accessible debug/management interfaces of the
1084 product

1085 • Activities: Examine the product for undocumented physical management interfaces, then attempt to access the
1086 documented interfaces without authorization

1087 • Verdict: No undocumented interfaces are found, no documented interfaces can be used without authorization
1088 other than those documented as necessary and the instructions to the user are sufficient => PASS, otherwise =>
1089 FAIL

1090 • Evidence: List of interfaces, log of examinations, log of attempts to access

1091 5.2.5.6 MI-PDDI-3: Protect or disable local software access to debug/management 1092 interfaces

1093 All debug/management interfaces accessible via unprivileged users on the host system shall be protected or disabled by
1094 default, unless necessary for backward compatibility and use by an appropriately sophisticated user who has been
1095 sufficiently informed of the risk and how to mitigate it.

1096 Guidance: This is for the use case of an end user in use cases where local host system software access is possible for a
1097 threat actor.

1098 • Reference: ER-SDEF

1099 • Objective: Secure by default

1100 • Preparation: Examine the documentation of the network accessible interfaces of the product and follow the
1101 instructions to mitigate the risk of any necessary unprotected or enabled interfaces

1102 • Activities: Using a network scanner, scan the product for both documented and undocumented debug or
1103 remote management interfaces and determine whether they are enabled or protected

1104 • Verdict: No undocumented interfaces are found and no interfaces can be accessed without authorization other
1105 than those documented as necessary and the instructions to the user are sufficient => PASS, otherwise =>
1106 FAIL

1107 • Evidence: List of interfaces, log of attempts to access

1108 5.2.5.7 MI-PDDI-4: Protect or disable network access to debug/management 1109 interfaces

1110 All debug/management interfaces accessible via the network shall be protected or disabled by default, unless necessary
1111 for backward compatibility and use by an appropriately sophisticated user who has been sufficiently informed of the
1112 risk and how to mitigate it.

1113 Guidance: This is for the use case of an end user in use cases where network access is possible for a threat actor.

1114 • Reference: ER-SDEF

1115 • Objective: Secure by default

1116 • Preparation: Examine the documentation of the network accessible interfaces of the product and follow the
1117 instructions to mitigate the risk of any necessary unprotected or enabled interfaces

1118 • Activities: Using a network scanner, scan the product for both documented and undocumented debug or
1119 remote management interfaces and determine whether they are enabled or protected

1120 • Verdict: No undocumented interfaces are found and no interfaces can be accessed without authorization other
 1121 than those documented as necessary and the instructions to the user are sufficient => PASS, otherwise =>
 1122 FAIL

1123 • Evidence: List of interfaces, log of attempts to access

1124 5.2.5.8 Mapping of mitigations to risk factors and security profiles

1125 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.

1126 5.2.6 ER-SCUD: Secure updates

1127 5.2.6.1 Cybersecurity requirement

1128 The product shall be securely updatable by the user.

1129 TODO: Specification of how secure updates can be done securely is in progress.

1130 5.2.6.2 MI-SUDC: Documentation of secure update

1131 The product shall be accompanied by documentation of the secure update methods for any firmware or software in the
 1132 product.

1133 • Applicability: Product expected use is long enough to require updates

1134 • Reference: ER-SCUD

1135 • Objective: Prevent exploitation of known vulnerabilities

1136 • Activities: Assess the documentation for completeness

1137 • Verdict: Documentation describes secure update methods sufficiently for a third party to implement them =>
 1138 PASS, otherwise FAIL

1139 • Evidence: Documentation and analysis of completeness

1140 5.2.6.3 MI-SUVP: Secure update via product

1141 The product shall provide a method of securely updating any firmware or software in the product via the product itself.

1142 • Applicability: Product expected use is long enough to require updates

1143 • Reference: ER-SCUD

1144 • Objective: Prevent exploitation of known vulnerabilities

1145 • Preparation: Prepare an update for each part of the product that can be updated with a different version number
 1146 from the currently installed product version

1147 • Activities: Check the versions of all parts of the product that can be updated, install the new update, and check
 1148 the versions again

1149 • Verdict: The second versions read are that of the new product update => PASS, otherwise FAIL

1150 • Evidence: New update version numbers, and log of querying the product parts' versions, installing the update,
 1151 and querying the versions again

1152 5.2.6.4 MI-SUAP: Automatic secure update via product

1153 The product shall provide a method of automatically securely updating any firmware or software in the product via the
 1154 product itself with an option for the user to disable automatic updates.

1155 • Applicability: Product expected use is long enough to require updates

1156 • Reference: ER-SCUD

- 1157 • Objective: Prevent exploitation of known vulnerabilities
- 1158 • Preparation: Prepare an update for each part of the product that can be updated with a different version number
- 1159 from the currently installed product version
- 1160 • Activities: Check the versions of all parts of the product that can be updated, create the conditions that allow
- 1161 automatic secure update to occur, check the versions again, then repeat except disabling automatic updates
- 1162 • Verdict: For the first test, the second versions read are that of the new product update, and for the second test
- 1163 with automatic updates disabled, the second versions read are the same as the first versions read => PASS,
- 1164 otherwise FAIL
- 1165 • Evidence: New update version numbers, and log of querying the product parts' versions, installing the update,
- 1166 and querying the versions again

1167 5.2.6.5 MI-SUOE: Secure update provided by operational environment

1168 The technical documentation provided with the product shall document that the operational environment shall provide a
1169 method of securely updating the product.

- 1170 • Applicability: Product expected use is long enough to require updates
- 1171 • Reference: ER-SCUD
- 1172 • Objective: Prevent exploitation of known vulnerabilities
- 1173 • Activities: Assess the documentation provided with the product
- 1174 • Verdict: Documentation describes cybersecurity requirements for the secure updates provided by the
- 1175 operational environment => PASS, otherwise FAIL
- 1176 • Evidence: Documentation and analysis of completeness

1177 5.2.6.6 MI-SUAO: Automatic secure update provided by operational environment

1178 The technical documentation provided with the product shall document that the operational environment shall provide a
1179 method of automatically securely updating the product with an option for the user to disable automatic updates.

- 1180 • Applicability: Product expected use is long enough to require updates
- 1181 • Reference: ER-SCUD
- 1182 • Objective: Prevent exploitation of known vulnerabilities
- 1183 • Activities: Assess the documentation provided with the product
- 1184 • Verdict: Documentation describes cybersecurity requirements for automatic secure updates provided by the
- 1185 operational environment => PASS, otherwise FAIL
- 1186 • Evidence: Documentation and analysis of completeness

1187 5.2.6.7 Mapping of mitigations to risk factors and security profiles

1188 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.

1189 5.2.7 ER-AUTH: Authentication and access control

1190 TODO: Fill in very limited authentication cybersecurity requirements (for remote
1191 management or self-update) and reference cross-vertical authentication standards
1192 when they exist.

1193 5.2.7 ER-CDST: Confidentiality of data stored on the product

1194 5.2.7.1 Cybersecurity requirement

1195 The product shall protect data stored on the product from unauthorized access.

1196 5.2.7.2 MI-CDST: Protect confidentiality of data stored on the product

1197 TODO: This is a blanket mitigation that is too vague and high-level. Public
1198 comment or delegate activity is needed to contribute more detailed and specific
1199 mitigations.

1200 The product shall protect data stored on the product from unauthorized access.

1201 Guidance: This may include keys, firmware, configuration, packets, credentials, and data stored in volatile or
1202 non-volatile memory or storage.

1203 • Reference: ER-CDST

1204 • Objective: Confidentiality of data

1205 • Preparation: List all types of data that may be stored on the product that should not be readable without
1206 authorization, what methods of ensuring confidentiality are appropriate for each type, all methods of accessing
1207 that data available to an attacker based on the risk assessment, and what the allowable authorization methods
1208 are for that access method

1209 • Activities: For each type of data and each access mechanism, determine the method of ensuring confidentiality
1210 used, and attempt to read the data without authorization

1211 • Verdict: If all methods of ensuring confidentiality match the type of the data stored, and all the attempts to read
1212 confidential data without authorization fail => PASS, otherwise => FAIL

1213 • Evidence: Logs of determination of type of data and method of confidentiality and attempts to read
1214 confidential data without authorization

1215 Guidance: Data may be protected by the environment, permissions, encryption, salting and hashing, offline storage, or
1216 hardware-backed secrets.

1217 5.2.7.3 Mapping of mitigations to risk factors and security profiles

1218 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.

1219 5.2.8 ER-CDTX: Confidentiality of data transmitted by product

1220 5.2.8.1 Cybersecurity Requirement

1221 The product shall protect data transmitted by the product from unauthorized access.

1222 5.2.8.2 MI-CDTX: Protect confidentiality of data transmitted by product

1223 TODO: This is a blanket mitigation that is too vague and high-level. Public
1224 comment or delegate activity is needed to contribute more detailed and specific
1225 mitigations.

1226 The product shall protect data transmitted by the product from unauthorized access on the local network.

1227 Guidance: Protecting confidentiality of data transmitted across indirectly attached networks is not the responsibility of
1228 the network interface.

1229 • Reference: ER-CDTX

1230 • Objective: Confidentiality of data

1231 • Preparation: List all types of data that may be transmitted on the product that should not be readable without
1232 authorization, what methods of ensuring confidentiality are appropriate for each type, all methods of accessing

- 1233 that data available to an attacker based on the risk assessment, and what the allowable authorization methods
1234 are for that access method
- 1235 • Activities: For each type of data and each access mechanism, determine the method of ensuring confidentiality
1236 used, and attempt to read the data without authorization
 - 1237 • Verdict: If all methods of ensuring confidentiality match the type of the data transmitted, and all the attempts
1238 to read confidential data without authorization fail => PASS, otherwise => FAIL
 - 1239 • Evidence: Logs of determination of type of data and method of confidentiality and attempts to read
1240 confidential data without authorization

1241 Guidance: Data transmitted may be protected by the environment or encryption.

1242 5.2.8.3 MI-DOCC: Document transfer of risk of confidentiality of data transmitted by 1243 product

1244 The product shall be accompanied by documentation informing the user of the transfer of risk for protecting the
1245 confidentiality of data transmitted by the product.

- 1246 • Reference: ER-CDTX
- 1247 • Objective: Protect data confidentiality
- 1248 • Activities: Examine the documentation
- 1249 • Verdict: Transfer of risk documented in a manner appropriate to the user => PASS, otherwise FAIL
- 1250 • Evidence: Documentation, analysis of documentation

1251 5.2.8.4 Mapping of mitigations to risk factors and security profiles

1252 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.

