ETSI White Paper No. 21

Software Radio Reconfiguration:

A highly efficient and modular software reconfiguration approach for mobile devices

First edition – October 2017

ISBN No. 979-10-92620-15-3

Authors:

Markus Mueck (editor), Francois Ambrosini, Paul Bender, Scott Cadzow, Seungwon Choi, Vladimir Ivanov, Marcello Pagnozzi, Isabelle Siaud

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 (editor)
INTEL Deutschland GmbH, Germany, Email: Markus.Dominik.Mueck@intel.com

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

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

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

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

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

Contents

Executive Summary

The ETSI software reconfiguration approach enables reconfiguration of wireless equipment through software [1], [2], [3], [4], [5], [6], [7], [8]. The solution has 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 new Radio Equipment Directive [9] 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.
- 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.

[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).

With the above features, the ETSI software reconfiguration solution is perfectly suited to meet the requirements of 5G 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 Introduction

Even after years of extensive research into Software Defined Radio, the technology has not had the expected impact. Solutions on offer often have limited scope for optimization. They may require complete redesign of radio architectures. Or they may present potential security weaknesses. In many cases, they are suitable for niche applications, but not for the commercial mass-market.

ETSI has developed a framework which enables reconfiguration of wireless equipment through software. The technology is flexible in that original hardwired components may selectively be re-parameterized or replaced by software components. Therefore it is applicable to software-only as well as hybrid platforms and enables a gradual roll-out of software reconfiguration in devices. The solution is designed to address technical, security and regulatory challenges, being tailored to the needs of the new Radio Equipment Directive.

In presenting this technology, we will first identify some use cases which would benefit from software radio reconfiguration, together with some of the challenges that must be faced when deploying such technology. We then present the ETSI solution in more detail, and examine how it addresses specific challenges.

2 Use Cases for Software Radio Reconfiguration

2.1 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. The optimum configuration is identified (e.g., new power-efficient modulation and coding schemes, etc.) to meet power efficiency [14], 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 – e.g. specific interference properties in a factory environment. Other types of features may consist of proprietary extensions such as Device-to-Device Communication, etc. which are not yet part of the 3GPP standard. 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

2.2 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 to provide 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. Certainly, wide-area mobile network technology does evolve, with new access technology (4G, 5G) introduced typically every ten years, and older technology networks shut down. 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 of change since a vehicle does not need to be upgraded by an authorized dealer (as would be the case for hardware changes), but the process is handled through over-the-air remote control.

In extreme cases, for example to address platform vulnerabilities which may arise suddenly over the lifetime of a vehicle, immediate action may be required in order to ensure the safety of passengers and other road users. There may not be time to recall and manually update millions of vehicles. Over-the-air software reconfiguration provides an efficient solution to deal with these issues.

Figure 2: Automotive Applications

2.3 Use Case 3 – Internet-of-Things product design

Future IoT devices, including 5G, 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

3 The ETSI Software Reconfiguration Solution

ETSI has developed a software reconfiguration solution [1], [2], [3], [4], [5], [6], [7], [8] 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.

3.1 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 [3] 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 [7], [8].

3.2 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.

3.3 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.

3.4 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 [12], [13] for example).

3.5 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.

4 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.

4.1 Legacy approach to software reconfiguration

A multitude of software radio reconfiguration approaches exist. Among these, the Software Communication Architecture (SCA) [12] 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.

4.2 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.

4.3 ETSI software reconfiguration eco-System and architecture

Figure 5 illustrates the reconfigurable mobile device architecture and related interfaces enabling software reconfiguration.

