ETSI White Paper No. #38

# Software Radio Reconfiguration:

## A modular Software Reconfiguration approach for radio equipment in general

1st Edition – September 2020

ISBN No. 979-10-92620-33-3

**Authors:**

**Markus Mueck, Seungwon Choi, Vladimir Ivanov, Heungseop Ahn, Zhongfeng Zhang, Daejin Kim, Francois Ambrosini, Scott Cadzow, Isabelle Siaud, Paul Bender, Ben Smith, Wolfgang Krammer, Adrian Minder, Marcello Pagnozzi, Michael Gundlach**

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

# About the authors

**Dr. Markus Mueck**
*INTEL Deutschland GmbH, Germany, Email: Markus.Dominik.Mueck@intel.com*

**Prof. Seungwon Choi**
*Hanyang University, Korea, Email: choi@dsplab.hanyang.ac.kr*

**Dr. Vladimir Ivanov**
*State University of Aerospace Instrumentation, Russia, Email: vnvvldmr0@gmail.com*

**Heungseop Ahn**
*Hanyang University, Korea, Email: ahs90@dsplab.hanyang.ac.kr*

**Zhongfeng Zhang**
*Hanyang University, Korea, Email: zhongfeng.zhang@dsplab.hanyang.ac.kr*

**Daejin Kim**
*Hanyang University, Korea, Email: kdj317@dsplab.hanyang.ac.kr*

**Francois Ambrosini**
*IBIT Ambrosini UG, Germany, Email : francois.ambrosini@famb.info*

**Scott Cadzow**
*Cadzow Communications Consulting Ltd, United Kingdom, Email: scott@cadzow.com*

**Isabelle Siaud**
*b<>com, France, Email : isabelle.siaud@orange.com*

**Paul Bender**
*Bundesnetzagentur, Germany, Email : Paul.Bender@BNetzA.de*

**Ben Smith**
*Radiocommunications Agency Netherlands, Email: ben.smith@agentschaptelecom.nl*

**Wolfgang Krammer**
*Federal Ministry of Agriculture, Regions and Tourism, Austria, Email: Wolfgang.Krammer@bmlrt.gv.at*

**Adrian Minder**
*OFCOM Switzerland, Email: Adrian.Minder@bakom.admin.ch*

**Marcello Pagnozzi**
*ETSI, France, Email: marcello.pagnozzi@etsi.org*

**Michael Gundlach**
NOKIA, Germany, Email: michael.gundlach@nokia.com

# Contents

# Executive Summary

The **generalized** ETSI software reconfiguration approach enables reconfiguration of radio equipment through software as specified in EN 303 641 [1], EN 303 648 [2], EN 303 681-1 [3], EN 303 681-2 [4], [5], EN 303 681-4 [6] and in support of use cases identified in TR 103 585 [7]; the overall framework is complemented by security solutions in TS 103 436 [15]. The specific case of Mobile Device reconfiguration is addressed in EN 303 095 [9], EN 303 146-1 [10], EN 303 146-2 [11], [12], EN 303 146-4 [13], TR 103 087 [14] and TS 103 436 [15]. 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-mass (e.g., automatic upgrade of all platforms).

The ETSI solution is also tailored to the needs of the Radio Equipment Directive [16] which includes articles on software reconfiguration.

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.

Moving from today's hardware design principles to software reconfiguration solutions will require a paradigm change which cannot happen in a single step. The ETSI solution has thus been designed to allow for a gradual approach proceeding step-by-step:

- In a first-generation implementation, the functionality may be limited to a replacement of specific (hardwired) components by executable software, designed specifically for a given target platform. Features such as secure delivery of software components and installation will be sufficient to address this need. Hardware resources (such as FPGA resources) are typically added to the original design to enable the replacement.
- Second generation solutions may furthermore build on the ETSI solution to design portable and yet highly (power) efficient code thanks to the Radio Virtual Machine[1] principle.

[1] A Radio Virtual Machine corresponds to an abstract representation of a radio algorithm (note that this is different from other virtual machine concepts as generally applied in the computer science and Information Technology context).

- Furthermore, the level of autonomy of the platform may evolve over time, including distributed selection of the most relevant features and dynamic replacement of corresponding software components.

With the above features, the ETSI software reconfiguration solution is perfectly suited to meet the requirements of 5G and beyond applications. For example, it will enable automotive communication platforms to remain relevant over the lifetime of a vehicle and to address platform vulnerabilities which may arise over the lifetime of a vehicle, enable product adaptation to specific market needs for Internet of Things solutions, etc.

# 1 Use Cases for Software Radio Reconfiguration

The generalized ETSI software reconfiguration approach given in EN 303 641 [1], EN 303 648 [2], ETSI EN 303 681-1 to EN 303 681-4 [3][4][5][6], can be applied to a variety of use cases in which there is a need to reconfigure radio equipment through software. In this section, we briefly introduce some potential use cases based on generalized ETSI software reconfiguration approach.

## 1.1 Use Case 1 – Smartphone Reconfiguration

In today's world, the usage of smartphone apps is ubiquitous. These applications, however, typically provide new tools or games to the end-user without altering any radio parameters. The ETSI software reconfiguration solution provides a framework for introducing *RadioApps*, i.e. applications which extend or modify existing radio features and define solutions for technical, certification and security needs.

Such *RadioApps* will be used to optimize the operation of a smartphone i) in general or ii) for usage in a specific market with special needs. In a typical example of case i) *RadioApps* will be used to optimize the operation of a smartphone in response to the introduction of new features on the network side as they evolve in future releases of the 3GPP standard. In addition, the optimum configuration is identified (e.g., new power-efficient modulation and coding schemes, etc.) to meet power efficiency (see Green-oriented multi-techno link adaptation metrics for 5G heterogeneous networks [21]), predictable QoS and other requirements. To give an example of case ii), in an industrial environment, new mechanisms may be added through software reconfiguration taking the specific characteristics of the usage environment into account. Beyond the provisioning of additional modules, the ETSI framework also allows for the replacement of entire RATs in cases where sufficient computational resources are available.