1253 5.2.9 ER-CRYP: Encryption

1254 TODO: Fill in very limited encryption cybersecurity requirements that are not
1255 performance-related (this is probably remote management and self-update). Need to
1256 specify any necessary encryption algorithms that are not already included in the
1257 Agreed Cryptographic Mechanism and CRA Addendum.

1258 5.2.10 ER-IDST: Integrity of data stored on the product

1259 5.2.10.1 Cybersecurity requirement

1260 The product shall protect the integrity of data stored on the product from unauthorized modification and report
1261 corruption.

1262 Guidance: Integrity may be protected by the environment, permissions, duplication, backups, and/or checksums.

1263 5.2.10.2 MI-IDST: Protect integrity of data stored on the product

1264 TODO: This is a blanket mitigation that is too vague and high-level. Public
1265 comment or delegate activity is needed to contribute more detailed and specific
1266 mitigations.

1267 The product shall protect the integrity of data stored on the product from unauthorized modification.

- 1268 • Reference: ER-IDST
- 1269 • Objective: Integrity of data
- 1270 • Preparation: List all types of data that may be stored on the product that should not be modifiable without
1271 authorization, what methods of protecting integrity are appropriate for each type, all methods of modifying that

1272 data available to an attacker based on the risk assessment, and what the allowable authorization methods are
1273 for that modification method

1274 • Activities: For each type of data and each access mechanism, determine the method of protecting integrity
1275 used, and attempt to modify the data without authorization

1276 • Verdict: If all methods of ensuring integrity match the type of the data stored, and all the attempts to modify
1277 protected data without authorization fail => PASS, otherwise => FAIL

1278 • Evidence: Logs of determination of type of data and method of integrity and attempts to modify protected data
1279 without authorization

1280 5.2.10.3 MI-DCST: Detect corruption of data stored

1281 TODO: This is a blanket mitigation that is too vague and high-level. Public
1282 comment or delegate activity is needed to contribute more detailed and specific
1283 mitigations.

1284 The product shall detect corruption of the data stored on the product.

1285 • Reference: ER-IDST

1286 • Objective: Integrity of data

1287 • Preparation: List all types of data that may be stored on the product whose corruption should be detected and
1288 what methods of detecting corruption are appropriate for each type

1289 • Activities: For each type of data and method of detecting corruption, corrupt the data in a way that the method
1290 will detect

1291 • Verdict: If all methods of detecting corruption match the type of the data stored, and all the corruptions of data
1292 are detected => PASS, otherwise => FAIL

1293 • Evidence: Logs of determination of type of data and corruptions of data

1294 5.2.10.4 Mapping of mitigations to risk factors and security profiles

1295 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.

1296 5.2.11 ER-IDTX: Integrity of data transmitted by the product

1297 5.2.11.1 Cybersecurity requirement

1298 The product shall detect corruption of the data transmitted by the product.

1299 Guidance: Integrity may be protected by the environment, permissions, duplication, backups, and/or checksums.

1300 5.2.11.2 MI-DCTX: Detect corruption of data transmitted by the product

1301 TODO: This is a blanket mitigation that is too vague and high-level. Public
1302 comment or delegate activity is needed to contribute more detailed and specific
1303 mitigations.

1304 The product shall detect corruption of the data transmitted by the product.

1305 • Reference: ER-IDTX

1306 • Objective: Integrity of data

1307 • Preparation: List all types of data that may be transmitted by the product whose corruption should be detected
1308 and what methods of detecting corruption are appropriate for each type

1309 • Activities: For each type of data and method of detecting corruption, corrupt the data in a way that the method
1310 will detect

1311 • Verdict: If all methods of detecting corruption match the type of the data transmitted, and all the corruptions of
 1312 data are detected => PASS, otherwise => FAIL

1313 • Evidence: Logs of determination of type of data and corruptions of data

1314 5.2.11.3 Mapping of mitigations to risk factors and security profiles

1315 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.

1316 5.2.12 ER-DMIN: Data Minimization

1317 5.2.12.1 Cybersecurity requirement

1318 The product shall minimize the data processed.

1319 5.2.12.2 MI-DJST: Document and justify processed data

1320 The product operation can require storing information relevant for the protocol implementation like out-of-order TCP
 1321 packets, that are later recombined for the receiver as a continuous stream of information. This can be often considered to
 1322 be part of the core functionality of the product.

1323 Outside of the core functionality, the default set size of data that needs to be collected from the operation is zero.
 1324 Therefore:

1325 All sources of data processed by the product in its secure-by-default configuration shall be documented. All sources of
 1326 data processed shall have a documented rationale for why its processing is necessary for the functioning of the product
 1327 in its secure-by-default configuration.

1328 Example MI-DJST-1: The product supports NetFlow protocol and collects
 1329 information from traffic going through the interface.

1330 Example MI-DJST-2: The product is a managed interface and supports a variety of
 1331 different collectable metrics which are by default off, but the collection and
 1332 reporting can be activated remotely.

1333 Example MI-DJST-3: The product is purpose-built for high level application co-
 1334 operation and participates on the content delivery network function by storing most
 1335 frequent replies in the network interface volatile memory. The replies are served
 1336 directly from the memory without relying the request forward. Key information and
 1337 metrics are collected and relied for the application.

1338 • Reference: ER-DMIN

1339 • Objective: Minimize data processed

1340 • Preparation: List all potential sources of data for the product. For each source of data, identify a method to
 1341 detect whether the product is processing data from that source.

1342 • Activities: Using the list of sources of data, and the method to detect whether the product is processing data
 1343 from that source, list all sources of data processed. Compare to the documented list.

1344 • Verdict: All sources of processed data are documented, including rationale => PASS, otherwise => FAIL

1345 • Evidence: List of sources of data, documentation of each source of data, list of sources of data processed,
 1346 connection between each discovered source of processed data to its documentation

1347 5.2.12.3 Mapping of mitigations to risk factors and security profiles

1348 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.

1349 5.2.13 ER-AVAI: Availability

1350 5.2.13.1 Cybersecurity requirement

1351 The product shall protect the availability of essential and core functions.

1352 5.2.13.2 MI-WDOG: Watchdog and self-initiated reset

1353 The product shall implement a mechanism to trigger an automatic reset when it detects that it is no longer able to
1354 perform its functions.

- 1355 • Reference: ER-AVAI
- 1356 • Objective: Availability
- 1357 • Preparation: Document the conditions that indicate the product cannot perform its functions
- 1358 • Activities: Cause each of the conditions to occur and observe whether the product resets
- 1359 • Verdict: Every condition triggers an automatic reset => PASS, otherwise FAIL
- 1360 • Evidence: Documentation, log messages

1361 5.2.13.3 MI-NTFY: Watchdog and notification of host

1362 The product shall implement a mechanism to notify the host system when it detects that it is no longer able to perform
1363 its functions and a way for the host to reset the product.

- 1364 • Reference: ER-AVAI
- 1365 • Objective: Availability
- 1366 • Preparation: Document the conditions that indicate the product cannot perform its functions
- 1367 • Activities: Cause each of the conditions to occur and observe whether the product notifies the host system
- 1368 • Verdict: Every condition triggers a notification to the host => PASS, otherwise FAIL
- 1369 • Evidence: Documentation, log messages

1370 5.2.13.4 MI-FDRP: Fast packet drop

1371 The product shall check each incoming packet for validity - at minimum frame length, header fields, and destination
1372 address - in order from least to most computationally expensive, and shall drop invalid packets before further
1373 processing. The check sequence and its rationale shall be documented.

- 1374 • Reference: ER-AVAI
- 1375 • Objective: Availability

1376

1377 5.2.13.5 MI-LMEM: Limit memory usage

1378 The product shall enforce documented limits on internal resources consumed by received data (e.g. packet buffers,
1379 receive queues, descriptor rings). When a limit is reached, the product shall drop new incoming data without crashing or
1380 corrupting existing state.

- 1381 • Reference: ER-AVAI
- 1382 • Objective: Availability

1383

1384 5.2.13.6 MI-FAIR: Fair resource usage and prioritisation

1385 The product shall prevent any single source of input from monopolising processing resources and shall prioritise at least
1386 one class of input (e.g. host commands, management traffic) over others under contention. The prioritisation mechanism
1387 and its default configuration shall be documented.

- 1388 • Reference: ER-AVAI

- 1389 • Objective: Availability

1390

1391 5.2.13.7 MI-DOST: Document risk transfer to operational environment for 1392 denial of service

1393 The product shall be accompanied by documentation describing what denial-of-service protections the product provides
1394 and what protections the operational environment shall provide.

- 1395 • Reference: ER-AVAI

- 1396 • Objective: Availability

1397 5.2.14 ER-LMAS: Minimize exposed interfaces

1398 5.2.14.1 Cybersecurity requirement

1399 The product's exposed interfaces shall be minimized in the default configuration of the product in all operating modes,
1400 including initial configuration, during initialization, while in use, while shutting down or paused, or after reset.

1401 5.2.14.2 MI-JSTY: Document and justify exposed interfaces

1402 All exposed interfaces on the product in any state that is part of its reasonably foreseeable use or misuse in its
1403 secure-by-default configuration shall be documented. Every interface shall have a documented rationale for why its
1404 exposure is necessary for the functioning of the product in its secure-by-default configuration.

- 1405 • Reference: ER-LMAS

- 1406 • Objective: Limit attack surface

- 1407 • Preparation: List all types of interfaces on the product that may be exposed to an attacker, whether enabled or
1408 disabled. For each type of interface, list all exposed interfaces of that type, and document the method or
1409 methods used to create and verify these lists. List all states of the product with different exposed interfaces of
1410 the product in its secure-by-default configuration, including but not limited to initial configuration, startup, in
1411 use, idle, shutdown, and reset, if applicable. For each distinct exposed interface in each state, describe the
1412 interface and why it has to be enabled by default.

- 1413 • Activities: Using the list of types of interfaces, the list of states of the product, list all exposed interfaces in
1414 each state, and document the method or methods used to create and verify this list. Compare the list of exposed
1415 interfaces by state to the documented list by type.

- 1416 • Verdict: All discovered interfaces are documented, including rationale => PASS, otherwise => FAIL

- 1417 • Evidence: List of types of interfaces, list of product states, documentation of each exposed interface, output of
1418 methods to list all exposed interfaces, connection between each discovered interface to its documentation

1419 5.2.14.3 Mapping of mitigations to risk factors and security profiles

1420 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.

