## Radio Equipment Directive: The ETSI Status

Holger Butscheidt, Bundesnetzagentur, ETSI TC ERM Chairman

ETSI's ElectroMagnetic Compatibility (EMC) and Radio Spectrum Matters Committee (TC ERM) is still focusing on the introduction of the new Radio Equipment Directive (RED) which replaced the Radio and Telecommunications Terminal Equipment (R&TTE) Directive in June 2016, subject to a one-year transition period. For many years ETSI's committee has provided more than 75 percent of the Harmonized Standards required under the R&TTE Directive. The new RED has implications for ETSI's radio work, especially in relation to receivers, software defined radio and cognitive radio. After review and alignment, the committee is currently maintaining nearly 150 Harmonized Standards related to the Radio Equipment Directive, which includes radio as well as EMC Harmonized Standards.

In addition, since the scope of the RED is broader than the R&TTE Directive, we continued to develop new Harmonized Standards in areas such as radio and TV broadcast receivers, equipment below 9 kHz and radio determination equipment, which were not addressed by the R&TTE Directive.

Currently, a majority of titles and references of Harmonized Standards under the responsibility of TC ERM have been listed in the Official Journal of the European Commission, to confer a presumption of conformity. Nevertheless, improvement is still required with regard to some of these Harmonized Standards, in particular to address requirements related to receiver performance parameters. In addition, other Harmonized Standards are undergoing revision to achieve a positive assessment by the European Commission.

To assist radio groups in defining new receiver performance parameters, an ETSI-specific group in the committee has been established to investigate and describe a new concept of signal interferer handling.

The ERM Technical Committee is responsible for the coordination of ETSI positions on the effective and efficient use of the radio spectrum and the administration of the Memorandum of Understanding between the European Conference of Postal and Telecommunications Administrations (CEPT/ECC) and ETSI. Several System Reference documents (SRdoc) have been published recently. Others are under preparation in close cooperation with the relevant ETSI Technical Bodies in order to request a change to the present frequency designation/utilization within CEPT/ECC, or a change in the current regulatory framework for the proposed band(s), regarding either intended or unwanted emissions.

In parallel, a Liaison group under TC ERM has been established to improve cooperation in the area of Wireless Power Transmission (WPT) between CENELEC and ETSI. The intention is to assist with providing input to the ongoing discussions in order to prepare the necessary regulatory conditions for the introduction of WPT in Europe, as well as worldwide.

## ETSI NFV Specification Progress: NFV to Become Operational

Joan Triay, TSC Technical Manager of the ETSI NFV ISG

The ETSI NFV Industry Specification Group (ETSI NFV)[1] is at the core of the industry for NFV technology definition, and it has provided the foundation standards underpinning the NFV ecosystem since late 2012, when it was launched by global carriers. The ETSI NFV specification work has matured to a level where the specifications[2] are implementable and being widely referenced by all industry stakeholders.

Since its inception, ETSI NFV has completed several phases of specification. Currently, it is working intensively on the specification of features that will comprise Release 3. At the same time, the group is maintaining the set of published Release 2 specifications while finalizing a few key ones, such as the descriptors for the Virtualized Network Function (VNF) and Network Service (NS), and security enhancements related to VNF packaging and APIs. The security aspects are a major pillar for NFV to be deployed in carrier-grade networks and to become operational, goals to which the ETSI NFV gives particular emphasis by pursuing the "secure by design" philosophy. More details are provided in an accompanying article.

The Release 2 specifications covering requirements, interfaces definition and information model were published in 2016. Since that time, ETSI NFV has completed three maintenance cycles (roughly every six months) to correct bugs and improve the documents. Specifications on protocols and data models have followed with the so called NFV-SOL RESTful APIs, and the standard VNF packaging solution. The relevant specifications have been delivered by the Solutions (SOL) Working Group, and more information is provided in an accompanying article. It is worth highlighting that the NFV-SOL specifications are implementable representations of the stage 2 designs defined in the NFV-IFA specifications, and not alternative solutions.

The ETSI NFV work on testing actual NFV solutions is rapidly building momentum and has become one of the driving activities because specific implementations have emerged based on the functionality and APIs specified by ETSI NFV. A concrete example is the ongoing "API conformance testing" specification work (to be published, once completed, as ETSI GS NFV-TST 010) and the maintenance of the "testing guidelines" (ETSI GR NFV-TST 007). NFV-TST 007 is the reference documentation for the ETSI NFV Plugtests. The third Plugtest event was planned for May/June 2018.

The NFV Release 3 specification work is ongoing. A feature-based development approach is being taken whereby new specifications and updates (i.e., evolution) of the current Release 2 specifications will be delivered together. Release 3 focuses on enriching the NFV Architectural Framework to prepare NFV for global deployment and operations. The Release 3 features are categorized into three main groups: i) advances in virtualization technologies (e.g., to support cloud-native VNF, acceleration, etc.); ii) support for future and emerging networks (e.g., 5G and network slicing); and iii) new operational features. Within the last group, some of the features that will be defined by the summer of 2018 include operational enablers, such as a means for increasing the level of automation (e.g., policy framework), continuous delivery and integration (e.g., VNF snapshots), and support for carrier-grade network operations (e.g., support for host reservations and management of NFV-MANO components). The remaining feature specifications are expected to be completed during 2018 and the early part of 2019. In the meantime, the reports and study items that have driven the analysis work of the features and their feasibility have been published. Information about the specification progress of Release 3 features is publicly available on the ETSI NFV public wiki[3].

