ETSI TR 104 012 V1.1.1 (2023-12)

TECHNICAL REPORT

Reconfigurable Radio Systems (RRS);
Feasibility study of the usage of software reconfiguration for Radio Equipment Directive and Proposal for Cyber Resilience Act

Reference

DTR/RRS-0157

Keywords

CRA, radio, RED, RRS, software reconfiguration

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

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

Contents

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 Report (TR) has been produced by ETSI Technical Committee Reconfigurable Radio Systems (RRS).

Modal verbs terminology

In the present document "**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.

Executive summary

The present document analyses the viability of the existing ETSI framework of Software Reconfiguration to address the needs of the Radio Equipment Directive [i.16] and the draft Cyber Resilience Act [i.17] in the context of "Software" updates.

ETSI has published a generalized software reconfiguration approach which enables reconfiguration of radio equipment through software as specified in ETSI EN 303 641 [i.1], ETSI EN 303 648 [i.2], ETSI EN 303 681-1 [i.3], ETSI EN 303 681-2 [i.4], ETSI EN 303 681-3 [i.5], ETSI EN 303 681-4 [i.6] and in support of use cases identified in ETSI TR 103 585 [i.7]; the overall framework is complemented by security solutions in ETSI TS 103 436 [i.14] and the definition of a Radio Application Package [i.15]. The specific case of Mobile Device reconfiguration is addressed in ETSI EN 303 095 [i.8], ETSI EN 303 146-1 [i.9], ETSI EN 303 146-2 [i.10], ETSI EN 303 146-3 [i.11], ETSI EN 303 146-4 [i.12], ETSI TR 103 087 [i.13] and ETSI TS 103 436 [i.14]. The ETSI software reconfiguration framework is a general approach; the upload of software components, including firmware, patches and configuration files is a subset of this framework. The present document is focusing on this sub-set.

The results of the present document indicate that for both cases, i.e. the Radio Equipment Directive and the draft Cyber Resilience Act, the existing ETSI framework of Software Reconfiguration provides a suitable base to meet inherent requirements.

Introduction

ETSI has published a generalized software reconfiguration approach which enables reconfiguration of radio equipment through software as specified in ETSI EN 303 641 [i.1], ETSI EN 303 648 [i.2], ETSI EN 303 681-1 [i.3], ETSI EN 303 681-2 [i.4], ETSI EN 303 681-3 [i.5], ETSI EN 303 681-4 [i.6] and in support of use cases identified in ETSI TR 103 585 [i.7]; the overall framework is complemented by security solutions in ETSI TS 103 436 [i.14] and the definition of a Radio Application Package [i.15]. The specific case of Mobile Device reconfiguration is addressed in ETSI EN 303 095 [i.8], ETSI EN 303 146-1 [i.9], ETSI EN 303 146-2 [i.10], ETSI EN 303 146-3 [i.11], ETSI EN 303 146-4 [i.12], ETSI TR 103 087 [i.13] and ETSI TS 103 436 [i.14]. The ETSI software reconfiguration framework is a general approach; the upload of software components, including firmware, patches and configuration files, is a subset of this framework. The present document is focusing on this sub-set.

The present document analyses the viability of the existing ETSI framework of Software Reconfiguration to address the needs of the Radio Equipment Directive [i.16] and the draft Cyber Resilience Act [i.17] in the context of "Software" updates.

1 Scope

The present document analyses the applicability of available ETSI deliverables on Software Reconfiguration to the implementation of regulation initiatives currently under way, including specifically:

- Radio Equipment Directive Article 3(3)(i) and Article (4) [i.16].

NOTE: One aspect of those Articles relates to the combination of Software and Hardware.

- Cyber Resilience Act [i.17].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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] ETSI EN 303 641 (V1.1.2): "Reconfigurable Radio Systems (RRS); Radio Equipment (RE) reconfiguration requirements".

[i.2] ETSI EN 303 648 (V1.1.2): "Reconfigurable Radio Systems (RRS); Radio Equipment (RE) reconfiguration architecture".

[i.3] ETSI EN 303 681-1 (V1.1.2): "Reconfigurable Radio Systems (RRS); Radio Equipment (RE) information models and protocols for generalized software reconfiguration architecture; Part 1: generalized Multiradio Interface (gMURI)".

[i.4] ETSI EN 303 681-2 (V1.1.2): "Reconfigurable Radio Systems (RRS); Radio Equipment (RE) information models and protocols for generalized software reconfiguration architecture; Part 2: generalized Reconfigurable Radio Frequency Interface (gRRFI)".

