

ETSI TS 103 929 V1.1.1 (2023-02)



**Cyber Security (CYBER);
Mapping of specific requirements of standardization request
for RED articles 3(3)(d), 3(3)(e) and 3(3)(f) to IEC 62443-4-2
requirements and to ETSI EN 303 645 provisions**

Reference

DTS/CYBER-0091

Keywords

cyber security

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:
<http://www.etsi.org/standards-search>

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 at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at <https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

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.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

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 2023.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Methodology	7
4.1 Mapping of IEC 62443-4-2 requirements	7
4.2 Mapping of ETSI EN 303 645 provisions.....	8
5 Mapping results and resulting transition requirements	8
5.1 Mapping results based on IEC 62443-4-2 requirements	8
5.2 Mapping results based on ETSI EN 303 645 provisions.....	10
5.3 Transition requirements based on mapping results	11
History	12

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

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

Trademarks

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

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

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

Introduction

According to the standardization request [i.5], harmonised standards (hENs) are to be developed for the articles 3(3)(d), 3(3)(e) and 3(3)(f) of the Radio Equipment Directive (RED) [i.1]. Due to the adoption of the delegated act [i.2], the essential requirements given in the RED articles 3(3)(d), 3(3)(e) and 3(3)(f) will come into force on the 1st of August 2024.

It is understood that requirements from IEC 62443-4-2 [i.4] and the provisions from ETSI EN 303 645 [i.3] address many products that fall under the scope of the RED articles 3(3)(d), 3(3)(e) and 3(3)(f). The ETSI EN 303 645 [i.3] goes even beyond the scope of the RED [i.1] as the ETSI EN 303 645 [i.3] does not only cover product-related requirements, but also process-related requirements addressing the manufacturer.

The present document shows the mapping of specific requirements of the standardization request for the RED articles 3(3)(d), 3(3)(e) and 3(3)(f) to IEC 62443-4-2 [i.4] requirements and to ETSI EN 303 645 [i.3] provisions. This could be useful, e.g. for industry stakeholders to be prepared for/implement the transition from product conformity with IEC 62443-4-2 [i.4] and/or ETSI EN 303 645 [i.3] to product conformity with future requirements in the hENs for the RED articles 3(3)(d), 3(3)(e) and 3(3)(f). In addition, the mapping results could be referenced for work on the hENs for the RED articles 3(3)(d), 3(3)(e) and 3(3)(f).

1 Scope

The present document provides mapping tables to show which security requirements and provisions from the IEC 62443-4-2 [i.4] and the ETSI EN 303 645 [i.3], respectively, cover the specific requirements from the standardization request for the RED articles 3(3)(d), 3(3)(e) and 3(3)(f) and are therefore relevant to fulfil the essential requirements given by the RED articles 3(3)(d), 3(3)(e) and 3(3)(f). In addition, so-called transition requirements are provided which help and are to be considered for implementing the transition from product conformity based on provisions from ETSI EN 303 645 [i.3] and/or requirements from IEC 62443-4-2 [i.4] to product conformity based on the RED Delegated Regulation [i.2].

NOTE: The present document only provides a rough mapping, i.e. only (at least) one of the specific requirements for each RED article 3(3)(d), 3(3)(e) and 3(3)(f) of the standardisation request [i.5] is mapped to each requirement/provision of IEC 62443-4-2 [i.4]/ETSI EN 303 645 [i.3]. A second version of the present document is expected to be published in near future including a detailed mapping, i.e. all specific requirements for each RED article 3(3)(d), 3(3)(e) and 3(3)(f) of the standardisation request [i.5] are mapped to the provisions and requirements of the ETSI EN 303 645 [i.3] and of the IEC 62443-4-2 [i.4], respectively.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found at <https://docbox.etsi.org/Reference>.

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

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

Not applicable.

2.2 Informative references

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

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] Consolidated text: [Directive 2014/53/EU](#) of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Text with EEA relevance).
- [i.2] Commission Delegated [Regulation \(EU\) 2022/30](#) of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive.
- [i.3] ETSI EN 303 645 (V2.1.1) (2020-06): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

- [i.4] IEC 62443-4-2:2019: "Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components".
- [i.5] Commission implementing [Decision of 5.8.2022](#) on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in [i.1], [i.2], [i.3], [i.4], [i.5] and the following apply:

process-related requirement: requirement that is addressed to the process around the product functionality

EXAMPLE: If a standard requires that a product manufacturer provides a publicly available vulnerability disclosure policy, this would be a process-related requirement.

product-related requirement: requirement that is only addressed to the product with its functionality

EXAMPLE: If a standard requires that a product provides authentication and access control mechanisms, this would be a product-related requirement.

transition requirement: requirement that specifies which requirements/provisions of an existing standard/existing standards are to be considered in order to help to perform the transition from being compliant with these requirements/provisions to being compliant with requirements of another standard/other standards

EXAMPLE: If a standard requires that a manufacturer does not consider process-related requirements, but rather product-related requirements from existing cybersecurity standards with the intention to meet the requirements of the upcoming hENs for the RED articles 3(3)(d), 3(3)(e) and 3(3)(f), this would be a transition requirement.