Last but not least, despite the high workload to deliver the Release 2 and Release 3 specifications, ETSI NFV continues to engage and strengthen collaboration with other industry stakeholders, including other SDOs and open source communities. For example, feedback from open source implementations has

been one of the main drivers of the maintenance work performed on the Release 2 documentation. Further interaction with open source projects is expected now that fully implementable APIs and associated artefacts are available.

[1] http://www.etsi.org/nfv

[2] All published specifications are available on: https://docbox.etsi.org/ISG/NFV/Open/Publications_pdf/Specs-Reports

[3] Available on: https://nfvwiki.etsi.org/index.php?title=Feature_Tracking

## Carrier Grade Resiliency in Virtualized Environments

### Stefan Arntzen, Chairman of the Reliability, Availability and Assurance Working Group (REL)

The Reliability, Availability and Assurance Working Group (REL) was created in late 2012 to examine resiliency aspects for NFV infrastructure, software architecture and management and orchestration (MANO). The goal was to ensure that reliability and availability levels for services in a virtualized environment which comply with requirements for carrier grade networks and services can be supported in an NFV environment. A large group of reliability experts representing operator and vendor companies participated in this work. The initial output of the group was a reference document on resiliency aspects in NFV environments, ETSI GS NFV-REL 001 Resiliency Requirements.

The second phase of ETSI NFV specification work commenced at the beginning of 2015. In this second phase, the REL working group focused its efforts on analyzing important aspects of service reliability, availability and assurance in more detail. This work led to the publication of the following documents:

- Scalable Architectures for Reliability Management (ETSI GS NFV-REL 002)
- Models and Features for End-to-End Reliability (ETSI GS NFV-REL 003)
- Active Monitoring and Failure Detection (ETSI GS NFV-REL 004)
- Quality Accountability Framework (ETSI GS NFV-REL 005)
- Maintaining Service Availability and Continuity Upon Software Modification (ETSI GS NFV-REL 006)
- Resilience of NFV-MANO critical capabilities (ETSI GR NFV-REL 007)

Currently REL is working on creating normative requirements that will enable the NFV interfaces to support interworking of reliable building blocks. In-life software upgrade has been identified as an area that can significantly impact the reliability of an NFV system. Normative requirements for software upgrade published in ETSI GS NFV-REL 006 are currently being translated into the necessary changes to the interfaces specified by the Interfaces and Architecture Working Group (IFA). A complete and comprehensive set of normative requirements that address the resiliency aspects for carrier-grade virtualized environments is currently being developed.

The REL working group is also examining the resiliency aspects of future enhancements to NFV. Work items are in progress to study error handling as well as the resiliency of network slicing in 5G environments implemented using NFV.

## The ETSI NFV Security Standards Activities and Output

### Igor Faynberg, Cable Labs, ETSI NFV Security Working Group Chairman

As underlined in an accompanying article by Joan Triay Marques (ETSI NFV Technical Steering Committee Chair), which provides an overarching review of the ETSI NFV Industry Specification Group project, the ETSI NFV Security (SEC) Working Group charter has been to ensure "security-by-design" principles are adopted by the NFV community. The main task of the group was to outline the security problems that were specific to NFV and thus develop a sharp focus on specific issues for the telecommunications industry. Originally created as an "Expert Group" in 2013, the NFV SEC WG has become an ETSI NFV Working Group with a remit to develop industry standards where necessary.

As it turned out, the set of problems identified in the NFV Security Problem Statement, ETSI GS NFV-SEC 001, was comprehensive in that all but one of the 22 subsequent work items progressed by the NFV SEC WG address problems identified in that set. The exception was a study of OpenStack security, ETSI GS NFV-SEC 002, which documented the state of the art in this open source project in relation to security. These two deliverables illustrate the two-pronged, i.e., top-down and bottom-up, modus operandi of the SEC Working Group.

A fundamental difference between the NFV and the generic Cloud environments is that telecommunications networks are considered to be critical national infrastructures and are therefore heavily regulated. This translates into stringent (and rather challenging to implement in the virtualized environment) requirements related, for example, to lawful interception. Examples of other stringent regulatory requirements, which differ from country to country, are those related to data retention, personally-identifiable information sharing, and movement of data that are considered private across national or regional borders.

The ten problems identified in the NFV Problem Statement are:

1. Topology validation and enforcement
2. Availability of management support infrastructure
3. Secured boot
4. Secure crash
5. Performance isolation
6. User/tenant authentication, authorization and accounting
7. Authenticated time service
8. Private keys within cloned images
9. Back-doors via virtualized test & monitoring functions
10. Multi-administrator isolation

One use case for the multi-administrator isolation is lawful interception (an activity that may not be interfered with or even detected by the administrating entity without the need to know). It is also important to note that multi-administrator isolation is also indispensable to the proper operation of the NFV tenants.

The implications of lawful interception are reported in ETSI GS NFV-SEC 004, while the requirements for a multi-layer isolation approach and the lawful interception architecture in the NFV environment are specified in ETSI GR NFV-SEC 009 and ETSI GR NFV-SEC 011, respectively. The technical measures and software and hardware interfaces that ensure the execution of sensitive software components are specified in ETSI GR NFV-SEC 009.