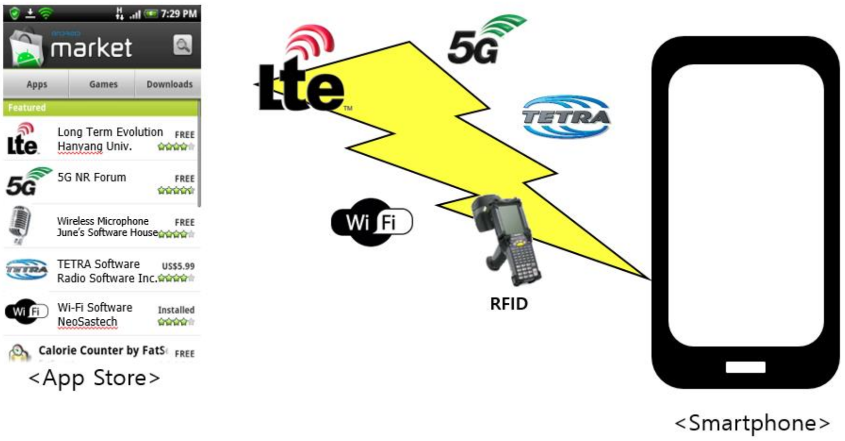


**Figure 1: Smartphone reconfiguration**

## 1,2 Use Case 2 – Automotive Applications

Automotive communication is currently a key trend in the industry. Solutions for Vehicle-to-Everything (V2X) communications, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), etc., are currently being developed with the objective to guarantee a safe(r) driving environment for the future. The challenge is to ensure that a radio communications component remains relevant over the entire lifetime of a vehicle, i.e. ten years and beyond. It is almost certain that a V2X framework feature-set will evolve within this period. Software reconfiguration will enable manufacturers to replace specific software and thus maintain related feature-sets up to date without requiring changes to the hardware. This approach reduces the overall cost for change since a vehicle does not need to be upgraded by an authorized dealer (as it would be required for hardware changes), but the process is handled through over-the-air remote control.

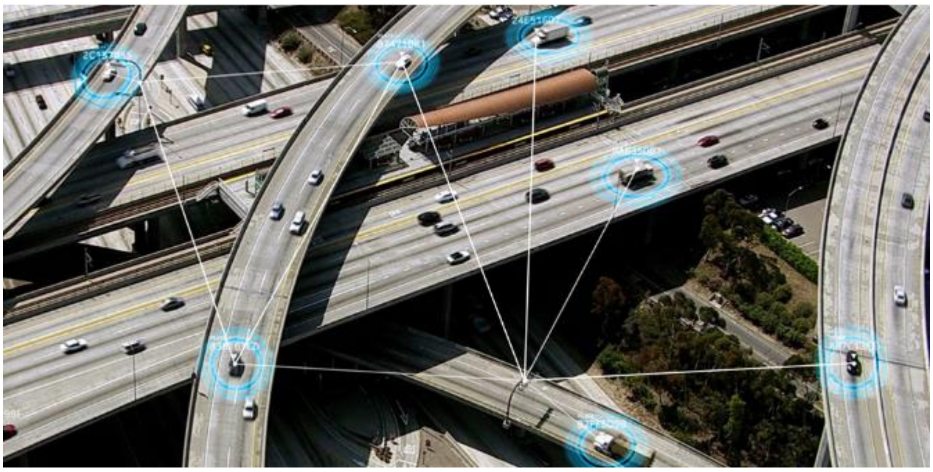


**Figure 2: Automotive Applications**

## 1.3 Use Case 3 – Radio Access Network (RAN) Reconfiguration

With the evolution of wireless standards, network functions need to be updated. In this use case, the installation of *RadioApps* can be used to provide updated or new features which address the radio characteristics of the network. Network functions are distributed across a variety of physical entities which all require dedicated software updates for the provisioning of a specific new service.

Typically, such equipment is then further connected to a larger network, for example through wireless or cabled backbone network access. In this use case, the network operator is able to alter or extend the functionalities of this equipment through installation of suitable *RadioApps*.

## 1.4 Use Case 4 – Internet-of-Things Device Reconfiguration

Future IoT devices, including 5G and beyond, will address a substantial variety of use cases, encompassing for example gaming, voice communication, medical applications, industrial automation, etc. Each such application has its particular needs in terms of features, form factors, etc. Due to quasi-infinite possibilities, it is unlikely that chipmakers will offer tailored components for each application. Rather, a limited number of generic and reconfigurable components will be made available which are suitably tailored to the target market through software components. The ETSI software reconfiguration solution provides a suitable ecosystem to support the future IoT market needs.

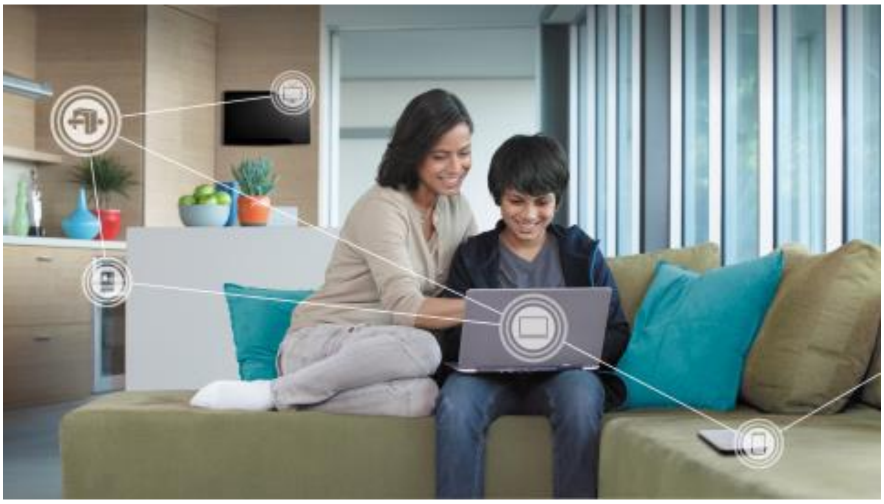


Figure 3: Software reconfiguration enabling Internet-of-Things

## 1.5 Use Case 5 – Radio Reconfiguration through an external Component (e.g., USB Stick)

This use case concerns standalone radio external components that embed all the capabilities necessary to radio processing. The host device is not involved in radio processing but may configure operational parameters as allowed by the external component (e.g., a USB Stick). Thus, the separation between the host device and the external component is clear and embodied by the physical interface between the two. On the host device, only a device driver is necessary to operate the external component and integrate it into the networking stack. In order to reconfigure the external component, the host device may be used as a staging area to store Radio Applications which are then loaded on the external component via the device driver (e.g. the device driver may leverage the Administrator).