[i.5] ETSI EN 303 681-3 (V1.1.2): "Reconfigurable Radio Systems (RRS); Radio Equipment (RE) information models and protocols for generalized software reconfiguration architecture; Part 3: generalized Unified Radio Application Interface (gURAI)".

[i.6] ETSI EN 303 681-4 (V1.1.2): "Reconfigurable Radio Systems (RRS); Radio Equipment (RE) information models and protocols for generalized software reconfiguration architecture; Part 4: generalized Radio Programming Interface (gRPI)".

[i.7] ETSI TR 103 585 (V1.2.1): "Reconfigurable Radio Systems (RRS); Radio Equipment (RE) reconfiguration use cases".

[i.8] ETSI EN 303 095 (V1.3.1): "Reconfigurable Radio Systems (RRS); Radio reconfiguration related architecture for Mobile Devices (MD)".

[i.9] ETSI EN 303 146-1 (V1.3.1): "Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 1: Multiradio Interface (MURI)".

[i.10] ETSI EN 303 146-2 (V1.2.1): "Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 2: Reconfigurable Radio Frequency Interface (RRFI)".

[i.11] ETSI EN 303 146-3 (V1.3.1): "Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 3: Unified Radio Application Interface (URAI)".

[i.12] ETSI EN 303 146-4 (V1.1.2): "Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 4: Radio Programming Interface (RPI)".

[i.13] ETSI TR 103 087 (V1.2.1): "Reconfigurable Radio Systems (RRS); Security related use cases and threats".

[i.14] ETSI TS 103 436 (V1.2.1): "Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios".

[i.15] ETSI TS 103 850 (V1.1.1): "Reconfigurable Radio Systems (RRS); Definition of Radio Application Package".

[i.16] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

[i.17] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, Brussels, 15.9.2022, COM(2022) 454 final, 2022/0272 (COD).

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

CRA	Cyber Resilience Act
RED	Radio Equipment Directive

4 Radio Equipment Directive and Proposal for Cyber Resilience Act

4.1 Radio Equipment Directive

The Radio Equipment Directive (RED) [i.16] establishes a regulatory framework for placing radio equipment on the market.

RED includes "essential requirements" to be fulfilled by any radio equipment in scope. RED was enacted on 11 June 2014 and was applicable as of 13 June 2016.

In the present document, the applicability of available ETSI deliverables is assessed for the context of the following RED Articles [i.16]:

Article 3

Essential Requirements

…

3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

…

(i) radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated.

…

Article 4

Provision of information on the compliance of combinations of radio equipment and software

1. Manufacturers of radio equipment and of software allowing radio equipment to be used as intended shall provide the Member States and the Commission with information on the compliance of intended combinations of radio equipment and software with the essential requirements set out in Article 3. Such information shall result from a conformity assessment carried out in accordance with Article 17, and shall be given in the form of a statement of compliance which includes the elements set out in Annex VI. Depending on the specific combinations of radio equipment and software, the information shall precisely identify the radio equipment and the software which have been assessed, and it shall be continuously updated.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 44 specifying which categories or classes of radio equipment are concerned by the requirement set out in paragraph 1 of this Article.

3. The Commission shall adopt implementing acts laying down the operational rules for making the information on compliance available for the categories and classes specified by the delegated acts adopted pursuant to paragraph 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 45(3).

4.2 Cyber Resilience Act

When the present document was created, the Cyber Resilience Act (CRA) was available as a draft [i.17]:

This proposed Regulation lays down (a) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products; (b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity; (c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes; (d) rules on market surveillance and enforcement of the above-mentioned rules and requirements. The proposed Regulation will apply to all products with digital elements whose intended and reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.

It is noted, that the CRA specifically addresses software updates including security updates [i.17]:

…, to ensure, among others, appropriate information on security support and provision of security updates.

In the present document, the applicability of available ETSI deliverables is assessed for the specific context of such software updates including security updates.