Another essential regulatory requirement to be implemented in the NFV environment concerns retained data, which is dealt with in ETSI GS NFV-SEC 010.

The foundation for developing security in the NFV environment is the identity management of all entities involved in its operation, which results in building trust relationships (as specified in ETSI GR NFV-SEC 003). Once the hardware root of trust is established with the help of hardware such as the Trusted Platform Modules (TPM), the proper booting of software can be ensured and measured remotely through to run time. To achieve this, the mechanism of Remote Attestation is described in ETSI GR NFV-SEC 007.

As the software is being deployed and booted, both security monitoring and security management mechanisms

must be implemented to ensure proper operation. This subject is treated comprehensively in ETSI GS NFV-SEC 013. This standard has already been partially implemented in the open-source project, https://github.com/intel/vnb-main.

A significant part of the SEC WG responsibilities is to help other groups develop security considerations material relevant to their output. To enforce a systematic approach to security development within ETSI NFV, ETSI GS NFV-SEC 006 has been applied to the development of a specification for the management and operational interfaces, which in turn resulted in publishing the respective interface specifications by the SEC, IFA, and SOL working groups: ETSI GS NFV-SEC 014, ETSI GR NFV-IFA 021, ETSI GRNFV-IFA 022, ETSI GR NFV-IFA 028, ETSI GS NFV-IFA 027, ETSI GS NFV-SOL 002, ETSI GS NFV-SOL 003, and ETSI GS NFV-SOL 005.

Current SEC Working Group activities are focused on furthering the specification of identity management aspects of NFV, including dynamic NFV public key infrastructure specifications (e.g., using the Hardware Security Modules (HSM)) while continuing to study solutions that address regulatory issues related to ascertaining the location of virtualized network function component instantiations and timestamping.

## Bringing NFV Solutions to the Market

### Bruno Chatras, Chairman of the Solutions (SOL) Working Group

The Solutions (SOL) Working Group was created in 2016 within the ETSI NFV Industry Specification Group (ETSI NFV) to develop standard protocols and data models enabling vendors to bring interoperable products to the market. Encouraging interoperability within an open ecosystem was a key objective for ETSI NFV when it was launched in late 2012 by global carriers. Indeed, to enable an effective market, Virtualized Network Functions (VNFs) must be interoperable and packaged in a way that makes them interoperable with independently developed management systems. Furthermore, multi-vendor interoperability is also expected between the components of NFV management and orchestration systems, as well as between these NFV-specific systems and other Operations Support Systems (OSS) deployed by service providers.

In July 2017, ETSI published the specifications for a set of RESTful APIs enabling interoperability between an NFV Orchestrator (NFVO) and a VNF Manager (VNFM), and between a VNFM and a VNF or an associated Element Management (EM) function. These specifications are documented respectively in ETSI GS NFV-SOL 003 and ETSI GS NFV-SOL 002. In February 2018, the specifications for the RESTful APIs exposed by an NFV Orchestrator (NFVO) toward OSS components were published in ETSI GS NFV-SOL 005. Furthermore, the development of OpenAPI specifications (formerly known as a Swagger specifications) for each of these APIs is ongoing; some of them have already been published by ETSI, in the form of YAML and JSON files, along with tools to navigate the specifications and report bugs (https://nfvwiki.etsi.org/index.php?title=API_specifications#OpenAPIs). The provision of these files to the industry is intended to facilitate the development and validation of products exposing or consuming these APIs.

Multi-vendor interoperability requires standard APIs as well as standard VNF packaging solutions. In July 2017, ETSI published the specifications for the structure and format of a VNF package, a file archive that contains all necessary files to deploy and manage a VNF. These specifications leverage the OASIS Cloud Service Archive (CSAR) format specification and are documented in ETSI GS NFV-SOL 004. One of the artefacts contained in a VNF package is the VNF descriptor (VNFD), a deployment template that drives the behavior of NFV orchestration functions. Additional work is ongoing in ETSI NFV to specify the format and syntax a VNFD will have to comply with. These specifications leverage the "OASIS TOSCA Simple Profile in YAML" specification and are expected to be stable by mid-2018 and published by the end of the year as ETSI GS NFV-SOL 001. This document will also incorporate the specifications of a YAML rendering for NFV Service Descriptors (NSD).

Work is also starting on an alternative YANG-based representation of the VNFD and the NSD and on the specification for the format and structure of the NSD file archive, gathering the NSD itself and various other files it references (e.g., network service lifecycle management scripts). These specifications are expected to be published by the end of 2018.

All aforementioned ETSI specifications are subject to an ongoing maintenance process to fix bugs reported by open source communities and other industry players involved in NFV. A further step toward multi-vendor operability is also being taken by ETSI NFV with the development of conformance test suites for each of these APIs. Furthermore, these specifications are expected to be enhanced within the framework of the NFV Release 3 specification effort to support new features and new architecture reference points (e.g. APIs between NFVOs).

## ETSI Open Source MANO (OSM)

### Francisco-Javier Ramón Salguero (Telefonica), OSM Chair; Pål Grønsund (Telenor), OSM Vice-Chair

ETSI Open Source MANO (OSM) provides the industry with a fully functional orchestrator for Network Function Virtualization (NFV) implemented as open source and aligned to the ETSI NFV framework. OSM announced Release FOUR on 23 May 2018 with a high level of maturity both in the supported features and in the robustness of the code.