## 1.6 Use Case 6 – Reconfigurable Satellite Telecom Payload

The lifetime of satellites varies from a few years for Low Earth Orbiting (LEO) satellites until 10 or even 15 years for Geostationary Earth Orbit (GEO) satellites. This fact and the rapid progress in the field of digital communications raise the problem of technological obsolescence of onboard telecom payload. The emergence of new signal processing algorithms and new standards that provide reliable and high-speed transmission of information requires the reconfiguration of the onboard equipment. Satellite communication systems are considered as a part of the global network infrastructure with the integrated satellite segment. Therefore, they should be provisioned within the same management framework as the terrestrial segment, including the management approach for radio software reconfiguration.

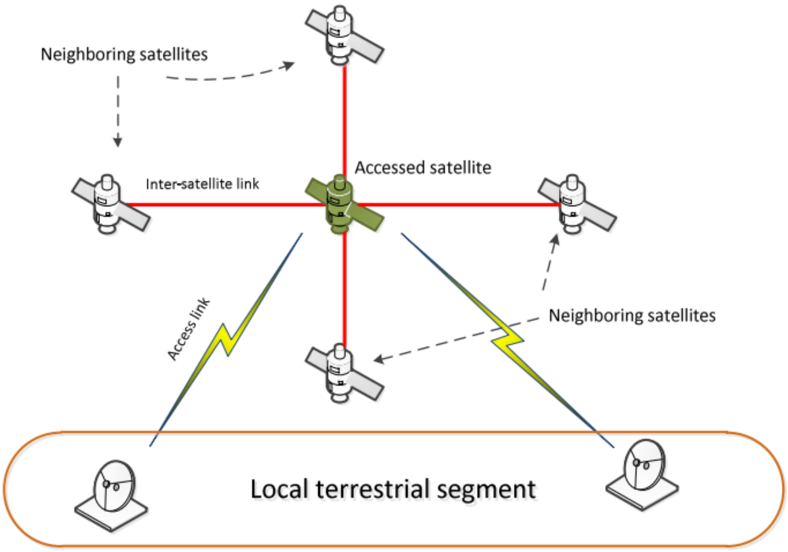


**Figure 4: Software reconfiguration enabling satellite telecom payload**

## 1.7 Use Case 7 – Bug-fix and Security Updates

Bug-fixes and security updates are essential to the maintenance of software, and as such also for a Radio Application throughout its lifecycle. Bug-fixes help ensure that Radio Applications will behave according to specification even after the Radio Application has been installed on a device.

Security updates help ensure the integrity of an implementation. Application security is an evolving field and implementations believed to be secure at some point in time may later become insecure as new attack methods are devised.

## 1.8 Use Case 8 – Medical Applications

Medical applications, such as remote surgery, monitoring of patient's life support data, etc. require highly reliable and stable communication systems. Still, software reconfiguration is expected to be broadly applied in order to enable users to have access to latest software updates and best possible functionalities. For example, in this context it is of specific importance to immediately remedy any incorrect behavior or security vulnerabilities in order to ensure a maximum level of protection.

# 2 The ETSI Software Reconfiguration Solution

ETSI has developed a general Radio Equipment software reconfiguration solution in EN 303 641 [1], EN 303 648 [2], ETSI EN 303 681-1 to EN 303 681-4 [3][4][5][6], as well as a specific instantiation for Mobile Devices in EN 303 095 [9], EN 303 146-1 to EN 303 146-4 [10] to [13], TR 103 087 [14] and TS 103 436 [15], addressing, among others, the specific needs of the use cases introduced above. In this section, some of the key challenges are presented together with indications how they are addressed by the ETSI solution.

## 2.1 Problem Statement 1: How to transfer and install radio software components to a target platform in a secure way?

The ETSI software reconfiguration solution introduces a multitude of features. While the overall solution supports implementations of extended capabilities, a sub-set of these features (see EN 303 681-1 [10]) is sufficient to provide the possibility i) to load novel software components to a target platform, ii) to install and execute and iii) to uninstall such components in a secure way (see TR 103 087 [14] and TS 103 436 [15]).

## 2.2 Problem Statement 2: How to enable a user to access to new software components?

The ETSI software reconfiguration solution supports a so-called *RadioApp Store*, i.e. an entity which offers access to a selection of radio software components. A user is able to access this store, to identify all available software components and finally to download and install any selected component. Only those software components will be made visible to the User which have been previously tested and validated and which are included in the Declaration of Conformity (DoC) of the target platform.

Beyond the individual download of *RadioApps*, the ETSI approach also allows for an en-mass deployment, i.e. upgrading all concerned devices of a given type.

## 2.3 Problem Statement 3: How to deal with device certification in the context of novel radio software components?

The ETSI software reconfiguration solution allows for the installation of new software components which alter the radio behavior of a target platform. A continued operation is only possible if the modified platform has been tested and validated and a Declaration of Conformity (DoC) is made available by the responsible party (i.e. the manufacturer) which comprises the combination of the hardware and the new software components.

## 2.4 Problem Statement 4: How to achieve software portability and execution efficiency?

The ETSI software reconfiguration solution addresses the problem of how to make software portable to a multitude of distinct target platforms, such as smartphones of different manufacturers, etc. The ETSI software reconfiguration solution introduces an efficient abstraction method based on a radio virtual machine approach which first creates a generic representation of a radio algorithm which, in a second step, is optimized for the target platform. The ETSI approach thus inherently provides high execution efficiency by omitting a middleware (as employed by the Software Communications Architecture (see SOFTWARE COMMUNICATIONS ARCHITECTURE SPECIFICATION [19] and SOFTWARE COMMUNICATIONS ARCHITECTURE SPECIFICATION USER'S GUIDE [20] for example).

## 2.5 Problem Statement 5: How to enable a gradual evolution towards software reconfigurability?

Legacy software reconfiguration solutions typically assume that entire Radio Access Technologies (RATs) are being loaded through software onto a target platform. The ETSI software reconfiguration solution does not require that an entire application is replaced. Rather, the ETSI solution allows for a gradual replacement or re-parameterization of selected (hardwired) components. The particular components being available for replacement by software components are chosen by a manufacturer and this selection can be modified over time. I.e., the manufacturer is able to manage the level of reconfigurability of the platform in a gradual and controlled way.

# 3 ETSI Software Reconfiguration Architecture and differences to State-of-the-Art solutions

The ETSI software reconfiguration solution has been specifically designed for the needs of commercial mass-market devices and thus differs from other state-of-the-art approaches whose target markets lie in different domains (such as military, etc.). In this section, we comment on the key differences and introduce the ETSI architecture. The next section will introduce further technical details.