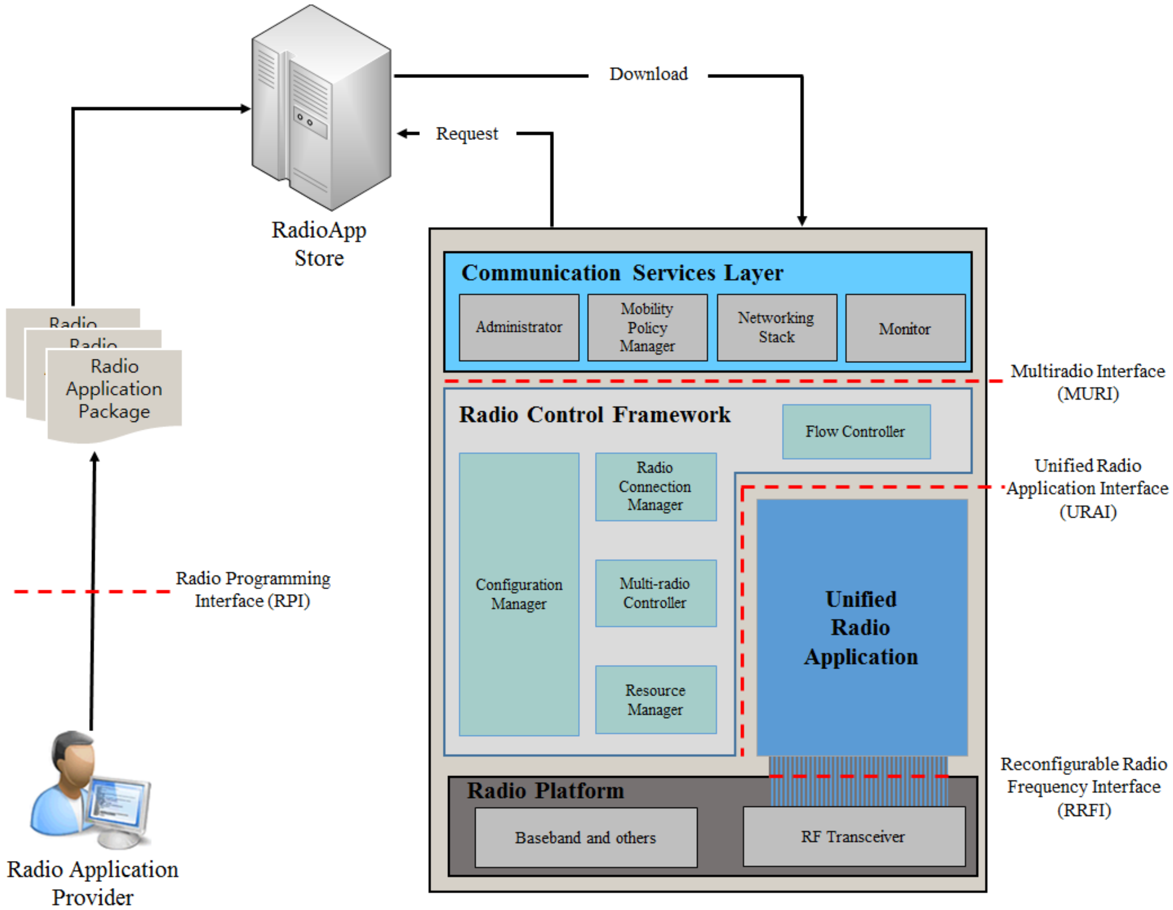

Figure 4: Standard reconfigurable mobile device architecture and related interfaces

As outlined in further detail in [2], a reconfigurable mobile device 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 mobile device 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 [2].
- The Radio Control Framework (RCF) manages the actual software execution through a number of functionalities which are introduced in [2].
- The Unified Radio Application (URA) represents the software downloaded and installed onto the target platform [2].
- The interfaces between the different layers are defined in [3], [4], [5], [6].

5 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 [1], [2], [3], [4], [5], [6], [7], [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.

5.1 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 Mobile Device Reconfiguration Classes (MDRCs) [1] as illustrated in Figure 5. 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 MDRCs. While the exact definitions of MDRCs are given in [1], examples are used below in order to facilitate the basic understanding.

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

Figure 5: Mobile Device Reconfiguration Classes

MDRC-0 (No reconfiguration) and MDRC-1 (No resource share – fixed hardware) represent today's commercial equipment. MDRC-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. MDRC-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.

MDRC-2 to MDRC-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 (MDRC-2 and MDRC-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 (MDRC-3 and MDRC-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 (MDRC-4 and MDRC-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, step-wise 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.

5.2 ETSI Security Framework: Security for Software Reconfiguration

The ETSI security framework for software reconfiguration [7], [8] 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 Radio Equipment (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.