The NFV standards are necessarily complex, and assessing interoperability according to these standards is also complex. The rise of open source implementation projects provides a fresh approach to achieving effective interoperability by an open cyclical process. With complex standards, some level of ambiguity or functional deficiency might be expected, even with the best possible intentions of those involved. OSM provides the opportunity through its open development of a real system to validate these standards and provide open and early feedback.

OSM implements the NFV Orchestrator (NFVO) and generic VNF Manager (VNFM) functional blocks and re-architects them as different internal modules in OSM. The benefit of this approach is to avoid the VNFM to NFVO granting/reservation process. OSM strongly encourages the use of the generic VNFM developed in OSM, but specific VNFMs can be integrated if required. OSM is agnostic to the reference points between VNFM and VNF/EM since this interaction is mediated by a dedicated agent whose code is provided by the VNF vendor. In addition, OSM augments the NFVO role with service orchestration capabilities that include the ability to add day-2 configuration primitives to manage Network Service (NS) instances once deployed.

OSM supports NS and VNF life-cycle management functions and in addition implements critical features such as: multi Virtual Infrastructure Manager (VIM) support (e.g. OpenStack,

VMware vCD, AWS); multiple SDN controller support (e.g. OpenDaylight, ONOS, Floodligh); public cloud integration (AWS); monitoring usable for service assurance; network service design GUI; DevOps framework; service chaining.

OSM will continue its focus on supporting the ETSI NFV ISG standards. In OSM Rel FOUR we implemented the support of the critical northbound interface SOL 005.

OSM maintains the pace of a release every six months and is working on several critical features such as support for container based VNF deployments and 5G use cases including network slicing. In addition to this, OSM focuses on improving existing features such as monitoring and service assurance, service chaining, support for physical deployment units, public cloud integration and support for 5G network slicing.

## Standardization Progress in ETSI Quantum Safe Cryptography

Mark Pecen, Chairman, ETSI TC Cyber Working Group for Quantum Safe Cryptography (QSC) (France); Chief Operating Officer, ISARA Corporation (Canada); Board Member, Institute for Quantum Computing, (Canada)

**Why the ETSI TC Cyber Working Group QSC exists**

Emerging quantum computers use physical quantum effects to achieve mathematical computation. Major breakthroughs have been made recently and governments as well as industry have all made substantial investments in quantum computing over the past 18 months.

Quantum computers are problem-class dependent, able to solve problems non-solvable by conventional super-computers. This opens up new possibilities for areas like drug discovery, new materials development and other problems that were previously regarded as intractable. Unfortunately, problems such as the integer factorization problem and discrete logarithms problem are very easily solved by quantum computers. Both problems are the basis for the Public Key Infrastructure (PKI), which protects our information and identity over the Internet and wireless networks, and the reason why we have created the ETSI TC Cyber QSC.

**About ETSI Cyber QSC**

Cyber QSC was founded in March 2015 as an ETSI Industry Specification Group and was converted to a working group of TC Cyber in March 2017. We focus on the practical implementation of quantum safe primitives, including performance considerations, implementation capabilities, protocols, benchmarking and practical architectural considerations for specific applications. Our work fed into other groups and standards bodies such as the International Telecommunications Union (ITU).

Our objectives do not include the development of cryptographic primitives. This is a proposition best left to academia and other groups who specialize in the area, such as the ETSI Security Algorithms Group of Experts (SAGE) and the National Institute of Standards and Technology (NIST) in the U.S.

**Publications to date**

ETSI Group Report (GR) QSC001, "Analysis of Quantum-Safe Primitives" [1], discusses the basic principles of quantum-safe cryptography, the range of options available for implementation and usage, as well as certain performance considerations and constraints such as cryptographic key-lengths and computational requirements.

ETSI GR QSC003, "Quantum-Safe Case Studies & Use Cases" [2], is a practical analysis of the consequences of implementing and deploying certain quantum-safe methods. In this report, we cover some aspects of network security, such as transport layer security (TLS), security for the Internet of Things (IoT), and the inherent constraints as well as satellite communication and the issues associated with security of one-to-many broadcast data.

ETSI GR QSC004, "Quantum-Safe Threat Analysis" [3], is an overview of what is vulnerable over time to quantum attacks, including applications in banking and finance, intelligent transportation systems, Internet of Things, digital media content protection eHealth, as well as how some of the quantum attacks are formulated.

ETSI GR QSC006, "Limits of Quantum Computing on Symmetric Key Cryptography" [4], is the only effort addressing Symmetric Key Cryptography thus far. Although rather speculative, it is an excellent grounding on the limits of quantum computing as we know it today.

ETSI TR 103 570, "Quantum-Safe Key Exchanges, Implementation Analysis" [5], covers a range of quantum-safe key exchange mechanisms, such as Learning with Errors (LWE), Ring Learning with Errors (RLWE), supersingular isogenies, and others regarding parameter selection, performance and implementation constraints.

**Ongoing work**

The group is currently working on quantum safe cryptographic signature assessment, Virtual Private Network (VPN), identity-based encryption and migration techniques to quantum-safe systems.