## 3.1 Legacy approach to software reconfiguration

A multitude of software radio reconfiguration approaches exist. Among these, the Software Communication Architecture (SCA) [19] is a very prominent solution. The SCA is published by the Joint Tactical Networking Center (JTNC) in support of the United States Department of Defense. The key fundamental feature of the SCA is that entire Radio Access Technologies (RATs) – or *Waveforms*, as they are called in the military domain - are separated and isolated by middleware from specific radio hardware of implementations.

While the specific features of the SCA are perfectly suited to specific markets, such as military, commercial mass market products have different requirements. To give an example, commercial equipment typically applies a joint optimization of hardware and software which is the main source of efficiency for embedded devices; since SCA middleware separates and isolates software from hardware, this joint optimization approach cannot be applied.

## 3.2 The ETSI Technical Approach to Software Reconfiguration

The ETSI approach applies novel design principles in order to address needs of commercial mass market equipment such as execution efficiency, software portability (in particular due to the radio virtual machine approach), etc.

Taking into account the lessons learned from legacy approaches for software reconfiguration, ETSI decided to apply the following basic principles:

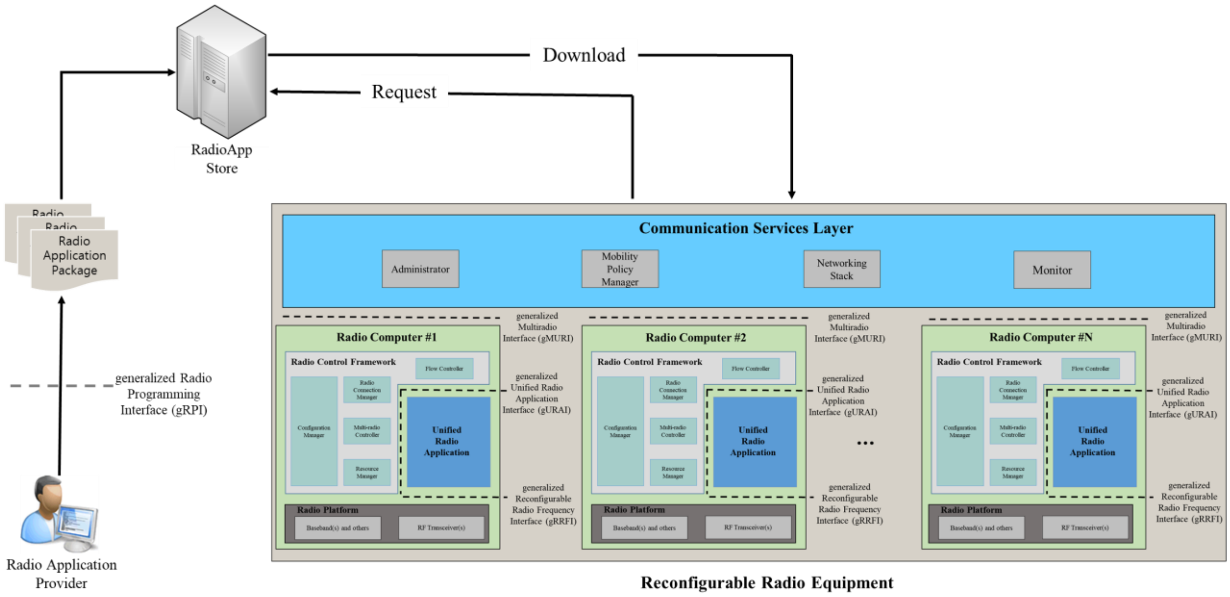
- Apply a modular approach – i.e., to support the replacement of specific platform components, enabling a gradual update of radio features over time. It is up to the manufacturer to define which components may be replaced and thus the level of reconfigurability of a platform can be managed efficiently and evolve.

- Define a generic but yet efficient way to create portable software – i.e., to adopt, instead of a middleware, a novel radio virtual machine-based approach (creating an abstract representation of a radio algorithm) which allows an efficient porting to any specific target platform.

It is expected that the above principles will serve as a successful framework for commercial mass market applications.

## 3.3 ETSI software reconfiguration eco-System and architecture

Figure 5 illustrates the reconfigurable radio equipment architecture and related interfaces enabling software reconfiguration.



Download
Request
RadioApp Store
Radio
Radio
Radio Application Package
generalized Radio Programming Interface (gRPI)
Radio Application Provider
Communication Services Layer
Administrator
Mobility Policy Manager
Networking Stack
Monitor
generalized Multiradio Interface (gMURI)
Radio Computer #1
Radio Control Framework
Flow Controller
Radio Connection Manager
Configuration Manager
Multi-radio Controller
Resource Manager
Unified Radio Application
Radio Platform
Baseband(s) and others
RF Transceiver(s)
generalized Unified Radio Application Interface (gURAI)
generalized Reconfigurable Radio Frequency Interface (gRRFI)
Radio Computer #2
…
Radio Computer #N
Reconfigurable Radio Equipment

**Figure 5: Standard reconfigurable radio equipment architecture and related interfaces**

As outlined in further detail in EN 303 648 [9], a reconfigurable radio equipment may include one or more radio computers for supporting distributed computations. For the specific case of Mobile Device Reconfiguration as given in EN 303 095 [9], EN 303 146-1 to EN 303 146-4 [10] to [13], TR 103 087 [14] and TS 103 436 [15], only a single Radio Computer is used in the target platform.

For each radio computer, it can execute the Radio Application (RA) code consisting of various functional blocks of which the granularities might be all different depending upon hardware platform vendors – depending on the features provided by radio equipment manufacturers, the (3rd party) software manufacturer develops the entire or partial RA code using the standard programming interfaces as depicted in Figure 5. A modular software approach is applied in order to maximize the reusability of software components. The evolution of RATs can be supported by adding and/or replacing the functional blocks on a given hardware platform.