1421 5.2.15 ER-LOGG: Logging and monitoring

1422 5.2.15.1 Cybersecurity requirement

1423 The product shall record security-relevant internal events, including but not limited to changes to configuration and
1424 access or modification of data and functions. The product shall provide an opt-out mechanism.

1425 5.2.15.2 MI-LOGG: Logging

1426 The product shall record log messages indicating security-relevant internal events in an internal log or transmit them to
1427 the host system logging system. The log messages shall not include any confidential information such as PII, secrets, or
1428 credentials, or any information which might reasonably be expected to include such items.

- 1429 • Reference: ER-LOGG
 - 1430 • Objective: Monitoring and recording security-relevant events
 - 1431 • Preparation: List all types of security-relevant internal events
 - 1432 • Activities: For each type of security-relevant internal event, trigger the event
 - 1433 • Verdict: For each triggered event, the log contains a message indicating the event, log message does not
 - 1434 include any information likely to be confidential => PASS, otherwise FAIL
 - 1435 • Evidence: Method of triggering events, log messages with annotations
- 1436 Guidance: One type of event whose log message must take care to not accidentally include a secret is failed password
- 1437 authentication attempts. Since people often type their password into the username field, including the username field in
- 1438 the log message may result in including a secret in the log message.

1439 5.2.16 ER-SCDL: Secure deletion

1440 5.2.16.1 Cybersecurity requirement

1441 The product shall provide a method of deleting all user data and settings and resetting the product to its

1442 secure-by-default configuration.

1443 Guidance: Overwriting all user-writable storage or encrypting all user data and deleting the key are two secure deletion

1444 mechanisms.

1445 5.2.16.2 MI-RSET: Secure deletion via reset

1446 The product shall reset to its secure-by-default state after a power cycle or reset command.

- 1447 • Applicability: Product has the capability for the user to write data and/or settings
- 1448 • Reference: ER-SCDL
- 1449 • Objective: Secure deletion
- 1450 • Preparation: Document every kind of stored data or setting that may be changed by the user on the product,
- 1451 how to store it on the product, and how to read it from the product
- 1452 • Activities: For each kind of user data or setting that may be stored and changed by the user on the product,
- 1453 write an instance of the data or setting stored on the product that is different from the default and read it from
- 1454 the product; once all kinds of data have been written and read, power cycle or reset the product, and read each
- 1455 kind of data again
- 1456 • Verdict: If any data or setting is the same for both of the reads => FAIL, otherwise => PASS
- 1457 • Evidence: Record of each type of data or setting, what data or setting was written, what data or setting was
- 1458 returned by the first read, and what data or setting was returned by the second read, comparison of each one

1459 5.2.16.3 MI-INST: Secure deletion via reinstallation

1460 The product shall reset to its secure-by-default state after a reinstallation that securely deletes all previous user data or

1461 settings.

- 1462 • Applicability: Product has the capability for the user to write data and/or settings
- 1463 • Reference: ER-SCDL
- 1464 • Objective: Secure deletion
- 1465 • Preparation: Document every kind of data or setting that may be stored and changed by the user on the
- 1466 product, how to store it on the product, and how to read it from the product

1467 • Activities: For each kind of user data or setting that may be stored and changed by the user on the product,
 1468 write an instance of the data or setting stored on the product that is different from the default and read it from
 1469 the product; once all kinds of data have been written and read, reinstall the product with the secure delete
 1470 option, and read the data or settings again

1471 • Verdict: If any data or setting is the same for both of the reads => FAIL, otherwise => PASS

1472 • Evidence: Record of each type of data or setting, what data or setting was written, what data or setting was
 1473 returned by the first read, and what data or setting was returned by the second read, comparison of each one

1474 5.2.16.4 MI-DELE: Secure deletion via secure deletion function

1475 The product shall reset to its secure-by-default state after the secure deletion function is used.

1476 • Applicability: Product has the capability for the user to write data and/or settings

1477 • Reference: ER-SCDL

1478 • Objective: Secure deletion

1479 • Preparation: Document every kind of data or setting that may be stored and changed by the user on the
 1480 product, how to store it on the product, and how to read it from the product

1481 • Activities: For each kind of user data or setting that may be stored and changed by the user on the product,
 1482 write an instance of the data or setting stored on the product that is different from the default and read it from
 1483 the product; once all kinds of data have been written and read, activate the secure deletion function, and read
 1484 the data or settings again

1485 • Verdict: If any data or setting is the same for both of the reads => FAIL, otherwise => PASS

1486 • Evidence: Record of each type of data or setting, what data or setting was written, what data or setting was
 1487 returned by the first read, and what data or setting was returned by the second read, comparison of each one

1488 5.2.16.5 Mapping of mitigations to risk factors and security profiles

1489 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.

1490 5.2.17 ER-SDTR: Secure data read and transfer

1491 5.2.17.1 Cybersecurity requirement

1492 The product shall provide a method to read all data and settings from the product, and if provided, securely transfer data
 1493 and settings to another product.

1494 5.2.17.2 MI-SDRF: Secure data read from product

1495 The product shall provide a method by which an authorized user can securely read all data and settings from the
 1496 product.

1497 • Applicability: Product has the capability for the user to write data and/or settings

1498 • Reference: ER-SDTR

1499 • Objective: Secure data read

1500 • Preparation: List all data and settings

1501 • Activities: For each kind of data or setting, read the data or setting as an authorized user, then attempt read the
 1502 data or setting as an unauthorized user, if any exists

1503 • Verdict: All data and settings can be read by the authorized user, and no data or setting can be read by an
 1504 unauthorized user => PASS, otherwise FAIL

1505 • Evidence: List of data and settings, log message showing success or failure of each read by the authorized user
 1506 and, if applicable, the unauthorized user

1507 5.2.17.3 MI-SDTR: Secure data transfer to another product

1508 If the product provides a method to transfer data and settings to another product, it shall do so securely.

- 1509 • Applicability: Product has the capability for the user to write data and/or settings and to transfer them to
1510 another product.
- 1511 • Reference: ER-SDTR
- 1512 • Objective: Secure data transfer
- 1513 • Preparation: Prepare methods by which an unauthorized user could read the data during transfer as outlined in
1514 the risk assessment
- 1515 • Activities: Read the data or settings, initiate the data transfer, attempt to read or alter the transferred data and
1516 settings as an unauthorized user, read the new data and settings on the target product
- 1517 • Verdict: No data or settings could be read or altered by an an unauthorized user, and the data and settings read
1518 from the original product and target product are the same wherever technically possible => PASS, otherwise
1519 FAIL
- 1520 • Evidence: List of data and settings, log messages from the attempts to read or alter data as the unauthorized
1521 user, data and settings as read from the source product and as read from the target product, comparison
1522 explaining technical reasons for any differences in the two versions

1523 5.2.17.4 Mapping of mitigations to risk factors and security profiles

1524 See clause 5.3 for which mitigations are necessary for which security profiles and Annex C.4 for the rationale.

1525 5.2.18 ER-VULH: Vulnerability handling

1526 5.2.18.1 Cybersecurity requirement

1527 The product shall have vulnerability handling processes compliant with prEN 40000-1-3 [3].

1528 5.2.18.2 MI-VULH: Vulnerability handling

1529 The product shall have vulnerability handling processes compliant with prEN 40000-1-3 [3].

- 1530 • Applicability: (for cybersecurity requirements that depend on a feature)
- 1531 • Reference: ER-VULH
- 1532 • Objective: Vulnerability handling
- 1533 • Activities: Review documentation associated with vulnerability handling.
- 1534 • Verdict: Vulnerability handling documentation is compliant with prEN 40000-1-3 [[3]].(#_ref_3) => PASS,
1535 otherwise FAIL
- 1536 • Evidence: Vulnerability handling documentation, comparison with prEN 40000-1-3 [3].

1537 5.3 Risk Mitigation Sets

1538 5.3.1 Introduction

1539 This clause lists all the mitigations necessary to meet cybersecurity requirements for each security profile.

1540 5.3.1 Wired network interface risk mitigation sets

1541 5.3.1.1 SP-WD-1 required mitigations

- 1542 1. SCFS

- 1543 2. SUDC
- 1544 3. (SUVP or SUAP or SUOE or SUA0)
- 1545 4. DJST
- 1546 5. (NTFY or WDOG)
- 1547 6. DOST
- 1548 7. LOGG
- 1549 **5.3.1.2 SP-WD-2 required mitigations**
- 1550 1. (KEVD or KEVA or KEVT or SCAN)
- 1551 2. SCFS
- 1552 3. SSCA
- 1553 4. (FZ95 or BTIN or IMSL)
- 1554 5. IMSL or (MSAF-*, MZRO-*)
- 1555 6. ADEF
- 1556 7. DPAH
- 1557 8. PDDI-1
- 1558 9. PDDI-4
- 1559 10. SUDC
- 1560 11. (SUVP or SUAP or SUOE or SUA0)
- 1561 12. AUTH
- 1562 13. CDST
- 1563 14. DCTX
- 1564 15. DJST
- 1565 16. NTFY
- 1566 17. WDOG
- 1567 18. FDRP
- 1568 19. LMEM
- 1569 20. FAIR
- 1570 21. DOST
- 1571 22. MDOC
- 1572 23. MPHY
- 1573 24. JSTY
- 1574 25. LOGG
- 1575 26. VULH
- 1576 **5.3.1.3 SP-WD-3 required mitigations**
- 1577 1. (KEVD or KEVA or KEVT or SCAN)

- 1578 2. SCFS
- 1579 3. SSCA
- 1580 4. (FZ95 or BTIN or IMSL)
- 1581 5. IMSL or (MSAF-*, MZRO-*)
- 1582 6. ADEF
- 1583 7. DPAH
- 1584 8. PDDI-1
- 1585 9. PDDI-4
- 1586 10. SUDC
- 1587 11. (SUVVP or SUAP or SUOE or SUA0)
- 1588 12. AUTH
- 1589 13. CDST
- 1590 14. DCTX
- 1591 15. DJST
- 1592 16. (NTFY or WDOG)
- 1593 17. LMEM
- 1594 18. DOST
- 1595 19. MDOC
- 1596 20. MPHY
- 1597 21. JSTY
- 1598 22. LOGG
- 1599 23. VULH

1600 5.3.1.4 SP-WD-4 required mitigations

- 1601 1. (KEVD or KEVA or KEVT or SCAN)
- 1602 2. SCFS
- 1603 3. SSCA
- 1604 4. (FZ95 or BTIN or IMSL)
- 1605 5. IMSL or (MSAF-*, MZRO-*)
- 1606 6. ADEF
- 1607 7. DPAH
- 1608 8. PDDI-*
- 1609 9. SUDC
- 1610 10. (SUVVP or SUAP or SUOE or SUA0)
- 1611 11. AUTH
- 1612 12. CDST