**References and official links:**

[1] ETSI Group Report (GR) QSC001 "Analysis of Quantum-Safe Primitives": http://www.etsi.org/deliver/etsi_gr/QSC/001_099/001/01.01.01_60/gr_QSC001v010101p.pdf
[2] ETSI GR QSC003 "Quantum-Safe Case Studies & Use Cases": http://www.etsi.org/deliver/etsi_gr/QSC/001_099/003/01.01.01_60/gr_QSC003v010101p.pdf
[3] ETSI GR QSC004 "Quantum-Safe Threat Analysis": http://www.etsi.org/deliver/etsi_gr/QSC/001_099/004/01.01.01_60/gr_QSC004v010101p.pdf
[4] ETSI GR QSC006 "Limits of Quantum Computing on Symmetric Key Cryptography": http://www.etsi.org/deliver/etsi_gr/QSC/001_099/006/01.01.01_60/gr_QSC006v010101p.pdf
[5] ETSI TR 103 570 "Quantum-Safe Key Exchanges, Implementation Analysis": http://www.etsi.org/deliver/etsi_tr/103500_103599/103570/01.01.01_60/tr_103570v010101p.pdf
[6] Quantum Safe Cryptography and Security: an introduction, benefits, enablers and challenges, (M. Pecen, *et al.*; ETSI, ISBN No. 979-10-92620-03-0), June 2015.

## System Aspects and Functionalities for Reconfigurable Radio Systems and Spectrum Sharing

Michael Gundlach, Senior Standardization Specialist at Nokia, Chairman of ETSI RRS WG 1

ETSI TC RRS is the center of expertise for reconfigurable radio systems (RRS). These are expected to become important drivers for the evolution of wireless communications and to bring substantial benefits, from reconfigurable flexible and cost-effective architectures for wireless devices to a better utilization of the radio frequency spectrum, thereby helping to mitigate the spectrum scarcity problem. It is the objective of ETSI RRS to enable the deployment and operation of cognitive radio systems, including white space (WS) devices and entities for licensed shared access (LSA). Working Group 1 has the task to collect and define requirements on reconfigurable radio systems from relevant stakeholders, to develop and maintain a common technical framework for system-level aspects, to define the cognitive functionalities for reconfigurable radio systems, and to deliver technical reports and specifications as appropriate.

In response to EC Mandate M/512, RRS WG 1 has developed TV white space related deliverables, including a description of use cases, requirements and interfaces. An important result are the specifications of the system architecture for the information exchange between different geo-location databases (GLDBs) enabling the operation of white space devices (WSDs) for the protection of the incumbent services.

In close alignment with CEPT WG FM, with ETSI TC ERM, and also in response to EC Mandate M/512, RRS WG 1 has developed LSA related deliverables, including a System Reference document (SRdoc) and technical specifications (TS) describing the system requirements, the architecture and the interface between the LSA repository and the LSA controller (according to the mandate in the 2.3-2.4 GHz spectrum, however, easily adaptable to other spectra). LSA based spectrum sharing is expected to be a key element in the tool box of regulatory administrations to address future 5G spectrum needs. The results of RRS WG 1 offer a ready-to-use package for Licensed Shared Access technology in Europe and other regions.

To continue the work on Licensed Shared Access, last year ETSI TC RRS started to address the different technical possibilities for local high-quality wireless networks to access spectrum temporarily on a shared basis, specifically for use in vertical markets. A Technical Report (TR) has been published and the requirement specification for an evolved LSA (eLSA) is currently being elaborated. This will be followed by the system architecture specification and the interface specification. Finalization is expected at the end of next year. The concept is agnostic to the radio frequency bands used.

Local high-quality wireless networks have been identified in the TR as a collective term to enclose a type of use case targeting local area services requiring predictable levels of QoS, e.g., in vertical industrial sectors such as industrial automation, Programme Making and Special Events (PMSE), Public Protection and Disaster Relief (PPDR), and e-Health. Their need for predictable levels of QoS mostly preclude operation in a license-exempt spectrum, due to coexistence issues, and target exclusively licensed spectrum. However, due to the current scarcity of suitable exclusive licensed spectrum resources, which can be directly accessible by vertical local area service providers, spectrum sharing has been proposed in the TR as the enabling spectrum technology for introducing QoS enabled local area services in licensed bands.

Another activity of RRS WG 1 is a set of a TRs and TSs for a radio interface engine (RIE). This engine empowers a decision unit to operate in a heterogeneous environment. The unit can be located either at the mobile devices or in the network. The decision relies on the eco-system that comprises multiple entities, including a context information acquisition entity, context management entity, configuration management entity, flexible modulation entity, and others. The RIE enables the efficient acquisition and management of context information and suitable equipment configuration in a heterogeneous radio environment.

The purpose of the RIE is to provide a defined method to interchange relevant context information to a decision unit. It provides a standard interface access to model based data that could represent historical data or relies on typical alternatively characterized scenarios. The predictive decision making relies on context information which serves as input to the RIE. The reliability of the data is improved by the RIE through iterative processing including a combination of multiple sources and KPI based decision making. The finalization of all related specifications is expected at the end of next year.

New work items related to reconfigurable radio systems will be started as appropriate. This may include a phase 2 of LSA providing, e.g., more dynamicity, additional functionality, and the use in other spectra. Also, the concept of a radio interface engine may be further developed. Other new projects may emerge, e.g., from international and national research projects. There was already in the past very good collaboration between such projects and the standardization work of RRS WG 1.