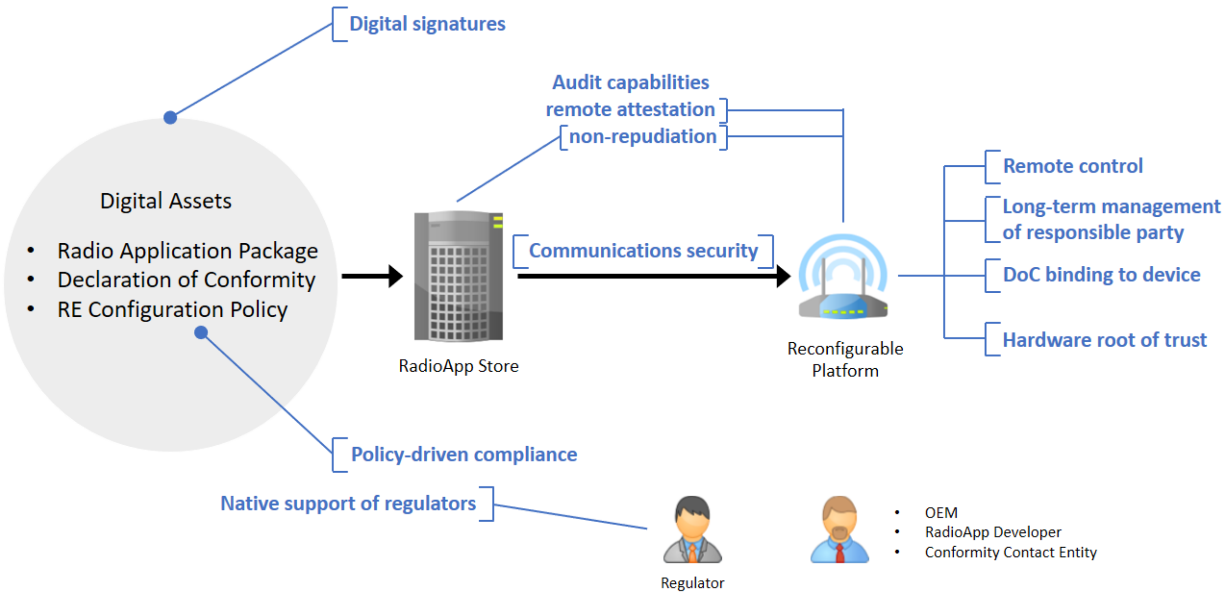

Figure 6: Security measures for the ETSI Software Reconfiguration framework

The role of security countermeasures is to defend the system against attack. Attacks against a reconfigurable radio are 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 the 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. by 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 reconfigurable radio systems (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 third 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 or masquerade of any of the actors, and against regulatory bypass.

The trusted third 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, Radio Equipment Configuration Policy and Declaration of Conformity;
- Proof of the identity of the developer of radio applications, the issuer of the Radio Equipment 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).

5.3 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 [6]. 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 6 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 6, 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.

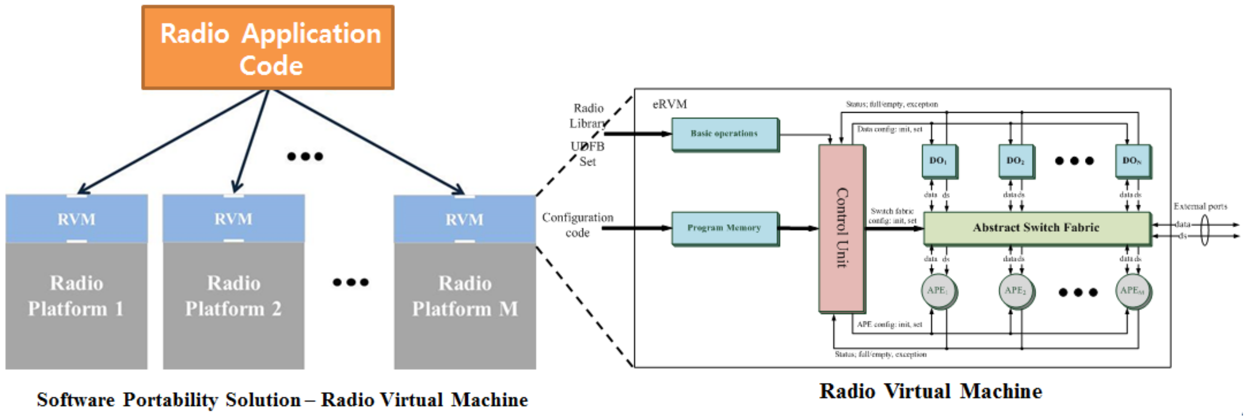

Figure 7. Concept of the Radio Virtual Machine

The above 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.

5.4 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 wireless equipment in a heterogeneous radio environment. Figure 8 illustrates how an efficient software adaptation 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.