1613	13. CDTX
1614	14. DOCC
1615	15. DCTX
1616	16. DJST
1617	17. NTFY
1618	18. WDOG
1619	19. FDRP
1620	20. LMEM
1621	21. FAIR
1622	22. DOST
1623	23. MDOC
1624	24. MPHY
1625	25. JSTY
1626	26. LOGG
1627	27. VULH

1628 5.3.2 Wireless network interface risk mitigation sets

1629 5.3.2.1 SP-WL-1 required mitigations

1630	1. (KEVD or KEVA or KEVT or SCAN)
1631	2. SCFS
1632	3. SSCA
1633	4. IMSL or (MSAF-*, MZRO-*)
1634	5. ADEF
1635	6. DPAH
1636	7. PDDI-1
1637	8. SUDC
1638	9. (SUVP or SUAP or SUOE or SUA0)
1639	10. AUTH
1640	11. CDST
1641	12. DOCC
1642	13. IDST
1643	14. DCTX
1644	15. DJST
1645	16. (NTFY or WDOG)
1646	17. LMEM

1647	18. DOST
1648	19. MDOC
1649	20. JSTY
1650	21. LOGG
1651	22. (RSET or INST or DELE)
1652	23. SDRF
1653	24. VULH
1654	5.3.2.2 SP-WL-2 required mitigations
1655	1. AUTH
1656	2. KEVD
1657	3. KEVA
1658	4. (KEVT or SCAN)
1659	5. SCFS
1660	6. SSCA
1661	7. (FZ95 or BTIN or IMSL)
1662	8. IMSL or (MSAF-*, MZRO-*)
1663	9. ADEF
1664	10. DPAH
1665	11. PDDI-1
1666	12. PDDI-4
1667	13. SUDC
1668	14. (SUAP or SUA0)
1669	15. AUTH
1670	16. CDST
1671	17. CDTX
1672	18. DOCC
1673	19. IDST
1674	20. DCTX
1675	21. DJST
1676	22. (NTFY or WDOG)
1677	23. LMEM
1678	24. MDOC
1679	25. MPHY
1680	26. DOST
1681	27. JSTY

- 1682 28. LOGG
- 1683 29. (RSET or INST or DELE)
- 1684 30. SDRF
- 1685 31. VULH
- 1686 5.3.2.3 SP-WL-3 required mitigations
- 1687 1. AUTH
- 1688 2. KEVD
- 1689 3. KEVA
- 1690 4. (KEVT or SCAN)
- 1691 5. SCFS
- 1692 6. SSCA
- 1693 7. (FZ95 or BTIN or IMSL)
- 1694 8. IMSL or (MSAF-*, MZRO-*)
- 1695 9. ADEF
- 1696 10. DPAH
- 1697 11. PDDI-*
- 1698 12. SUDC
- 1699 13. (SUAP or SUA0)
- 1700 14. AUTH
- 1701 15. CDST
- 1702 16. CDTX
- 1703 17. DOCC
- 1704 18. IDST
- 1705 19. DCTX
- 1706 20. DJST
- 1707 21. (NTFY or WDOG)
- 1708 22. LMEM
- 1709 23. DOST
- 1710 24. MDOC
- 1711 25. MPHY
- 1712 26. JSTY
- 1713 27. LOGG
- 1714 28. (RSET or INST or DELE)
- 1715 29. SDRF
- 1716 30. VULH

1717 5.3.3 Virtual network interface risk mitigation sets

1718 5.3.3.1 SP-VI-1 required mitigations

- 1719 1. (KEVD or KEVA or KEVT or SCAN)
- 1720 2. SCFS
- 1721 3. IMSL or (MSAF-*, MZRO-*)
- 1722 4. SUDC
- 1723 5. (SUVP or SUAP or SUOE or SUA0)
- 1724 6. CDST
- 1725 7. IDST
- 1726 8. DCTX
- 1727 9. DJST
- 1728 10. (NTFY or WDOG)
- 1729 11. LMEM
- 1730 12. DOST
- 1731 13. JSTY
- 1732 14. LOGG
- 1733 15. SDRF
- 1734 16. VULH

1735 5.3.3.2 SP-VI-2 required mitigations

- 1736 1. AUTH
- 1737 2. KEVD
- 1738 3. KEVA
- 1739 4. (KEVT or SCAN)
- 1740 5. SCFS
- 1741 6. SSCA
- 1742 7. (FZ95 or BTIN or IMSL)
- 1743 8. IMSL or (MSAF-*, MZRO-*)
- 1744 9. ADEF
- 1745 10. DPAH
- 1746 11. PDDI-1
- 1747 12. PDDI-3
- 1748 13. PDDI-4
- 1749 14. SUDC
- 1750 15. (SUAP or SUA0)

1751	16. AUTH
1752	17. CDST
1753	18. IDST
1754	19. DCST
1755	20. DCTX
1756	21. DJST
1757	22. NTFY
1758	23. WDOG
1759	24. FDRP
1760	25. LMEM
1761	26. FAIR
1762	27. MDOC
1763	28. MPHY
1764	29. DOST
1765	30. JSTY
1766	31. LOGG
1767	32. (RSET or INST or DELE)
1768	33. SDRF
1769	34. SDTR
1770	35. VULH

1771 6 Conformity Assessment

1772 6.1 General

1773 This clause details the assessment process for compliance with the cybersecurity requirements specified in clause 5 of
 1774 the present document. Each assessment corresponds to a mitigation defined in clause 5 and specifies the activities,
 1775 verdict criteria, and supporting evidence required to determine conformity.

1776 6.2.13.4 MI-FDRP assessment

1777 **[MI-FDRP]** Verify the product performs ordered validity checks on incoming packets and drops invalid packets before
 1778 further processing.

1779 Activities

1780 Verify:

- 1781 • The documentation describes the packet-processing pipeline, including the sequence of validity checks and the
 1782 rationale for their ordering.
- 1783 • The documented ordering applies less computationally expensive checks (e.g. frame length, header field
 1784 validation) before more expensive checks (e.g. deep packet inspection, cryptographic verification).
- 1785 • Packets with invalid frame lengths (below minimum and above maximum for the link-layer protocol) are
 1786 dropped before further processing.

1787 • Packets with invalid frame header fields (e.g. malformed protocol version, incorrect type, invalid checksum)
1788 are dropped at the header validation stage.

1789 • Packets addressed to a destination other than the product's configured address are dropped (with promiscuous
1790 mode disabled).

1791 • Under sustained high-rate invalid traffic, resource consumption remains bounded and valid packet processing
1792 is not degraded.

1793 Verdict

1794 Pass if:

1795 • The documentation describes the packet-processing pipeline with an ordered sequence of validity checks and a
1796 rationale;

1797 • Invalid frame lengths, invalid header fields, and misaddressed packets are each dropped before further
1798 processing;

1799 • Under sustained invalid traffic, resource consumption remains bounded and valid packet processing is not
1800 degraded.

1801 Fail otherwise.

1802 Supporting evidence

1803 • Packet-processing pipeline documentation, including check ordering and rationale;

1804 • Description of each invalid-packet test case and the specific invalidity injected;

1805 • Packet capture or log showing the point at which each invalid packet was dropped;

1806 • CPU and memory utilisation measurements during sustained invalid-traffic testing;

1807 • Evidence that valid packet processing was not degraded during the test.

1808 6.2.13.5 MI-LMEM assessment

1809 **[MI-LMEM]** Verify the product enforces documented limits on internal resources consumed by received data and
1810 handles limit conditions gracefully.

1811 Activities

1812 Verify:

1813 • The documentation identifies all internal resources consumed by received data (e.g. packet buffers, receive
1814 queues, descriptor rings) and specifies a limit for each.

1815 • For each identified resource, external input designed to exhaust the documented limit causes the product to
1816 drop new incoming data without crashing or corrupting existing state.

1817 • After the load subsides, the product recovers normal operation without requiring a reboot or manual
1818 intervention.

1819 Verdict

1820 Pass if:

1821 • The documentation identifies all internal resources consumed by received data and specifies a limit for each;

1822 • The product drops new incoming data when each limit is reached without crashing or corrupting existing state;

1823 • The product recovers normal operation after the load subsides.

1824 Fail otherwise.

1825 Supporting evidence

- 1826 • Documentation identifying each resource, its limit, and the rationale;
- 1827 • Description of each exhaustion test case and the method used to generate load;
- 1828 • Logs or observations demonstrating the product's behaviour when each limit was reached;
- 1829 • Evidence that the product recovered normal operation after each test.

1830 6.2.13.6 MI-FAIR assessment

1831 **[MI-FAIR]** Verify the product prevents any single input source from monopolising processing resources and prioritises
1832 at least one class of input over others under contention.

1833 Activities

1834 Verify:

- 1835 • The documentation describes the fairness and prioritisation mechanisms, including the default configuration
1836 and any user-configurable parameters.
- 1837 • Under sustained concurrent load on at least two input sources, no single source completely starves another of
1838 processing resources.
- 1839 • The prioritised class of input receives preferential treatment under contention, consistent with the documented
1840 mechanism.
- 1841 • If the product supports user-configurable prioritisation, changes to the configuration take effect as documented.

1842 Verdict

1843 Pass if:

- 1844 • The documentation describes the fairness and prioritisation mechanisms and their default configuration;
- 1845 • Under sustained concurrent load, no single input source completely starves another;
- 1846 • The prioritised class receives preferential treatment consistent with the documented mechanism;
- 1847 • User-configurable prioritisation changes take effect as documented (where applicable).

1848 Fail otherwise.

1849 Supporting evidence

- 1850 • Documentation of fairness and prioritisation mechanisms;
- 1851 • Description of each test scenario, including input sources and traffic rates;
- 1852 • Throughput and latency measurements for each input source during concurrent-load testing;
- 1853 • Evidence that user-configurable changes took effect (where applicable).

1854 6.2.13.7 MI-DOST assessment

1855 **[MI-DOST]** Verify the product is accompanied by documentation describing its denial-of-service protections and the
1856 protections the operational environment shall provide.

1857 Activities

1858 Verify:

- 1859 • The documentation describes what denial-of-service protections the product provides.

- 1860 • The documentation describes what protections the operational environment shall provide.
- 1861 • The boundary between product-provided and environment-provided protection is clear.
- 1862 • The documentation is comprehensible to the intended user of the product.