## ETSI TC RRS: A Software Reconfiguration Standards Framework for Commercial Mass Market Applications

Seungwon Choi, Hanyang University, Seoul, Korea, ETSI RRS WG2 Chairman; Markus D. Mueck, INTEL Deutschland GmbH, Munich, Germany, ETSI TC RRS Chairman

An open software reconfiguration framework has been successfully introduced in the military domain through the Software Communications Architecture (SCA) and other approaches, but it has never penetrated the commercial mass market domain to a relevant extent. The ETSI Reconfigurable Radio Systems (RRS) Technical Committee (TC) has recently published a set of standards that fill this gap; the new approach enables highly efficient and portable software reconfigurability for the specific needs of commercial products, including an architecture and interface framework as well as security and (re-)certification solutions.

In order to achieve this objective, ETSI TC RRS has proposed common reference architectures for reconfigurable radio equipment, of which the configuration can be controlled by software download. For that purpose, TC RRS has collected and defined the requirements and scenarios from relevant stakeholders, such as smartphone manufacturers, the automotive industry, etc. The common reference architecture proposed by TC RRS specifies interfaces and protocols among software entities as well as the related functionalities of each software entity composing the common reference architecture. Starting from TR 102 944 entitled "Use Cases for Baseband Interfaces for Unified Radio Applications of Mobile Device", TC RRS has published the specific technical solution framework in two technical reports, six technical specifications, and six European standards between 2011 and 2017, all of which are related to reconfigurable mobile devices. Requirements, architecture, and interfaces and protocols of reconfigurable mobile devices are specified by European Standards as EN 302 969, EN 303 095, and EN 303 146-1/146-2/146-3/146-4, respectively. The key objective of the reference architecture released by TC RRS is to resolve the problem of software portability between the radio application code and hardware platforms of reconfigurable mobile devices while maintaining overall efficiency; the exact level of reconfigurability and thus the choice of combining reconfigurable and hard wired elements is left to the implementer. Any platform compliant with the standard architecture and interfaces defined by TC RRS will be able to exploit corresponding generic code and thus the problem of portability and efficiency is overcome.

Besides the functionalities for the reconfiguration itself, the TC RRS solution comprises a security framework as defined in TS 103 436, which ensures a 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. It should be understood as a toolbox whose elements

can be implemented for products as required. To give an example, key features are defined such as audit functionalities including a non-repudiation framework and remote attestation, proof of the integrity of the radio applications, radio equipment configuration policy, declaration of conformity, etc.

Since the standardization for the reconfigurable mobile devices was completed in early 2018, TC RRS is in the phase of generalizing the existing framework for general applicability for reconfigurable radio equipment, including connected vehicle radio reconfiguration, network radio reconfiguration, IoT device reconfiguration, and smartphone radio reconfiguration, summaries of which are available in ETSI TR 103 585. Among the various applications, TC RRS especially notices the importance of the connected vehicle radio reconfiguration. Considering that the expected lifespan of a vehicle is more than 10 years while the normal update cycle of a vehicle communication standard is much shorter, typically two to three years, vehicle manufacturers face a serious challenge: unless the communication platform of vehicles is reconfigurable through a software download, every vehicle would have to be sent to a garage to change its communication platform whenever the communication standard changes or whenever vulnerabilities are identified. Indeed, the importance of software reconfigurability of vehicular communication platforms cannot be overemphasized considering the estimation that the number of vehicles to be equipped with the communication platform is expected to be more than 40 million by the year 2025. A demonstration regarding the connected vehicle radio reconfiguration was released during CES2018 in Las Vegas, which is available at https://www.youtube.com/watch?v=o6maJuHOWgg.

Urgently recognizing the importance of the software reconfiguration, especially in connected vehicle applications, TC RRS will organize an international workshop on reconfigurable radio system technology for autonomous vehicles at Hanyang University Seoul Korea (http://dsplab.hanyang.ac.kr) on 19 September 2018. A demonstration of a reconfigurable vehicular communication platform and oral presentations will be presented in this workshop by Hyundai Motors, Intel, Samsung, LG, and SK Telecom, as well as the Korean/German government and Kyoto University Japan. A brief review of the overall reconfiguration technologies performed by TC RRS has been released through ETSI White Paper No. 21, which was published in October 2017 as ISBN No. 979-10-92620-15-3.

## The Future of SIM Cards in ETSI SCP TEC

Michele Berionne, Qualcomm, Chairman of ETSI SCP TEC Group

The ETSI SCP TEC group is responsible for the definition and the maintenance of the technical specifications of the UICC (often known as a SIM card by the public), which is the platform adopted by 3GPP and 3GPP2 groups to host the identity and the credentials required to register on cellular networks. In the last couple of years, the focus was on the ability to reduce the power consumption to make the UICC platform more suitable to the IOT markets, where strict power constraints often exist. In this regard, the ability to suspend the UICC was added in Rel.14.

The UICC platform is based on the ISO/IEC 7816 series of specifications for IC-cards developed in the 1980s, and for this reason it has a certain number of limitations, including a very tight link between the logical aspects and the physical aspects, such as its form factor and the electrical characteristics.

For this reason, in May 2017 ETSI SCP TEC started working on the Smart Secure Platform (SSP). The SSP is the new platform that is expected to resolve the limitations of the UICC, addressing some of the requirements that are emerging, such as the ability to embed the secure elements inside the terminal, the need to have a variety of faster physical interfaces and the possibility to securely store large amounts of data.