3.2 Symbols

Void.

3.3 Abbreviations

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

EN	European Standard
hEN	harmonised European Standard
IEC	International Electrotechnical Commission
RE	Requirement Enhancement
RED	Radio Equipment Directive

4 Methodology

4.1 Mapping of IEC 62443-4-2 requirements

First, foundational requirements of IEC 62443-4-2 [i.4] are mapped to see whether the foundational requirement is relevant so that the component requirements under this foundational requirement have not to be investigated further if the foundational requirement is not relevant.

Second, component requirements are mapped, in case the foundational requirement is considered as relevant for the coverage of the specific requirements of the standardization request [i.5].

4.2 Mapping of ETSI EN 303 645 provisions

First, the clauses (13 security + data protection requirements) of ETSI EN 303 645 are mapped against the specific requirements of the standardization request [i.3].

Second, all the provisions are evaluated whether they are possibly relevant or not for the essential requirements in the RED articles 3(3)(d), 3(3)(e) and 3(3)(f).

In the EN mapping, the strategy is to focus on the task to assign the provisions the values "relevant", "partly relevant" or "not relevant". More precisely, "relevant" denotes that the provision (partly) meets one specific requirement of the standardisation request [i.5] (with some editorial adaptations); "partly relevant" denotes that the provision has to be technically reworded but would then (partly) meet one specific requirement of the standardisation request [i.5]; "not relevant" denotes that the provision cannot be used to (partly) meet one specific requirement of the standardisation request [i.5]. Therefore, it is enough to show whether a certain provision covers one certain specific requirement to conclude that this certain provision is relevant, partly relevant or not relevant for the corresponding essential requirement given in RED article 3(3)(d), 3(3)(e) or 3(3)(f).

The same mapping methodology has been used to map the IEC 62443-4-2 [i.4] requirements. Since the intention of the mapping of the EN and IEC standards is to declare what provisions/requirements are relevant, it is enough to identify that at least one specific requirement is (partly) met. In such a case it is possible to declare the provision/requirement as "partly relevant" or even "relevant".

5 Mapping results and resulting transition requirements

5.1 Mapping results based on IEC 62443-4-2 requirements

The following notations are used (Relevant? Y-Yes, N-No, P-Partly relevant):

Y	the requirement as written covers at least one specific requirement from the RED article
P	the requirement after modification covers at least one specific requirement from the RED article
N	the requirement does not cover any specific requirements from the RED article

Table 5.1.1: Mapping the essential requirements of the RED articles 3(3)(d), (e) and (f) to the requirements of the IEC 62443-4-2 [i.4] based on the specific requirements of the standardization request [i.5]

IEC 62443-4-2 [i.4] Requirement	RED article		
	3(3)(d)	3(3)(e)	3(3)(f)
1 Identification and authentication control			
1.1 + RE1 + RE2	P	P	P
1.2 + RE1			
1.3			
1.4			
1.5 + RE1			
1.6 + RE1			
1.7 + RE1 + RE2			
1.8	Y	Y	Y
1.9 + RE1			
1.10			
1.11			
1.12	P	P	P
1.13 + RE1			
1.14 + RE1			
2 Use control			
2.1 + RE1 + RE2 + RE3 + RE4	P	P	P
2.2	Y	Y	Y
2.3	N	N	N
2.4 + RE1	Y	Y	Y
2.5	P	P	P
2.6	Y	Y	Y
2.7	P	P	P
2.8			
2.9 + RE1			
2.10			
2.11 + RE1 + RE2			
2.12 + RE1			
2.13 + RE1			
3 System integrity			
3.1 + RE1	P	Y	Y
3.2 + RE1	P	P	P
3.3 + RE1			
3.4 + RE1 + RE2			
3.5	Y	Y	Y
3.6			
3.7			
3.8			
3.9 + RE1	P	P	P
3.10 + RE1	Y	Y	Y
3.11 + RE1			
3.12	P	P	P
3.13			
3.14 + RE1			
4 Data confidentiality			
4.1	P	P	P
4.2 + RE1 + RE2	P	Y	Y
4.3	P	P	P
5 Restricted data flow			
5.1	P	P	P
5.2 + RE1 + RE2 + RE3	Y	Y	Y
5.3			
6 Timely response to events			
6.1 + RE1	P	P	P
6.2			