Note that the target platform provides several layers:

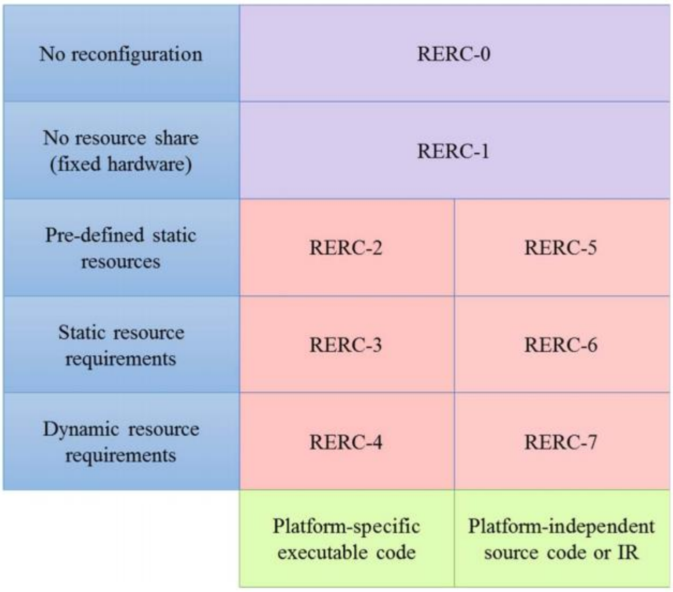
- The Communication Services Layer (CSL) introduces functionalities for the (de-)installation, selection and configuration of software components and the management of the data flows (see EN 303 648 [9]).
- The Radio Control Framework (RCF) manages the actual software execution through a number of functionalities which are introduced in EN 303 648 [9].
- The Unified Radio Application (URA) represents the software downloaded and installed onto the target platform as in EN 303 648 [9].
- The interfaces between the different layers are defined in EN 303 681-1 to EN 303 681-4 [10], [11], [12] and [13].

# 4 How the ETSI solution addresses specific challenges

As illustrated above, ETSI has defined a software reconfiguration approach comprising an entire ecosystem including technical, regulation and security solutions, standardized in EN 303 641 [1], EN 303 648 [2], EN 303 681-1 to EN 303 681-4 [3] to [6], EN 303 681-2 [4], [5], EN 303 681-4 [6], TR 103 585 [7] and EN 302 969 [8]. Following the high-level introduction in previous sections, further technical details are now presented in order to explain how the solution addresses specific challenges.

## 4.1 How to address a gradual increase of platform flexibility over time

Software reconfiguration represents a new paradigm in radio equipment design, and it will take time until a fully flexible, highly efficient platform will finally be commercially available. Rather, it is expected that a gradual increase in flexibility will be applied. For this purpose, ETSI has defined so-called Radio Equipment Reconfiguration Classes (RERCs) in EN 303 641 [1] as illustrated in Figure 6. The objective is to have a clear definition of the capabilities of a specific platform in order to address technical, certification and security issues. These may indeed differ between the various RERCs. While the exact definitions of RERCs are given in EN 303 641 [1], examples are used below in order to facilitate the basic understanding.



| | | |
|---|---|---|
| No reconfiguration | RERC-0 | |
| No resource share (fixed hardware) | RERC-1 | |
| Pre-defined static resources | RERC-2 | RERC-5 |
| Static resource requirements | RERC-3 | RERC-6 |
| Dynamic resource requirements | RERC-4 | RERC-7 |
| | Platform-specific executable code | Platform-independent source code or IR |

**Figure 6: Radio Equipment Reconfiguration Classes**

RERC-0 (No reconfiguration) and RERC-1 (No resource share – fixed hardware) represent today’s commercial equipment. RERC-0 does not support any reconfiguration at all and thus corresponds, for example, to a legacy WiFi modem which cannot be switched to any other RAT. RERC-1 still relies on fixed hardware implementations (e.g., ASIC type of chip designs, usage of static software, etc.); however, this reconfiguration class allows the switching between multiple distinct RATs and/or to operate a multitude of RATs simultaneously.

RERC-2 to RERC-7 represent classes which enable software radio reconfiguration. Two columns are introduced in order to differentiate between two types of code: either platform-specific executable code (to be used on the target platform as-is) is provided or platform-independent source code or Intermediate Representation (IR) code (which is further processed on the target platform, e.g. through back-end compilation, before execution) is provided.

In the pre-defined static resources case (RERC-2 and RERC-5), any software component has a fixed allocation to specific computational resources, e.g. a specific DSP among multiple DSPs is pre-defined for the code execution during compile time. This approach is advantageous from a certification and testing perspective, since the final configuration is identical every time the equipment is used.

For static resource requirements (RERC-3 and RERC-6), resource requirements are defined in a fixed way during design time, e.g. the need for a dedicated DSP for a piece of code may be identified. However, the specific DSP to be selected for the code execution is only identified during the installation of the corresponding software component and may thus differ each time the equipment is used.

In the final stage, called dynamic resource requirements (RERC-4 and RERC-7), any software component is dynamically mapped to any available computational resource during run time. This approach typically leads to the highest level of efficiency, but also implies a highly unpredictable configuration of the equipment.

Note that the ETSI software reconfiguration approach allows a gradual, stepwise approach to software reconfiguration. In a first step, for example, the manufacturer may choose to add spare computational resources (e.g., FPGA resources, etc.) to a hardwired (ASIC) implementation; whenever required, some selected hardwired components can be replaced through software updates. In the future, a platform may employ more and more software-based components; consequently, it offers further post-sale reconfiguration capabilities.

## 4.2 ETSI Security Framework: Security for Software Reconfiguration

The ETSI security framework for Software Reconfiguration (see TR 103 087 [14] and TS 103 436 [15]) applies the traditional thinking of the Confidentiality Integrity Availability paradigm to assuring proper behaviour of the radio equipment, providing tools for

- secure deployment of the technology,
- assisting the users and developers in the avoidance of fraud, and
- supporting developers in proving conformance to the regulatory framework in which the equipment operates.

Three assets are identified:

- the Radio Application;
- the RE Configuration Policy which can be used in managing the (re)configuration of the equipment; and,
- the Declaration of Conformity (DoC) which is a document with legal value.