1863 Verdict

1864 Pass if:

- 1865 • The documentation describes the product's denial-of-service protections;
- 1866 • The documentation describes the protections the operational environment shall provide;
- 1867 • The boundary between product and environment responsibility is clear;
- 1868 • The documentation is comprehensible to the intended user.

1869 Fail otherwise.

1870 Supporting evidence

- 1871 • Denial-of-service protection documentation;
- 1872 • Assessment of comprehensibility for the intended user.

1873

1874 **Annex A (informative):**
 1875 **Mapping between the present document and CRA**
 1876 **essential requirements**

1877 The present document has been prepared under the Commission's standardisation request C(2025)618 [i.3] to provide
 1878 one voluntary means of conforming to the requirements of Regulation (EU) 2024/2847 [i.1] known as the Cyber
 1879 Resilience Act (CRA).

1880 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
 1881 with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the
 1882 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
 1883 EFTA regulations.

N o.	Description	CRA Essential Requirements	Cybersecurity Requirements(s)
1	Secure design, development, production	Annex I, Part I, (1)	TR-SSDD, TR-LMII
2	No known exploitable vulnerabilities	Annex I, Part I, (2)(a)	TR-NKEV
3	Secure by default configuration	Annex I, Part I, (2)(b)	TR-SDEF
4	Secure updates	Annex I, Part I, (2)(c)	TR-SCUD
5	Authentication and access control mechanisms	Annex I, Part I, (2)(d)	TR-AUTH*
6	Confidentiality of store and transmitted information	Annex I, Part I, (2)(e)	TR-CDST, TR-CDTX, TR-CRYP*
7	Integrity protection for data and configuration	Annex I, Part I, (2)(f)	TR-IDST, TR-IDTX
8	Data minimization	Annex I, Part I, (2)(g)	TR-DMIN
9	Availability protection	Annex I, Part I, (2)(h)	TR-AVAI, TR-LMII
10	Minimize impact on other devices or services	Annex I, Part I, (2)(i)	TR-MINI, TR-SDEF, TR-AVAI, TR-SSDD, TR-LMII
11	Limit attack surface	Annex I, Part I, (2)(j)	TR-LMAS, TR-SSDD, TR-LMII
12	Exploit mitigation by limiting incident impact	Annex I, Part I, (2)(k)	TR-LMII, TR-AVAI, TR-SSD
13	Logging and monitoring mechanisms	Annex I, Part I, (2)(l)	TR-LOGG
14	Secure deletion and data transfer	Annex I, Part I, (2)(m)	TR-SCDL, TR-SDTR
15	Vulnerability handling	Annex I, Part II	TR-VULH

1884
 1885 * *waiting on cross-vertical*

1886

1887 **Annex B (informative):**
1888 **Relationship between the present document and any**
1889 **related ETSI standards (if any)**

1890 ETSI TS 103 732 "Consumer Mobile Device Protection Profile" provided some terms and definitions.

1891

1892 **Annex C (informative):**
1893 **Risk identification and assessment methodology**

1894 **C.1 Assets**

1895 **C.1.1 Data**

1896 **C.1.1.1 Physical network interfaces**

- 1897 • Firmware
- 1898 • Device identity (MAC address etc.)
- 1899 • Device configuration (transmit power/channel configuration/options)
- 1900 • Statistics
- 1901 • Security keys for validation of access to itself (firmware, management access)
- 1902 • Security keys for packet encryption or network access
- 1903 • Device driver stored on device, if any
- 1904 • All accessible host data and functions
- 1905 • Packet data

1906 **C.1.1.2 Virtual network interfaces or device drivers**

- 1907 • Device driver executable
- 1908 • Interface configuration
- 1909 • Statistics
- 1910 • Security keys

1911 **C.1.2 Product functions**

1912 **C.1.2.1 Physical network interface essential functions**

- 1913 • Receive and transmit data between host and network at data link layer
- 1914 • Execute commands from the host (power, config, tx/rx)
- 1915 • Read/write/etc host resources accessible from card

1916 Optional:

- 1917 • Send commands/trigger actions on host (e.g. wake on network messages)
- 1918 • Offload of packet processing at layers higher than data link
- 1919 • Packet encryption at data link layer
- 1920 • Packet encryption at higher layer
- 1921 • Keep and report network statistics
- 1922 • Update firmware with image provided by host
- 1923 • Manage firmware update autonomously (image received from the network)

- 1924 • Provide remote management interface
- 1925 • Implement/support network boot

1926 C.1.2.2 Device driver essential functions

- 1927 • Copy data between network device interface and host memory
- 1928 • Handle interrupts, set up tx/rx, keep/copy statistics, etc.
- 1929 • Configure the network interface
- 1930 • Monitor device interface and network interface health
- 1931 • Interact with operating system and user programs

1932 Optional:

- 1933 • Set up and execute firmware update/load with image provided by host software
- 1934 • Support optional features of the underlying device hardware or software
- 1935 • Provision keys to device (network access, management, packet encryption)
- 1936 • Generate log messages
- 1937 • Use debug interfaces

1938 C.1.2.3 Virtual network interface essential functions

- 1939 • Process/move around data sent to virtual network interface
- 1940 • Interact with operating system
- 1941 • Configure the network interface
- 1942 • Keep and report network statistics
- 1943 • Read/write/etc host resources accessible from device driver

1944 Optional:

- 1945 • Packet encryption
- 1946 • Provision keys (network access, management, packet encryption)
- 1947 • Generate log messages

1948 C.2 Risk factors

1949 C.2.1 List of risk factors

1950 Risk factors determine which mitigation(s) satisfy each of the technical cybersecurity requirements in clause 5.2. The
 1951 manufacturer of a product determines the level of each risk factor via the development of a threat model and risk profile
 1952 based on the intended and foreseeable use and misuse of the network interface.

1953 Risk factors may increase the likelihood of an incident, increase the impact of an incident, or both. As a result, different
 1954 mitigation strategies may be more or less relevant to different risk factors.

1955 The overall risk related to each use case should be considered as a result of combining risk factors affecting both
 1956 likelihood and impact of an incident.

1957 **[PHY]** Degree of physical access to the device

1958 Description: Exposure of the device to physical access by users.

- 1959 Rationale: More users with physical access to the device increases the likelihood of an attack via physical interfaces.
- 1960 Type: Affects likelihood of attacks originating from physical access
- 1961 • **[PHY-L-0]** Foreseeable use is physical access only by authorized users
- 1962 • **[PHY-L-1]** Foreseeable use is incidental physical access by untrusted users
- 1963 • **[PHY-L-2]** Foreseeable use is frequent physical access by untrusted users
- 1964 **[SFT]** Degree of local software access to the host system
- 1965 Description: How many agents have unprivileged software access to the host system.
- 1966 Rationale: More agents with software access on the host increase the likelihood of an attack originating from the host.
- 1967 Type: Affects likelihood of attacks originating from the host system.
- 1968 • **[SFT-L-0]** Foreseeable use is effectively no agents on the host
- 1969 • **[SFT-L-1]** Foreseeable use is trusted agents
- 1970 • **[SFT-L-2]** Foreseeable use includes untrusted agents
- 1971 **[NET]** Degree of public access to attached network
- 1972 Description: How publicly accessible the attached network is.
- 1973 Rationale: The more unrestricted the access to the attached network is, the more likely a threat actor can send packets to
- 1974 the device.
- 1975 Type: Affects likelihood of attacks originating from the network and impact of attacks on other systems.
- 1976 • **[NET-L-0]** Foreseeable use is in an isolated private network
- 1977 • **[NET-L-1]** Foreseeable use is in a private network with filtered connection to public network
- 1978 • **[NET-L-2]** Foreseeable use is in a public network
- 1979 **[COM]** Complexity of product functions
- 1980 Description: How complex the available product functions are in its secure-by-default configuration.
- 1981 Rationale: More complex functions means increased likelihood of errors in the implementation and more attack surface.
- 1982 Type: Affects likelihood of all attacks.
- 1983 • **[COM-L-0]** Product implements minimal features necessary to send/recv packets but not the features in
- 1984 COM-L-1 or COM-L-2
- 1985 • **[COM-L-1]** Product implements features such as simple performance improvements which are more complex
- 1986 than COM-L-0 but less complex than those in COM-L-2
- 1987 • **[COM-L-2]** Product implements complex features such as encryption functions, RTOS managing radio, PXE
- 1988 boot, remote management, etc.
- 1989 **[LIS]** Ease of reading from transmission media of directly attached network by unauthorized agents
- 1990 Description: Likelihood that unauthorized agents can read data from the transmission media on the directly attached
- 1991 network. For example, a wireless network in an apartment that is accessible from the shared hallway or another
- 1992 apartment, or a wired network with exposed jacks in a public library.
- 1993 Rationale: While confidentiality of data transmitted across public networks is usually handled by the system the
- 1994 network interface is integrated into, the network interface is usually responsible for confidentiality on the local directly
- 1995 attached network.
- 1996 Type: Affects likelihood of attack.

- 1997 • **[LIS-L-0]** Foreseeable use is only authorized agents with access to directly attached network
- 1998 • **[LIS-L-1]** Foreseeable use includes occasional access by unauthorized agents to directly attached network
- 1999 • **[LIS-L-2]** Foreseeable use includes frequent access by unauthorized agents to directly attached network
- 2000 **[ADM]** Availability and skill of administration
- 2001 Description: What the availability and skill of administration is for the product.
- 2002 Rationale: Skilled, fully resourced administration allows more risk transfer and can reduce the impact of incidents.
- 2003 Type: Affects likelihood and impact of all attacks.
- 2004 • **[ADM-L-0]** Foreseeable use is with fully resourced professional administration
- 2005 • **[ADM-L-1]** Foreseeable use is with professional administration with limited resources
- 2006 • **[ADM-L-2]** Foreseeable use is with unskilled or no administration
- 2007 **[SYS]** Impact of access to host system assets
- 2008 Description: Measures the impact of the product's access to host system assets, which is a combination of the level of
- 2009 access and the sensitivity of the host system assets.
- 2010 The communications bus used to connect to the host system usually controls the level of access. E.g., a network
- 2011 interface connected by USB versions below 4.0 can only access system resources via the host USB stack software, but a
- 2012 network interface on a PCIe bus (including tunneled over USB 4.0) or a virtual network interface that has privileged
- 2013 access to the host system can write any part of host system memory. The sensitivity of the host assets changes the
- 2014 impact of this risk factor.
- 2015 Rationale: An attacker can get access to host system functions via the product's access.
- 2016 Type: Affects impact of all attacks.
- 2017 • **[SYS-L-0]** Little or no access to the host, or little or no sensitivity of host assets
- 2018 • **[SYS-L-1]** High degree of access to host and moderate sensitivity of host assets, or moderate access and high
- 2019 sensitivity
- 2020 • **[SYS-L-2]** High degree of access and high sensitivity of host assets
- 2021 **[SDS]** Sensitivity of data stored
- 2022 Description: Sensitivity of data stored on the product.
- 2023 Rationale: The more sensitive the data stored, the higher the impact of compromise of that data.
- 2024 Type: Affects impact of attack.
- 2025 • **[SDS-L-0]** Foreseeable use stores unimportant or no data
- 2026 • **[SDS-L-1]** Foreseeable use stores moderately sensitive data
- 2027 • **[SDS-L-2]** Foreseeable use stores highly sensitive data
- 2028 **[SDT]** Sensitivity of data transmitted
- 2029 Description: Sensitivity of data transmitted on the product.
- 2030 Rationale: The more sensitive the data transmitted, the higher the impact of compromise of that data.
- 2031 Type: Affects impact of attack.
- 2032 • **[SDT-L-0]** Foreseeable use transmits unimportant or no data
- 2033 • **[SDT-L-1]** Foreseeable use transmits moderately sensitive data

- 2034 • **[SDT-L-2]** Foreseeable use transmits highly sensitive data

2035 **[FUN]** Sensitivity of functions

2036 Description: Sensitivity of functions of the product.

2037 Rationale: The more sensitive the functions of the product, the higher the impact of denial-of-service or corruption of
2038 the functions.