One specific class of SSP is the iSSP, an SSP integrated in a system on chip (SoC), which can further reduce the size of the secure element in the device. The iSSP is based on the combination of a primary platform, which partially abstracts the actual hardware and is agnostic of the use-case, and a secondary platform, containing the actual HLOS and which is use-case dependent. The iSSP architecture should allow the coexistence of applications of various stakeholders at the same time on the SSP (e.g., telecom, payments, and others).

SCP TEC has had a tight schedule of meetings and conference calls for the last six months with the goal of writing the SSP specifications and making them available to other standards bodies to adopt them. At this time, the work is about 90 percent complete with regards to existing requirements and completion is expected to be at the beginning of 2019, pending the approval of the final version of the requirement specification.

## Cybersecurity at Stake: How ETSI Cares for It

Charles Brookson, Chairman, ETSI TC CYBER, and Zeata Security Ltd.

ETSI is the recognized regional standards body – European Standards Organization (ESO) – dealing with globally applicable standards for ICT-enabled systems, applications and services across all sectors of industry and society.

We have a special role in Europe. This includes supporting European regulations and legislation through the creation of Harmonised European Standards. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European standards (ENs). We were founded initially to serve European needs, but we have a global perspective and our standards are now used the world over. We have over 800 members drawn from 66 countries across five continents.

TC CYBER has for four years mainly worked on cross-domain cybersecurity, while covering more specific areas, security tools and techniques, if they are not addressed by other ETSI groups. It liaises with many other external groups worldwide and is responsible for turning European requirements into standards. It includes a group on quantum safe cryptography.

We have achieved much during our existence: publications are available on the ETSI web site (www.etsi.org). Major publications include Network Gateway Cyber Defence, Design Requirements Ecosystem, Structured Threat Information Sharing, Secure by Default — Platform Security Technology, Global Cyber Security Ecosystem (a description of all those involved), a series on Critical Security Controls for Effective Cyber Defence, and a Method and Pro Forma for Threat, Vulnerability, Risk Analysis (TVRA) and a report on the implementation of the NIS Directive.

On quantum safe cryptography, for example: Quantum Computing Impact on Security of ICT Systems with Recommendations on Business Continuity and Algorithm Selection, Quantum-Safe Threat Assessment and Quantum Safe Key Exchange.

For the future we have a large number of works in progress, including a series on Middlebox Security, Attribute Based Encryption, Baseline Security Requirements Regarding Sensitive Func-

tions for NFV and Related Platforms and Quantum Safe VPNs, Signatures and Key Exchange.

There are other technical committees within ETSI working on cryptography, smart cards, electronic signatures, IoT and related work in 3GPP on mobile, of which ETSI is a founding partner.

We maintain a strategy to ensure we work on topics that are required, and to avoid duplication with other standards.

We also organize a workshop in June every year where over 200 people join for free during a week at our ETSI Security Week, where we also host other groups to help us all work together and share the latest topics and research. To register link to: http://www.etsi.org/news-events/events/1250-2018-06-security-week.

More information is available at our website: http://www.etsi.org/technologies-clusters/technologies/cyber-security.

## The Challenges of Body Area Networks in IoT

J. Farserotu, ETSI TC SmartBAN Chair;
H. Tanaka, ETSI TC SmartBAN Deputy Chair;
M. Hamalainen, M. Girod-Genet, L. Mucchi,
T. Paso, D. Anzai, and M. Pagnozzi, ETSI Technical Officer

### Introduction

The use of wearables and body sensor devices is rapidly growing in the Internet of Things (IoT). Wireless Body Area Networks (BAN) offer a means of connectivity, facilitating the sharing of data, interaction and interoperability within smart environments, such as smart homes and living environments, as well as, emerging automotive and aerospace applications. The challenges for BAN include interoperability in heterogeneous use cases, low power, low latency, security, robust operation and the ability to interact with embedded intelligence in smart environments. To meet these challenges, the ETSI Technical Committee (TC) SmartBAN (SmartBAN) aims at the realization of a smart BAN with improved and dedicated performance for medical, health, sports and leisure applications. SmartBAN covers communication and the associated physical layer (PHY), medium access control (MAC) layer, network layer, security, Quality-of-Service (QoS) and also provision of generic applications and services. The use of a star network is envisioned around a "smart" hub such as a handset or a watch, with the option for a multi-hop relay. SmartBAN targets a more efficient MAC and PHY, yielding very low latency emergency messaging, very low energy consumption and rapid initial set up time and channel reassignment. It provides additional semantic and data analytic enablers (e.g., semantic discovery, reasoning/rules) and automatic node discovery such as semantic discovery of nodes or composition. It also provides added robustness through forward error correction and it supports operation across heterogeneous networks with enhanced interoperability/connectivity options, including data, network and semantic interoperability.