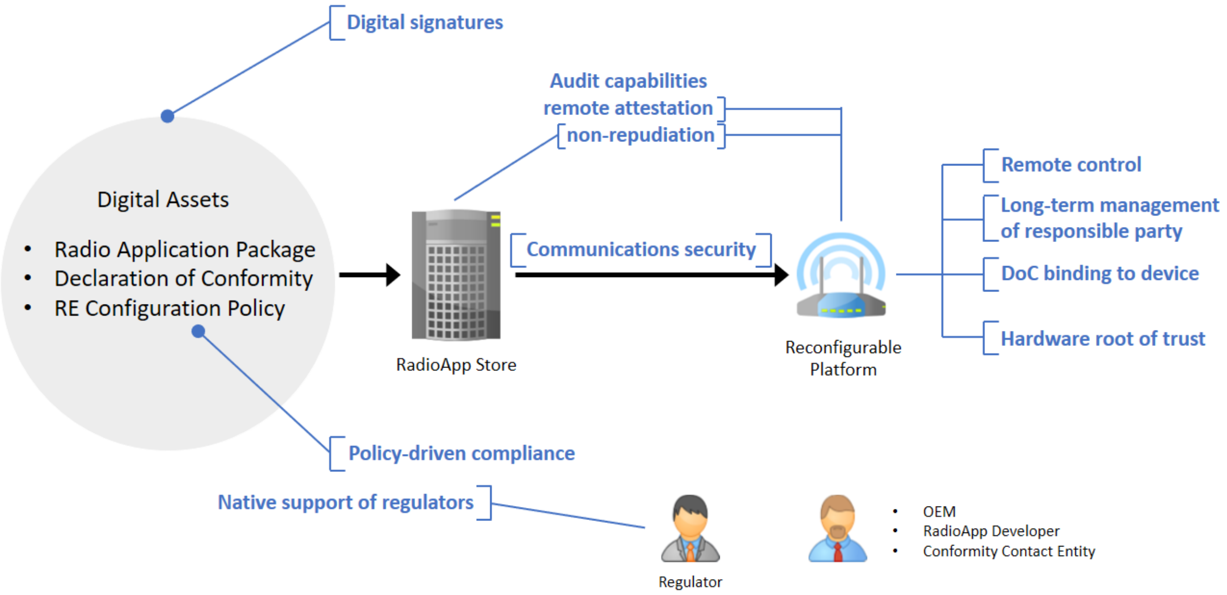


**Figure 7: Security measures for the ETSI Software Reconfiguration framework**

The role of security countermeasures is to defend the system against attack. The nature of attacks against a Reconfigurable Radio have been assumed to leverage the mutability of the platform where the wireless connectivity options of the platform are designed to be modifiable over time. A precursor for allowing radio applications to be installed is to have the base platform itself be secure, to act as a root of trust and security. The rationale being to build on firm foundations (not to build on sand) and to make a strong binding of application to the root of trust thus extending security in depth through the evolving platform.

The installation of purposefully misbehaving Radio Applications and other malicious assets is among the greatest threats to the security of the radio equipment and of the users. There is a risk that legitimate Radio Applications are not used properly, e.g. in the context of a user trying to bypass a hardware or policy-based limitation or in the context of device counterfeit. Additionally, an attacker may attempt to seize control of the equipment by taking advantage of a security vulnerability.

The overall architecture to achieve the security goals for RRS is that of a multi-party digital signature scheme complemented with a non-repudiation scheme with entities in the system delivering cryptographically sealed and identified proof that actions have been taken to assure the operation of the value chain (for example, that conformance testing took place), and to make that proof available to authorized and trusted 3rd parties. The result of application of the above measures is that there is assurance that the platform and its applications will work securely against threats of manipulation, masquerade of any of the actors, and against regulatory bypass.

The trusted 3rd parties can be the equipment manufacturer and network operators, for example. Regulatory bodies are natively supported as actors of the framework, which they can leverage to implement market surveillance and disturbance control.

Further extensions to the RRS security model have been developed that extend the scope of these proofs to allow for remote attestation of the radio (to ensure that only allowed radio applications exist on the RRS platform); furthermore, they give high assurance of the correct behaviour of radio applications. The model has provisions for a hardware root of trust, giving assurance of the Software Reconfiguration platform integrity to the highest possible industry standards. Remote control and long-term management features complement the model so that radio technology evolution and management are securely handled within the RRS framework.

To summarize, the security measures to address these threats in the ETSI Software Reconfiguration framework are as follows:

- Proof of the integrity of the Radio Applications, RE Configuration Policy and Declaration of Conformity;
- Proof of the identity of the developer of Radio Applications, the issuer of the RE Configuration Policy, and the issuer of the Declaration of Conformity;
- Prevention of an asset installation when the asset is not provided by a legitimate actor;
- Use of the reconfiguration feature as a security update mechanism;
- Proof of conformance of the radio platform and radio application to the regulatory Declaration of Conformity, considering that the set of installed radio applications can change over time;
- Prevention of illegitimate use of the Declaration of Conformity (in particular against counterfeit);
- Audit functionalities including a non-repudiation framework and remote attestation;

- Long-term management framework (e.g., transition of equipment responsibility from one manufacturer to another);
- Prevention of masquerade of stakeholders in the RRS value chain;
- Prevention of code theft; and,
- Supply chain integrity and assurance (which underpins all of the above measures).

## 4.3 ETSI approach towards execution efficiency and software portability – Radio Virtual Machine

The ETSI software reconfiguration solution is specifically designed for the requirements of commercial mass market equipment. In order to achieve high efficiency in terms of power consumption and computational complexity, ETSI has defined a highly innovative approach based on a Radio Virtual Machine (RVM) concept (see EN 303 681-4 [13]). The RVM abstracts the Radio Application (RA) code generated with the ETSI-standardized programming interfaces in such a way that the software code can be executed directly (i.e., no middleware is required) on any hardware platform compliant with the ETSI software reconfiguration framework.

For software portability, figure 8 illustrates a conceptual diagram showing how the RA code is abstracted through the RVM to be ported onto different hardware platforms. In this specific example, the RA code is made available to M different hardware platforms through the RVM.

As shown in the right side of figure 8, the RVM includes Data Objects (DOs) for data abstraction, Abstract Processing Elements (APEs) for computational element abstraction, and Abstract Switch Fabric (ASF) for switching the DOs and APEs. The RVM is indeed an abstract machine which abstracts the RA code for a given hardware platform. Therefore, the RVM allows the conversion of a given software component into a generic representation (as a result of front-end compilation) which is then optimized for the specific hardware resources available on a target platform (as a result of back-end compilation). Software developers are able to create software components without considering particular modem hardware details.