2039 Type: Affects impact of attack.

- 2040 • **[SDT-L-0]** Foreseeable use is for unimportant functions

- 2041 • **[SDT-L-1]** Foreseeable use is for moderately sensitive functions, such as encrypting transmitted data

- 2042 • **[SDT-L-2]** Foreseeable use is for highly sensitive functions, such as primary management interface of host
2043 system

2044 **[INT]** Integration in host system

2045 Description: How difficult it is to remove the product from the host system.

2046 Rationale: The more integrated a product is in the host system, the harder it is to disable, remove, or replace it if it has
2047 an exploitable unpatched vulnerability or is no longer supported.

2048 Type: Affects impact of attack.

- 2049 • **[INT-L-0]** Product is connected to host system via external adapter

- 2050 • **[INT-L-1]** Product is connected to host system via internal adapter requiring disassembly to change

- 2051 • **[INT-L-2]** Product is fully integrated into and cannot be removed from host system

2052 C.3 Assumptions

2053 C.3.1 Proper host system

2054 **[AS-PH]:** The host system the product is attached to is trustworthy.

2055 C.3.2 Proper administrator

2056 **[AS-PA]:** The product administrator is not intentionally hostile and is engaging in good faith efforts to administer the
2057 product properly.

2058 C.3.3 Attacker has limited physical access to product

2059 **[AS-LP]:** An attacker will have only temporary physical access to the product.

2060 C.3.4 Attacker has limited resources

2061 **[AS-LR]:** An attacker has the resources available to a small group of skilled individuals, without the backing of large
2062 corporations, nation-states, or immense wealth.

2063 C.4 Threats and risk assessment of threats

2064 C.4.1 General

2065 The approach to listing threats is to separate them by mitigation so that they may be associated with mitigations more
2066 directly.

2067 For the purposes of the list of threats, the product includes:

- 2068 • the physical network interface (if any)

- 2069 • the device driver (if any)
- 2070 • the virtual network interface (if any)

2071 C.4.2 Risk assessment methodology

2072 Risk factor levels for each security profile are determined by reading the descriptions for each risk factor level and
2073 choosing the one that most accurately represents the highest risk for the intended purpose and reasonably foreseeable
2074 use and misuse of the product, as specified by the manufacturer.

2075 For each threat, a formula based on the risk factor levels is used to calculate the Likelihood and Impact of the threat, on
2076 a scale of Low, Medium, and High.

2077 For each threat, both likelihood and impact must be Low before the risk is considered sufficiently mitigated. If the
2078 calculated levels are not already Low, then mitigations must be applied until they are both Low. The mitigation sets that
2079 will accomplish this are listed in each threat description.

2080 The risk factors by type are:

- 2081 • Likelihood: PHY SFT NET COM ADM LIS
- 2082 • Impact: SYS SDS SDT FUN INT

2083 The mitigations that reduce risk by type are:

- 2084 • Likelihood: KEVD, KEVA, KEVM, KEVT, SCAN, SCFS, SSCA, FZ95, BTIN, IMSL, MSAF-*, MZRO-*,
2085 ADEF, DPAH, PDDI-*, SUDC, SUVP, SUOE, SUAP, SUA0, CDTX, JSTY, RSET, INST, DELE, VULH
- 2086 • Impact: IMSL, DCTX, DJST, IDST, NTFY, WDOG, LOGG, SDRF, SDTR

2087 C.4.3 List of threats, risk assessments, and mitigations

2088 C.4.3.1 TH-UEVU: Unknown exploitable vulnerabilities

2089 Attacker may use unknown exploitable vulnerabilities in the product implementation to get unauthorized access to
2090 product assets.

Risk factors	Likelihood	Security profiles
max(PHY, SFT, NET) = 0 or COM = 0	Low	WD-1, VI-1
all others	Medium	WD-2, WD-3, WD-4, WL-1
max(PHY, SFT, NET) = 2 & COM = 2	High	WL-2, WL-3, VI-2

2091

Risk factors	Impact	Security profiles
max(SYS, SDS, SDT, FUN) = 0	Low	none
max(SYS, SDS, SDT, FUN) = 1	Medium	WD-1, WD-3, WL-1, VI-1
max(SYS, SDS, SDT, FUN) = 2	High	WD-2, WD-4, WL-2, WL-3, WL-4, VI-2

2092

2093 cybersecurity requirements that mitigate this threat: SSDD, LMII, DMIN, LMAS, LOGG

2094 Mitigations for Likelihood:

- 2095 • Medium to Low: SCFS, SSCA, ADEF, DPAH, PDDI-*
- 2096 • High to Low: SCFS, SSCA, (FZ95 or BTIN or IMSL), MSAF-*, MZRO-*, ADEF, DPAH, PDDI-*, JSTY

2097 Mitigations for Impact:

- 2098 • Medium to Low: LOGG
- 2099 • High to Low: DJST, LOGG

2100 C.4.3.2 TH-KEVU: Known exploitable vulnerabilities

2101 Attacker may use known exploitable vulnerabilities in the product implementation to get unauthorized access to product
2102 assets.

Risk factors	Likelihood	Security profiles
max(PHY, SFT, NET) = 0 or COM = 0 or ADM = 0	Low	WD-1
all others	Medium	WD-2, WD-3, WD-4, WL-1, VI-1
max(PHY, SFT, NET) = 2 & COM = 2 & ADM = 2	High	WL-2, WL-3, VI-2

2103

Risk factors	Impact	Security profiles
max(SYS, SDS, SDT, FUN) = 0	Low	none
max(SYS, SDS, SDT, FUN) = 1	Medium	WD-1, WD-3, WL-1, VI-1
max(SYS, SDS, SDT, FUN) = 2	High	WD-2, WD-4, WL-2, WL-3, WL-4, VI-2

2104

2105 Cybersecurity requirements that mitigate this threat: NKEV, SSDD, LMII, SCUD, DMIN, LMAS, LOGG, VULH

2106 All mitigations from TH-UEVU apply (using that cybersecurity requirement's risk formula), in addition to:

2107 Mitigations for Likelihood:

2108 • Medium to Low: (KEVD or KEVA or KEVT or SCAN), KEVM, (SUVP or SUAP or SUOE or SUA0),
2109 VULH

2110 • High to Low: KEVD, KEVA, (KEVT or SCAN), KEVM, (SUAP or SUA0), VULH

2111 C.4.3.3 TH-PHYS: Access to data via acquisition of used product

2112 Attacker may get unauthorized access to confidential data stored on the product through acquisition of a used product.

Risk factors	Likelihood	Security profiles
ADM = 0 or SDS = 0	Low	WD-*, VI-1
all others	Medium	WL-*
ADM = 2 & SDS = 2	High	VI-2

2113

Risk factors	Impact	Security profiles
SDS = 0	Low	WD-*
SDS = 1	Medium	WL-*, VI-1
SDS = 2	High	VI-2

2114

2115 Cybersecurity requirements that mitigate this threat: CDST, SCDL, SDEF

2116 Mitigations for Likelihood:

2117 • Medium to Low: ADEF, DPAH, (RSET or INST or DELE), SDRF

2118 • High to Low: ADEF, DPAH, PDDI-*, (RSET or INST or DELE), SDRF, SDTR

2119 Mitigations for Impact:

2120 • Medium to Low: CDST

2121 • High to Low: CDST

2122 C.4.3.4 TH-CONF: Access to assets via configuration errors

2123 Attacker may use configuration errors to get unauthorized access to the product assets.

Risk factors	Likelihood	Security profiles
max(PHY, SFT, NET) = 0 or ADM = 0	Low	WD-1, VI-1
all others	Medium	WL-1
max(PHY, SFT, NET) = 2 & ADM = 2	High	WD-3, WL-2, WL-3, VI-2

2124

Risk factors	Impact	Security profiles
$\max(\text{SYS}, \text{SDS}, \text{SDT}, \text{FUN}) = 0$	Low	none
$\max(\text{SYS}, \text{SDS}, \text{SDT}, \text{FUN}) = 1$	Medium	WD-1, WD-3, VI-1
$\max(\text{SYS}, \text{SDS}, \text{SDT}, \text{FUN}) = 2$	High	WD-2, WD-4, WL-* VI-2

2125

2126 Cybersecurity requirements that mitigate this threat: CDST, SDEF, DMIN, LOGG

2127 Mitigations for Likelihood:

2128 • Medium to Low: ADEF, DPAH, PDDI-1

2129 • High to Low: ADEF, DPAH, PDDI-2 if PHY = 2, PDDI-3 if SFT = 2, PDDI-4 if NET = 2

2130 Mitigations for Impact:

2131 • Medium to Low: CDST

2132 • High to Low: CDST, DJST, LOGG

2133 C.4.3.5 TH-UADT: Unauthorized access to confidential data transmitted

2134 Attacker may use network access to get unauthorized access to confidential data transmitted by the product.

Risk factors	Likelihood	Security profiles
LIS = 0	Low	WD-1, WD-2, WD-3, VI-1, VI-2
LIS = 1	Medium	WL-1
LIS = 2	High	WD-4, WL-2, WL-3