5 Introduction to existing ETSI framework for Software Reconfiguration

ETSI has published a generalized software reconfiguration approach which enables reconfiguration of radio equipment through software as specified in ETSI EN 303 641 [i.1], ETSI EN 303 648 [i.2], ETSI EN 303 681-1 [i.3], ETSI EN 303 681-2 [i.4], ETSI EN 303 681-3 [i.5], ETSI EN 303 681-4 [i.6] and in support of use cases identified in ETSI TR 103 585 [i.7]; the overall framework is complemented by security solutions in ETSI TS 103 436 [i.14] and the definition of a Radio Application Package [i.15]. The specific case of Mobile Device reconfiguration is addressed in ETSI EN 303 095 [i.8], ETSI EN 303 146-1 [i.9], ETSI EN 303 146-2 [i.10], ETSI EN 303 146-3 [i.11], ETSI EN 303 146-4 [i.12], ETSI TR 103 087 [i.13] and ETSI TS 103 436 [i.14]. The solutions have been designed from a holistic perspective with an emphasis on the needs of commercial equipment, addressing:

- Technical requirements (such as code portability and efficiency).
- Security requirements (such as security delivery and installation of software components).
- Regulatory requirements (such as technical solutions for re-certification of platforms when radio characteristics are modified).

Reconfiguration can be performed on an individual level (e.g. users choosing among new features for their respective component) or en-masse (e.g. automatic upgrade of all platforms).

Specific attention is given to security requirements, addressing in particular:

- Proof of conformance of the radio platform and radio applications to the regulatory Declaration of Conformity, considering that the set of installed radio applications can change over time.
- Proof of the integrity of radio applications.
- Proof of the identity of the developer of radio applications.
- Built-in support for security updates.
- Prevention of code theft.

6 Applicability of ETSI framework of Software Reconfiguration

6.1 Radio Equipment Directive

As detailed in clause 4.1 of the present document, RED Article 3(3)(i) requires that:

- *radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated.*

In order to address the requirement, the following assumptions are taken in the present document:

- "Software" is being considered which affecting essential requirements as defined by RED Article 3(1), Article 3(2) and applicable requirements of Article 3(3).
- Only authorized "Software" is accepted by a target radio equipment, other "Software" is rejected.

Under the upper assumptions, the main challenge relates to the secure delivery of the "Software" to the target radio equipment, where it is verified and installed in case that all requirements are being met (typically including the validation of the origin of the "Software" and the verification of the integrity of the "Software").

Within this context, relevant security threats are identified and assessed in ETSI TR 103 087 [i.13] (Reconfigurable Radio Systems (RRS); Security related use cases and threats in Reconfigurable Radio Systems). Security requirements to be met by a target radio equipment are subsequently derived in ETSI TS 103 436 [i.14] (Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios).

The ETSI framework for Software Reconfiguration as summarized in clause 5 of the present document provides a suitable base to address the above mentioned requirements.

6.2 Cyber Resilience Act (CRA)

As discussed in clause 4.2 of the present document, the CRA may include requirements related to "*providing security updates*", especially to "*address and remediate vulnerabilities without delay*".

The same conclusions as given above for RED also apply for any "Software" based security updates in the context of the CRA. Thus, the ETSI framework for Software Reconfiguration as summarized in clause 5 of the present document provides a suitable base to address the above mentioned requirements.

7 Conclusion

The present document identifies requirements relating to "Software" updates in the Radio Equipment Directive and the Proposal for a Cyber Resilience Act.

In both cases, for the Radio Equipment Directive and the Proposal for a Cyber Resilience Act, the existing ETSI framework of Software Reconfiguration provides a suitable base to meet inherent requirements: ETSI has published a generalized software reconfiguration approach which enables reconfiguration of radio equipment through software as specified in ETSI EN 303 641 [i.1], ETSI EN 303 648 [i.2], ETSI EN 303 681-1 [i.3], ETSI EN 303 681-2 [i.4], ETSI EN 303 681-3 [i.5], ETSI EN 303 681-4 [i.6] and in support of use cases identified in ETSI TR 103 585 [i.7]; the overall framework is complemented by security solutions in ETSI TS 103 436 [i.14] and the definition of a Radio Application Package [i.15]. The specific case of Mobile Device reconfiguration is addressed in ETSI EN 303 095 [i.8], ETSI EN 303 146-1 [i.9], ETSI EN 303 146-2 [i.10], ETSI EN 303 146-3 [i.11], ETSI EN 303 146-4 [i.12], ETSI TR 103 087 [i.13] and ETSI TS 103 436 [i.14]. The ETSI software reconfiguration framework is a general approach; the upload of software components, including firmware, patches and configuration files, is a subset of this framework. The present document is focusing on this sub-set.

The results of the present study indicate that for both cases, i.e. the Radio Equipment Directive and the Proposal for a Cyber Resilience Act, the existing ETSI framework of Software Reconfiguration provides a suitable base to meet inherent requirements.

History

Document history		
V1.1.1	December 2023	Publication