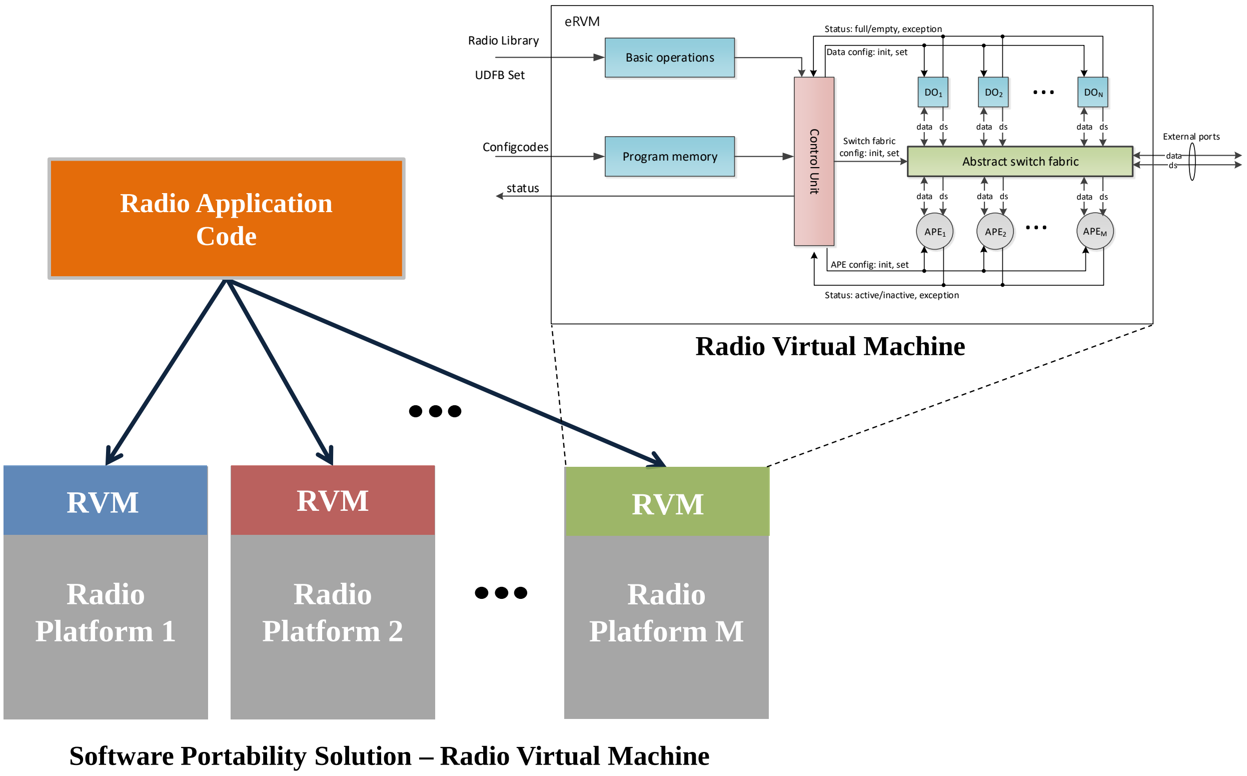


**Figure 8: Concept of the Radio Virtual Machine.**

The upper approach ensures code portability while maintaining efficiency; the latter is possible since no middleware is introduced and *RadioApp* designers have full flexibility for joint optimization of hardware and software designs.

## 4.4 Example application of software reconfiguration in a heterogeneous radio environment

While the ETSI software reconfiguration solution is applicable to a variety of use cases, a typical example relates to the optimum configuration of radio equipment in a heterogeneous radio environment. Figure 9 illustrates how an efficient software adaptation of a Mobile Device to a dynamically changing radio environment can be achieved through calculation of suitable Key Performance Indicators and a corresponding software component selection and parameterization by the Mobility Policy Manager (MPM) in the Communication Service Layer (CSL). The corresponding decisions are then forwarded to the Radio Connection Manager inside Radio Control Framework (RCF) through the MURI interface where they are executed. These basic principles are illustrated below.

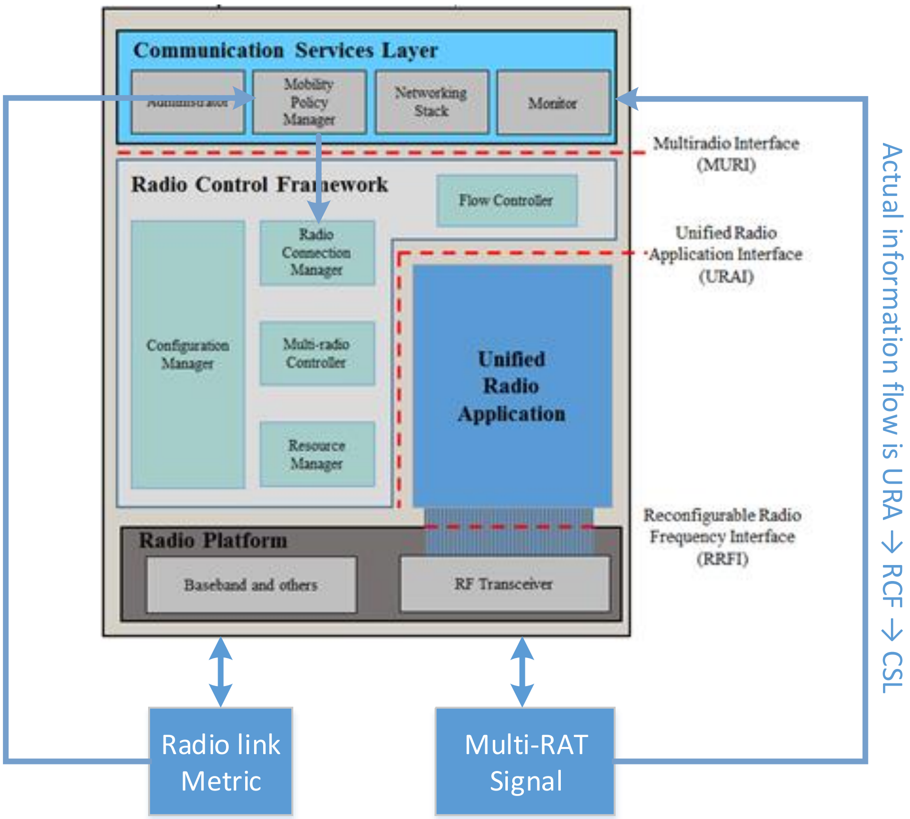


**Figure 9: Multi-RAT operation in a heterogeneous radio environment (using the Mobile Device Reconfiguration Architecture in this example)**

# 5 Recommendations and conclusions

The ETSI software reconfiguration solution introduces an entire standardized ecosystem (specified in EN 303 641 [1], EN 303 648 [2], EN 303 681-1 to EN 303 681-4 [3] to [6],  EN 303 681-2 [4], [5], EN 303 681-4 [6], TR 103 585 [7] and EN 302 969 [8]) including technical, regulation and security solutions  enabling the software reconfiguration of radio parameters. Note that the specific case of Mobile Device Reconfiguration is addressed in an independent set of specifications (see EN 303 095 [9], EN 303 146-1 to EN 303 146-4 [10] to [13], TR 103 087 [14] and TS 103 436 [15]). While the solution is applicable to various contexts, it is specifically tailored to the needs of commercial mass market applications. The ETSI solution is also tailored to the needs of the Radio Equipment Directive [16] which includes articles on software reconfiguration.