2135

Risk factors	Impact	Security profiles
SDT = 0	Low	none
SDT = 1	Medium	WD-*, WL-*, VI-1
SDT = 2	High	VI-2

2136

2137 Cybersecurity requirements that mitigate this threat: CDTX, IDTX, DMIN

2138 Mitigations for Likelihood:

2139 • Medium to Low: DOCC

2140 • High to Low: CDTX, DOCC

2141 Mitigations for Impact:

2142 • Medium to Low: DJST

2143 • High to Low: DJST

2144 C.4.3.6 TH-AVAI: Denial of service attack on product via exploitation of vulnerabilities

2145 Attacker may exploit vulnerabilities in the product to reduce availability of product assets.

Risk factors	Likelihood	Security profiles
$\max(\text{PHY}, \text{SFT}, \text{NET}) = 0$ or COM = 0 or ADM = 0	Low	WD-1
all others	Medium	WD-2, WD-3, WD-4, WL-1, VI-1
$\max(\text{PHY}, \text{SFT}, \text{NET}) = 2$ & COM = 2 & ADM = 2	High	WL-2, WL-3, VI-2

2146

Risk factors	Impact	Security profiles
$\max(\text{SDS}, \text{SDT}, \text{FUN}) = 0$	Low	none
$\max(\text{SDS}, \text{SDT}, \text{FUN}) = 1$	Medium	WD-1, WD-3, WL-*, VI-1
$\max(\text{SDS}, \text{SDT}, \text{FUN}) = 2$	High	WD-2, WD-4, VI-2

2147

2148 Cybersecurity requirements that mitigate this threat: NKEV, AVAI, LMII, LMAS, LOGG, VULH

2149 All mitigations for TH-KEVU apply (using that cybersecurity requirement's risk formula), plus:

2150 Mitigations for Impact:

2151 • Medium to Low: (NTFY or WDOG)

2152 • High to Low: NTFY, WDOG

2153 C.4.3.7 TH-PDOS: Denial of service attack on product functions via system or network 2154 access

2155 Attacker may use host system or network access for a denial-of-service attack on product functions.

Risk factors	Likelihood	
max(SFT, NET) = 0	Low	WD-1
max(SFT, NET) = 1	Medium	WL-1, VI-1
max(SFT, NET) = 2	High	WD-2, WD-3, WD-4, WL-2, WL-3, VI-2

2156

Risk factors	Impact	Security profiles
FUN = 0	Low	none
FUN = 1	Medium	WD-1, WD-3, WL-*, VI-1
FUN = 2	High	WD-2, WD-4, VI-2

2157

2158 Cybersecurity requirements that mitigate this threat: AUTH, AVAI, LMII, LOGG

2159 Mitigations for Likelihood:

2160 • Medium to Low: DOST

2161 • High to Low: DOST

2162 Mitigations for Impact:

2163 • Medium to Low: (NTFY or WDOG), LMEM, LOGG

2164 • High to Low: NTFY, WDOG, FDRP, LMEM, FAIR, LOGG

2165 C.4.3.8 TH-DDOS: Denial of service attack on other products via exploitation of 2166 vulnerabilities

2167 Attacker may exploit vulnerabilities in the product to attack other products.

Risk factors	Likelihood	Security profiles
NET = 0 or COM = 0 or ADM = 0	Low	WD-1
all others	Medium	WD-2, WD-3, WD-4, WL-1, VI-1
NET = 2 & COM = 2 & ADM = 2	High	WL-2, WL-3, VI-2

2168

Risk factors	Impact	Security profiles
NET = 0	Low	WD-1, VI-1
NET = 1	Medium	WL-1,
NET = 2	High	WD-2, WD-3, WD-4, WL-2, WL-3, V-2

2169

2170 Cybersecurity requirements that mitigate this threat: NKEV, LMII, MINI, LMAS, LOGG, VULH

2171 All mitigations from TH-KEVU apply (using that cybersecurity requirement's risk formula), plus:

2172 Mitigations for Impact:

2173 • Medium to Low: MDOC

2174 • High to Low: MDOC, MPHY

2175 C.4.3.9 TH-MQSE: Masquerading authorized server

2176 Attacker may masquerade as an authorized server to get unauthorized access to product assets.

Risk factors	Likelihood	Security profiles
NET = 0 or COM = 0	Low	WD-1, VI-1
all others	Medium	WD-2, WD-3, WD-4
NET = 2 & COM = 2	High	WL-2, WL-3, VI-2

2177

Risk factors	Impact	Security profiles
max(SYS, SDS, SDT, FUN) = 0	Low	none
max(SYS, SDS, SDT, FUN) = 1	Medium	WD-1, WD-3, VI-1
max(SYS, SDS, SDT, FUN) = 2	High	WD-2, WD-4, WL-* VI-2

2178

2179 Cybersecurity requirements that mitigate this threat: CDTX, IDTX, AUTH, SCUD, LOGG

2180 Mitigations for Likelihood:

2181 • Medium to Low: AUTH, SUDC, (SUVP or SUAP or SUOE or SUA0), CDTX, IDTX

2182 • High to Low: AUTH, SUDC, (SUAP or SUA0), CDTX, IDTX

2183 Mitigations for Impact:

2184 • Medium to Low: LOGG

2185 • High to Low: LOGG

2186 **C.4.3.10 TH-AHHS: Harm to host system via unauthorized access through the network**

2187 Attacker may use unauthorized access to the product through the network to harm the host system.

2188 NOTE: If the attacker has physical or host system software access, they do not need to use the network device to
2189 harm the system.

Risk factors	Likelihood	Security profiles
NET = 0 or COM = 0 or ADM = 0	Low	WD-1, VI-1
all others	Medium	WD-4
NET = 2 & COM = 2 & ADM = 2	High	WL-2, WL-3, VI-2

2190

Risk factors	Impact	Security profiles
SYS = 0	Low	none
SYS = 1	Medium	WD-1, WD-3, WL-1, VI-1
SYS = 2	High	WD-2, WD-4, WL-2, WL-3, VI-2

2191

2192 Cybersecurity requirements that mitigate this threat: NKEV, SSDD, LMII, SCUD, AUTH, LMAS, LOGG

2193 All mitigations from TH-KEVU apply (using that cybersecurity requirement's risk formula), plus:

2194 Mitigations for Likelihood:

2195 • Medium to Low: AUTH

2196 • High to Low: AUTH

2197 C.5.2 Mapping of use cases to risk factors and security profiles

2198 C.5.2.1 Wired network interface use cases

Use case	PHY	SFT	NET	COM	ADM	LIS	SYS	SDS	SDT	FUN	INT	Sec Pro
UC-WD-1	0	0	0	1	2	0	0	0	0	1	2	SP-WD-1
UC-WD-2	0	0	0	1	0	0	1	0	1	1	1	SP-WD-1
UC-WD-3	0	0	1	1	0	0	1	0	1	2	1	SP-WD-2
UC-WD-4	0	0	2	1	0	0	2	0	1	2	1	SP-WD-2
UC-WD-5	0	0	2	1	1	0	1	0	1	1	1	SP-WD-2
UC-WD-6	1	1	1	1	0	0	1	0	1	1	1	SP-WD-3
UC-WD-7	1	1	1	1	2	0	1	0	1	1	1	SP-WD-3
UC-WD-8	1	1	2	1	2	0	1	0	1	1	1	SP-WD-3
UC-WD-9	0	2	1	1	0	0	2	0	1	2	1	SP-WD-4
UC-WD-10	2	2	1	1	1	0	2	0	0	0	1	SP-WD-4

2199

2200 C.5.2.2 Wireless network interface use cases

Use case	PHY	SFT	NET	COM	ADM	LIS	SYS	SDS	SDT	FUN	INT	Sec Pro
UC-WL-1	0	0	0	2	0	0	1	1	1	1	1	SP-WL-1
UC-WL-2	0	0	1	2	2	1	0	0	0	1	2	SP-WL-1
UC-WL-3	0	0	2	2	0	1	2	1	1	1	1	SP-WL-2
UC-WL-4	1	1	2	2	0	2	2	1	1	1	1	SP-WL-2
UC-WL-5	0	1	1	2	2	1	1	1	1	1	1	SP-WL-2
UC-WL-6	1	1	2	2	2	2	2	1	1	1	1	SP-WL-3
UC-WL-7	2	2	1	2	1	2	1	0	0	0	1	SP-WL-3

2201

2202 C.5.2.3 Virtual network interface use cases

Use case	PHY	SFT	NET	COM	ADM	LIS	SYS	SDS	SDT	FUN	INT	Sec Pro
UC-VI-1	0	1	0	0	0	0	0	1	1	1	0	SP-VI-1
UC-VI-2	0	1	2	2	2	0	1	1	1	1	0	SP-VI-2
UC-VI-3	0	1	1	2	0	0	2	2	2	2	0	SP-VI-2
UC-VI-4	0	2	2	2	0	0	2	2	2	2	0	SP-VI-2

2203

2204 C.6 Security profiles

2205 C.6.1 General

2206 Security profiles are an informative resource to the manufacturer. Each security profile is associated with a collection of
 2207 levels of risk factors. Security profiles will be mapped to specific mitigations for each cybersecurity requirements
 2208 necessary to treat the risk.

2209 C.6.2 Mapping of security profile to risk factors

2210 Security profiles are associated with sets of risk factor levels.

2211 C.6.2.1 Wired network interface security profiles

Security profile	PHY	SFT	NET	COM	ADM	LIS	SYS	SDS	SDT	FUN	INT
SP-WD-1	0	0	0	1	2	0	1	0	1	1	2
SP-WD-2	0	0	2	1	1	0	2	0	1	2	1
SP-WD-3	1	1	2	1	2	0	1	0	1	1	1
SP-WD-4	2	2	2	1	1	2	2	0	1	2	1

2212

2213 C.6.2.2 Wireless network interface security profiles

Security profile	PHY	SFT	NET	COM	ADM	LIS	SYS	SDS	SDT	FUN	INT
SP-WL-1	0	0	1	2	2	1	1	1	1	1	1
SP-WL-2	1	1	2	2	2	2	2	1	1	1	1
SP-WL-3	2	2	2	2	2	2	2	1	1	1	1

2214

2215 C.6.2.3 Virtual network interface security profiles

Security profile	PHY	SFT	NET	COM	ADM	LIS	SYS	SDS	SDT	FUN	INT
SP-VI-1	0	1	0	0	0	0	1	1	1	1	0
SP-VI-2	0	2	2	2	2	0	2	2	2	2	0

2216

2217 C.7 How to add new security profiles

2218 To add a new security profile, do the following:

- 2219 1. Do a risk assessment on the category of product covered by the new security profile.
- 2220 2. Determine the risk factors for the new security profile.
- 2221 3. If there are any new threats, add them to the threats list along with their risk calculation formula.
- 2222 4. If any new risk factors are necessary to calculate risks for the new security profile, add the risk factors and
2223 update the score for all the security profiles.
- 2224 5. Use the risk factors of the new security profile and the risk formula for each threat to calculate which of the
2225 existing mitigations must be applied.
- 2226 6. After the existing risk mitigations are applied, check if all threats are sufficiently mitigated. If not, add new
2227 mitigations until the threats have been reduced sufficiently.
- 2228 7. Update all relevant mappings (e.g. security profile to risk mitigation sets).
- 2229 8. Propose the new security profile as a contribution to the standard.