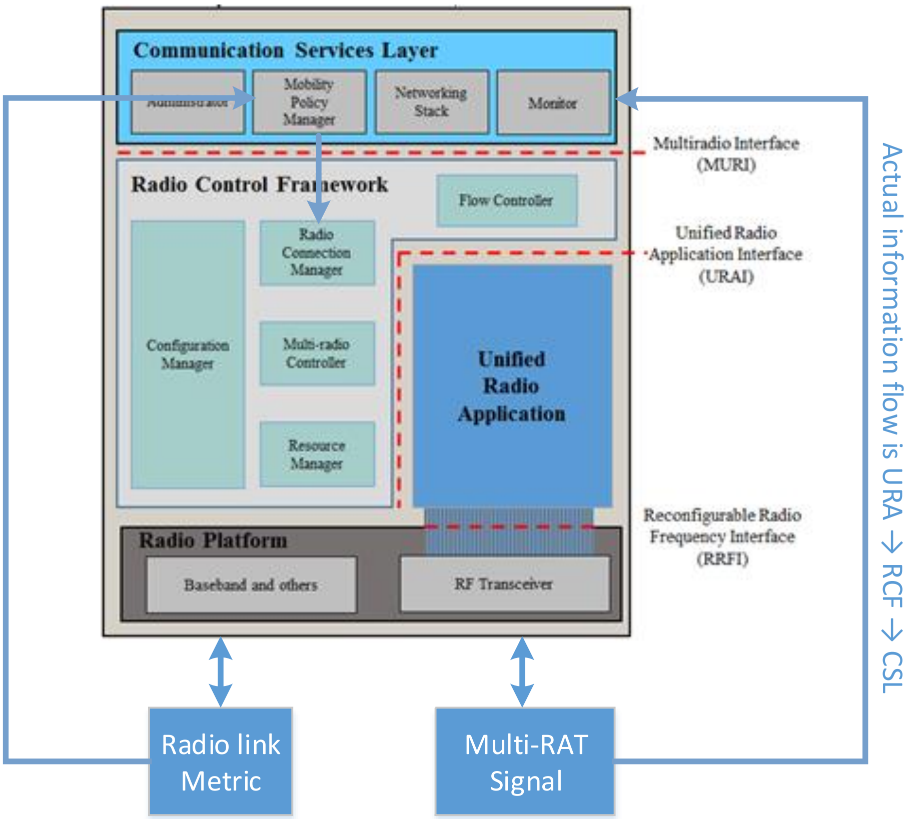

Figure 8. Multi-RAT operation in a heterogeneous radio environment.

6 Recommendations and conclusions

The ETSI software reconfiguration solution introduces an entire standardized ecosystem (specified in [1], [2], [3], [4], [5], [6], [7], [8]) including technical, regulation and security solutions enabling the software reconfiguration of radio parameters. 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 new Radio Equipment Directive [9] 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 three example use cases:

- Smartphone reconfiguration,
- Automotive applications and
- Internet-of-Things product design.

Furthermore, ETSI has considered security requirements and has introduced a corresponding security framework in [7], [8].

From an implementation pint of view, the ETSI software reconfiguration approach allows a gradual, step-wise 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 mobile device software reconfiguration framework will perfectly fit into the network virtualization context. The current trend of softwareization in the network will continue to expand and also encompass the client. Software reconfigurability is thus expected to be a key enabler for 5G technology across all network and client entities, as well as for support of vertical applications such as automotive, Internet of Things, etc.

Acronyms

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
MDRC	Mobile Device 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

References

[1] ETSI EN 302 969 V1.2.1 (2014-11), Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Requirements for Mobile Devices

[2] ETSI EN 303 095 V1.2.1 (2015-06), Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Architecture for Mobile Devices

[3] ETSI EN 303 146-1 V1.2.1 (2015-11), Reconfigurable Radio Systems (RRS); Mobile Device Information Models and Protocols; Part 1: Multiradio Interface (MURI)

[4] 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)

[5] ETSI EN 303 146-3 V1.2.1 (2016-08), Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 3: Unified Radio Application Interface (URAI)

[6] ETSI EN 303 146-4, to appear, Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 4: Radio Programming Interface (RPI)

[7] ETSI TR 103 087 V1.1.1 (2016-06); Reconfigurable Radio Systems (RRS); Security related use cases and threats in Reconfigurable Radio Systems

[8] ETSI TS 103 436 V1.1.1 (2016-08); Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios

[9] 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

[10] 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

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

[12] 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

[13] 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

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

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