IEC 62443-4-2 [i.4] Requirement	RED article		
	3(3)(d)	3(3)(e)	3(3)(f)
7 Resource availability			
7.1 + RE1	Y	Y	Y
7.2	P	P	P
7.3 + RE1			
7.4	N	N	N
7.5			
7.6 + RE1	P	P	P
7.7	Y	Y	Y
7.8	N	N	N

5.2 Mapping results based on ETSI EN 303 645 provisions

The following notations are used:

- Y the provision as written covers at least one specific requirement from the RED article
- P the provision after modification covers at least one specific requirement from the RED article
- N the provision does not cover any specific requirements from the RED article

Table 5.2.1: Mapping the essential requirements of the RED articles 3(3)(d), (e) and (f) to the provisions of ETSI EN 303 645 [i.3] based on the specific requirements of the standardization request [i.5]

ETSI EN 303 645 [i.3] Provision	RED article		
	3(3)(d)	3(3)(e)	3(3)(f)
5.1 No universal default passwords			
5.1-1	Y	Y	Y
5.1-2			
5.1-3			
5.1-4			
5.1-5			
5.2 Implement a means to manage reports of vulnerabilities			
5.2-1	N	N	N
5.2-2			
5.2-3			
5.3 Keep software updated			
5.3-1	Y	Y	Y
5.3-2			
5.3-3			
5.3-4	P	P	P
5.3-5			
5.3-6	Y	Y	Y
5.3-7			
5.3-8	N	N	N
5.3-9	P	P	P
5.3-10			
5.3-11	N	N	N
5.3-12	P	P	P
5.3-13	N	N	N
5.3-14			
5.3-15			
5.3-16			
5.4 Securely store sensitive security parameters			
5.4-1	Y	Y	Y
5.4-2			
5.4-3			
5.4-4			

ETSI EN 303 645 [i.3] Provision	RED article		
	3(3)(d)	3(3)(e)	3(3)(f)
5.5 Communicate securely			
5.5-1	P	Y	Y
5.5-2	P	P	P
5.5-3	P	Y	Y
5.5-4	Y	Y	Y
5.5-5	Y	Y	Y
5.5-6	P	Y	Y
5.5-7	P	Y	Y
5.5-8	N	N	N
5.6 Minimize exposed Attack surfaces			
5.6-1	Y	Y	Y
5.6-2			
5.6-3			
5.6-4	P	P	P
5.6-5	Y	P	P
5.6-6			
5.6-7			
5.6-8	N	N	N
5.6-9			
5.7 Ensure software integrity			
5.7-1	P	P	P
5.7-2	Y	Y	Y
5.8 Ensure that personal data is secure			
5.8-1	N	Y	Y
5.8-2			
5.8-3	P	P	P
5.9 Make systems resilient to outages			
5.9-1	Y	P	P
5.9-2			
5.9-3			
5.10 Examine system telemetry data			
5.10-1	P	P	P
5.11 Make it easy for users to delete user data			
5.11-1	N	Y	Y
5.11-2	N	P	P
5.11-3			
5.11-4			
5.12 Make installation and maintenance of devices easy			
5.12-1	Y	P	P
5.12-2	N	N	N
5.12-3			
5.13 Validate input data			
5.13-1	Y	Y	Y

5.3 Transition requirements based on mapping results

To realize the transition from product conformity with requirements and/or provisions of IEC 62443-4-2 [i.4] and ETSI EN 303 645 [i.3], respectively, to product conformity based on the future hENs for the RED articles 3(3)(d), 3(3)(e) and 3(3)(f), the following transition requirements are to be met.

TReq1: Process-related requirements/provisions from IEC 62443-4-2 [i.4]/ETSI EN 303 645 shall not be considered while transitioning, because they are out of the scope of the RED Delegated Regulation [i.2].

TReq2: Product-related requirements/provisions from IEC 62443-4-2 [i.4]/ETSI EN 303 645 [i.3] shall be considered while transitioning for products in the scope of IEC 62443-4-2 [i.4] and ETSI EN 303 645 [i.3], respectively, if the assignment "Y" or "P" has been used in the mapping tables of the present document.

History

Document history		
V1.1.1	February 2023	Publication