2230

2231 Annex D (informative): 2232 Risk evaluation guidance

2233 D.1 Explanation of Risk Modeling Approach

2234 The risk modeling approach followed in this document can be applied to two situations:

- 2235 1. *Covered*: For Manufacturers of products with use cases that are present in the text of this document, it states
2236 the mitigations which the product shall implement and provides guidance on how to verify that the mitigations
2237 are implemented in a product. Furthermore, it describes why that unique set of mitigations is sufficient for the
2238 use case.
- 2239 2. *Not Covered*: For Manufacturers of products whose use case does not precisely match use cases covered in the
2240 present document, the methodology used herein may be further used to derive the appropriate set of
2241 mitigations for a given product, and to communicate this justification in a structured way. This could inform
2242 revisions of this document and the list of use cases over time.

2243 Methodology

2244 This clause describes the methodology followed in the current text.

- 2245 1. Document a comprehensive range of foreseeable use cases for products of this type.
- 2246 2. For a particular use case, document the inherent and product-specific risk factors likely to affect products of
2247 that type which are not already covered by other relevant standards.
- 2248 3. For that use case, document environmental risk factors likely to affect products of that type which are not
2249 already covered by other relevant standards.
- 2250 4. Document a comprehensive list of threats. For each threat, create a formula to estimate the risk level using the
2251 risk factors.
- 2252 5. For each threat, document appropriate mitigations which should be present to mitigate the specific risk
2253 depending on the risk level. For each mitigation, also document at least one verification methodology.
- 2254 6. Create a mapping between each use case and each risk factor, assigning a proportionality score. The scoring
2255 range should start from zero, representing the inapplicability of a risk factor to a use case, and increase
2256 monotonically based on both the likelihood and severity of potential harm or impact.
- 2257 7. Develop security profiles from the use cases, which are collections of risk factor levels that can be used to fully
2258 describe the risk levels of all relevant threats. There may be one use case per security profile or multiple. There
2259 should be as many security profiles as are useful to manufacturers.
- 2260 8. Using the risk factors in the security profiles and the risk formulas and mitigations for all threats, derive the
2261 completed list of required mitigations for each security profile.

2262 D.2 Mapping of risks to cybersecurity requirements

Threat	Cybersecurity Requirements
KEVU	NKEV, SCUD, SSDD, LMII, LMAS, LOGG, VULH
UEVU	SSDD, LMII, DMIN, LMAS, LOGG
PHYS	SCDL, SDEF
CONF	SDEF
UADT	CDTX, DMIN, LMAS
AVAI	AVAI, LMII, LMAS, LOGG, VULH
PDOS	AVAI, LMII, LMAS, LOGG
DDOS	MINI, AVAI, LMII, LMAS, LOGG, VULH
MQSE	CDTX, IDTX, SCUD, LOGG
AHHS	NKEV, SCUD, SSDD, LMII, LMAS, LOGG, SDEF

2263

2264 D.3 Risk acceptance criteria

2265 If the Likelihood and Impact of a risk are already Low or have been reduced to Low by application of mitigations, then
2266 the risk is acceptable. Alternatively, the risk may be transferred to the user or the operational environment, given proper
2267 justification.

2268 D.4 Risks not treated by the cybersecurity requirements

2269 For each risk untreated by the product itself, a corresponding mitigation has been created to explicitly permit the risk to
2270 be transferred to the user or operational environment. These are:

- 2271 • MI-KEVD
- 2272 • MI-KEVM
- 2273 • MI-DPAH
- 2274 • MI-PDDI-1
- 2275 • MI-SUDC
- 2276 • MI-SUOE
- 2277 • MI-SUAO
- 2278 • MI-DOCC
- 2279 • MI-DOST

2280

2281 **Annex E:**
2282 **Explanation of the present document (informative**
2283 **only)**

2284 **E.1 Introduction**

2285 This is a short introduction to how standards work, how CRA vertical standards work in general, and how this standard
2286 specifically works.

2287 **E.2 How to understand a vertical standard**

2288 **E.2.1 General**

2289 The present document is a vertical standard for the Cyber Resilience Act. This is a new kind of standard with some
2290 unusual properties. Read the rest of this clause to understand how it works.

2291 **E.2.2 TL;DR**

2292 The manufacturer defines an intended purpose or use case for their product. This use case determines how the essential
2293 cybersecurity requirements of the CRA can be satisfied.

2294 The vertical standard is only one way of assessing CRA conformance. Others methods are available if the product uses
2295 incompatible methods of CRA conformance.

2296 Clauses 1 - 4 are not binding, just helpful context. Clause 5 sets out the cybersecurity requirements necessary to
2297 conform with the CRA. Clause 6 sets out how to assess the conformance of the product with the CRA.

2298 Each technical cybersecurity requirement can be satisfied by one or more mitigations describing the default behaviour
2299 of the product. The user may configure the product differently unless explicitly forbidden in the text of the
2300 cybersecurity requirement. Which mitigations are required depend on risk factors specific to each use case, and
2301 capabilities of the product. The tables at the end of each cybersecurity requirement show which mitigations are required.

2302 Security profiles are groups of use cases that can be satisfied with the same mitigations. A product must fit into a
2303 security profile to use the vertical standard for CRA conformance. If a security profile includes mitigations that are
2304 sufficient to treat all of a product's cybersecurity risks, then the product may be assessed using the vertical standard.

2305 **E.3 Standard basics**

2306 **E.3.1 Normative and informative text**

2307 Standards consist of two kinds of text: informative and normative. Informative text is just "for your information": it is
2308 helpful for understanding the standard but it has no legally binding meaning. Normative text describes things that matter
2309 for conforming for the standard.

2310 This vertical standard has only two normative clauses: Clause 5 Cybersecurity requirements and Clause 6 Assessment
2311 criteria. Everything else is just to help the reader understand the normative parts of the document. That means if
2312 something in clauses 1 - 4 or the Annexes isn't exactly correct, that doesn't affect the way you can use the standard.

2313 **E.3.2 Cybersecurity requirements describe default configuration only**

2314 The cybersecurity requirements describe the default configuration of the product. It is implied that the product can be
2315 configured to behave in a different way, unless the cybersecurity requirement explicitly states that the product may not
2316 permit such an option. For example, if a cybersecurity requirement says a debug interface must be disabled, then the
2317 product may have an option to enable the debug interface. Only if the requirement says a debug interface must be
2318 *permanently* disabled would it be not allowed to have an option to enable it.

2319 E.4 CRA vertical standard specifics

2320 E.4.1 Vertical standards are optional

2321 Using a CRA vertical standard to assess conformance with the CRA is optional. A product may be assessed for
2322 conformance using a variety of other options as outlined in the CRA. If the vertical standard does not fit a specific
2323 product, then the manufacturer has many other options for assessment.

2324 However, there are two advantages to using a vertical standard: (1) it allows self-assessment of Important Class II
2325 products, (2) it provides presumption of conformity. Note that all products consistently entirely of free and open source
2326 software as defined by the CRA can always self-assess, with or without a vertical standard.

2327 E.4.2 Manufacturer declares intended purpose/use case

2328 For the purposes of the CRA, the manufacturer declares an intended purpose and reasonably foreseeable use and misuse
2329 for a product. This allows the manufacturer to do a risk assessment that is specific to a particular use case.

2330 E.4.3 Intended purpose/use case and capabilities determines how to satisfy 2331 cybersecurity requirements

2332 A vertical standard includes a set of cybersecurity requirements and ways to satisfy them. The ways to satisfy them are
2333 **dependent on the use case and capabilities** of a product.

2334 E.4.4 Each cybersecurity requirement can be satisfied by one or more 2335 mitigations

2336 Each cybersecurity requirement is associated with a set of mitigations that reduce the cybersecurity risk of the product.
2337 Which mitigations are required to be implemented depend on the intended purpose/use case.

2338 E.4.5 Risk factors determine which mitigations are necessary

2339 Each vertical standard defines a set of risk factors. The values of these risk factors are determined by the use case and/or
2340 the capabilities of the product. Which mitigations are necessary are determined by a combination of risk factors and
2341 capabilities. Each cybersecurity requirement ends with a table showing which mitigations are required, based on risk
2342 factors and capabilities.

2343 E.4.6 Use cases are grouped into security profiles

2344 Security profiles are use cases grouped together by compatible mitigations. Each security profile describes a set of
2345 mitigations which can be used to satisfy the CRA essential requirements for any use case that is part of the security
2346 profile.

2347 E.4.7 New use cases and security profiles may be contributed

2348 New use cases and security profiles may be developed using existing or new risk assessments, risk factors, and
2349 mitigations. It is in the manufacturer's interest to contribute the risk assessment and mitigations for their use case to the
2350 vertical standard, as they may then get the benefits of conformance via a CRA vertical standard for their product.

2351 E.4.8 Manufacturer may use any CRA-conformant risk assessment 2352 methodology

2353 The risk assessment clause of a vertical standard is informative only. It exists to demonstrate that the standards writers
2354 have undertaken a risk assessment of the product. The manufacturer is explicitly permitted to use any risk assessment
2355 methodology consistent with the essential requirements in the CRA.

2356

2357 **Annex F (informative):**
2358 **Change history**

2359 The "Change history/Change request (history)" annex shall be included in every revised or amended harmonised
2360 standard and shall contain information concerning significant changes that have been introduced by it. It shall be
2361 presented as a table.

Date	Version	Information about changes
<Month year>	<#>	<Changes made are listed in this cell>

2362
2363

2364 History

2365 The following table will automatically be filled in by the ETSI Secretariat.

Document History		
Version	Date	Milestone
	<#>	

2366