The ETSI solution typically offers high efficiency in terms of power consumption and computational complexity as well as portability across various distinct hardware platforms. The applicability has been demonstrated for the following example use cases:

- Smartphone reconfiguration,
- Automotive applications,
- Network Radio Reconfiguration,
- Internet-of-Things device reconfiguration,
- Radio Reconfiguration through an external component,
- Reconfigurable satellite telecom payload,
- Bug-fix and security updates,
- Medical applications.

Furthermore, ETSI has considered security requirements and has introduced a corresponding security framework in TR 103 087 [14] and TS 103 436 [15].

From an implementation point of view, the ETSI software reconfiguration approach allows a gradual, stepwise approach from partial to fully flexible software reconfiguration. In a first step, for example, the manufacturer may choose to add spare computational resources to be used for hardwired component-replacement through software updates. In later generations, a platform may employ more and more software-based components for increased post-sale reconfiguration capabilities.

For the future, it is expected that such a radio equipment software reconfiguration framework will perfectly fit into the network virtualization context, providing full upgradability. That is, the current trend of “softwareization” in the network side will continue to expand and also encompass the client side. Software reconfigurability is thus expected to be a key enabler for 5G technology and beyond all network and client entities and for support of vertical applications such as automotive, Internet of Things, etc.

# Annex A: Acronyms and abbreviations

| | |
|---|---|
| APE | Abstract Processing Elements |
| ASF | Abstract |
| ASIC | Applications-Specific Integrated Circuit |
| CSL | Communication Services Layer |
| DO | Data Object |
| DoC | Declaration of Conformity |
| DSP | Digital Signal Processor |
| FPGA | Field Programmable Gate Array |
| HW | HardWare |
| IoT | Internet of Things |
| IR | Intermediate Representation |
| JTNC | Joint Tactical Networking Centre |
| RERC | Radio Equipment Reconfiguration Class |
| MPM | Mobility Policy Manager |
| MURI | MUltiRadio Interface |
| QoS | Quality of Service |
| RA | Radio Application |
| RAT | Radio Access Technology |
| RCF | Radio Control Framework |
| RF | Radio Frequency |
| RPI | Radio Programming Interface |
| RRFI | Reconfigurable Radio Frequency Interface |
| RVM | Radio Virtual Machine |
| SCA | Software Communication Architecture |
| URA | Unified Radio Applications |
| URAI | Unified Radio Applications Interface |
| V2X | Vehicle to Everything |
| V2V | Vehicle to Vehicle |

# Annex B: References

[1] ETSI EN 303 641 V1.1.2 (2020-03), Reconfigurable Radio Systems (RRS); Radio Equipment (RE) reconfiguration requirements

[2] ETSI EN 303 648 V1.1.2 (2020-03), Reconfigurable Radio Systems (RRS); Radio Equipment (RE) reconfiguration architecture

[3] ETSI EN 303 681-1 V1.1.2 (2020-03), Reconfigurable Radio Systems (RRS); Radio Equipment (RE) information models and protocols for generalized software reconfiguration architecture; Part 1: generalized Multi-radio Interface (gMURI)

[4] ETSI EN 303 681-2 V1.1.2 (2020-03), Reconfigurable Radio Systems (RRS); Radio Equipment (RE) information models and protocols for generalized software reconfiguration architecture; Part 2: generalized Reconfigurable Radio Frequency Interface (gRRFI)

[5] ETSI EN 303 681-3 V1.1.2 (2020-03), Reconfigurable Radio Systems (RRS); Radio Equipment (RE) information models and protocols for generalized software reconfiguration architecture; Part 3: generalized Unified Radio Application Interface (gURAI)

[6] ETSI EN 303 681-4 V1.1.2 (2020-03), Reconfigurable Radio Systems (RRS); Radio Equipment (RE) information models and protocols for generalized software reconfiguration architecture; Part 4: generalized Radio Programming Interface (gRPI)

[7] ETSI TR 103 585 V1.2.1 (2019-11), Reconfigurable Radio Systems (RRS); Radio Equipment (RE) reconfiguration use cases

[8] ETSI EN 302 969 V1.3.1 (2018-05), Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Requirements for Mobile Devices

[9] ETSI EN 303 095 V1.3.1 (2018-05), Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Architecture for Mobile Devices

[10] ETSI EN 303 146-1 V1.3.1 (2018-06), Reconfigurable Radio Systems (RRS); Mobile Device Information Models and Protocols; Part 1: Multi-radio Interface (MURI)

[11] ETSI EN 303 146-2 V1.2.1 (2016-06), Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 2: Reconfigurable Radio Frequency Interface (RRFI)

[12] ETSI EN 303 146-3 V1.3.1 (2018-06), Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 3: Unified Radio Application Interface (URAI)

[13] ETSI EN 303 146-4 V1.1.2 (2017-04), Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 4: Radio Programming Interface (RPI)

[14] ETSI TR 103 087 V1.2.1 (2017-11); Reconfigurable Radio Systems (RRS); Security related use cases and threats in Reconfigurable Radio Systems

[15] ETSI TS 103 436 V1.2.1 (2018-02); Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios

[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, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0053

[17] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0005

[18] ETSI TR 102 967 V1.2.1 (2015-11), Reconfigurable Radio Systems (RRS); Use cases for dynamic equipment reconfiguration

[19] SOFTWARE COMMUNICATIONS ARCHITECTURE SPECIFICATION, Joint Tactical Networking Center (JTNC), August 2015, V4.1, available at http://www.public.navy.mil/jtnc/sca/Pages/default.aspx

[20] SOFTWARE COMMUNICATIONS ARCHITECTURE SPECIFICATION USER'S GUIDE, Version: 4.1, 23 February 2016 , available at http://www.public.navy.mil/jtnc/sca/Pages/default.aspx

[21] Green-oriented multi-techno link adaptation metrics for 5G heterogeneous networks, Isabelle Siaud, Anne-Marie Ulmer-Moll, J Wireless Com Network (2016) 2016: 92

The Standards People

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

**This White Paper is issued for information only. It does not constitute an official or agreed position of ETSI, nor of its Members. The views expressed are entirely those of the author(s).**

ETSI declines all responsibility for any errors and any loss or damage resulting from use of the contents of this White Paper.

ETSI also declines responsibility for any infringement of any third party's Intellectual Property Rights (IPR), but will be pleased to acknowledge any IPR and correct any infringement of which it is advised.