| Status | Number | Title | Date |
|---|---|---|---|
| Published | TS 103 326 Ver. 1.1.1 | Smart Body Area Network (SmartBAN), Enhanced Ultra-Low Power Physical Layer | 2015-04-28 |
| | TS 103 325 Ver. 1.1.1 | Smart Body Area Network (SmartBAN), Low Complexity Medium Access Control (MAC) for SmartBAN | 2015-04-28 |
| | TS 103 378 Ver. 1.1.1 | Smart Body Area Networks (SmartBAN), Unified data representation formats, semantic and open data mode | 2015-12-11 |
| | TR103 395 Ver. 1.1.1 | Smart Body Area Network (SmartBAN); Measurements and modelling of SmartBAN Radio Frequency (RF) environment | 2016-12-20 |
| | TR103 394 Ver.1.1.1 | Smart Body Area Networks (SmartBAN); System Description | 2018-1-15 |
| In preparation | DTR/SmartBAN-001 | Comparative analysis between SmartBAN and other short-range standards | Q4 2018 (draft), Q3 2019 (approval) |
| | DTS/SmartBAN-004 – TS 103 327 | Smart Body Area Networks (SmartBAN); Service and application standardized enablers and interfaces, APIs and infrastructure for interoperability management | Q3 2018 (publication) |
| | RTS/SmartBAN-005r1 – TS 103 325 | Low complexity MAC and routing for SmartBAN, Draft started (TS 103 325) | Q2 2018 (draft), Q1 2019 (approval) |
| | RTS/SmartBAN-009r1 – TS 103 378 | SmartBAN unified data representation formats, semantic open data model and corresponding ontology | Q1 2019 (publication) |

**Table 1.** Specifications and reports released by ETSI TC SmartBAN.

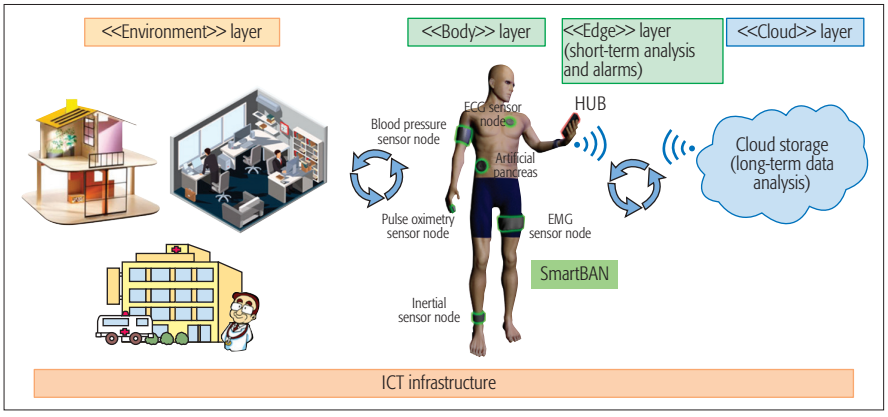


**Figure 1.** Envisioned SmartBAN solutions in the IoT.

### Timeline, Progress and Milestones Achieved

ETSI TC SmartBAN was approved in March 2013. The group has released the specifications and reports listed in Table 1.

Additionally, SmartBAN has collaborated with oneM2M and namely contributed to the ITEA3 CareWare project demonstrator for elderly support at home. In parallel, clinical tests in partnership with OHS (Office d'Hygiène Sociale) based in Nancy, France, are

ongoing. Liaisons with IEC were established in Syc. AAL (Active Assisted Living) and TC124 (Wearable device and technologies).

**Moving Forward**

New work on implant communication was initiated in Q1 2018, in cooperation with ETSI ERM TG 30. Work on security is also expected to start in 2018. A joint group between ETSI TC SmartBAN and ETSI TC SmartM2M is envisioned for merging and/or aligning the SmartBAN ontology with SAREF (Smart Appliances REFerence ontology) and oneM2M ontologies. A workshop is planned on SmartBAN, Connected Things for Wellbeing and Health, in Q4 2018 at ETSI headquarters, France. Demonstrations of SmartBAN technology will be held, including semantic interoperability and the SmartBAN reference IoT/oneM2M platform for remote monitoring and control applications and the SmartBAN 2.4GHz PHY. A dedicated SmartBAN Workshop is also planned in conjunction with the Bodynets 2018 conference to be organized in Oulu, Finland. Beyond this, we envision SmartBAN solutions in the IoT, as illustrated in Figure 1.

**Acknowledgement**

SmartBAN is supported by the Hermes Partnership (www.hermes-europe.net/), a network of leading European organizations in wireless and mobile communication, and the European H2020 ACTIVAGE project (http://www.activageproject.eu/).

## Millimetre Wave: A Key Enabler for 5G

Renato Lombardi, Huawei, Chairman of ETSI ISG mWT

The deployment of 4G, the future needs of 5G and the number of connections required for massive Machine Type Communications in the Internet of Things are making unprecedented demands on radio access networks and backhauling. Millimetre wave technologies are expected to be a major enabler of future mobile communications.

High interest in millimetre-wave bands (30 - 300 GHz) has risen in recent years due to the enormous amount of under-utilized bandwidth that lies in this part of the electromagnetic spectrum and the significant advantages offered in terms of frequency re-usability and large channel bandwidths. As regards backhaul and more general transmission, millimetre-wave offers more spectrum for radio transmission than lower bands, and larger channel bandwidths, delivering fibre-like capacity. The spectrum can be made available readily and can be reused easily, and lower licensing costs mean services can be provided more economically.

However regulations for millimetre wave radio differ greatly from country to country, making it difficult for operators to devise deployment strategies across different countries.

The interest in millimetre-wave technologies has found in the ETSI ISG mWT the proper industry wide platform to create the conditions for large scale usage of this still largely untapped spectrum resource.

In the first years of activity the ISG mWT has significantly grown its recognition in the industry, attracting more than 30 companies (telecommunications network operators, equipment manufacturers, component manufacturers, research institutes) to work together, and gained the reputation for the quality of its publications and for its contributions to forums and events.

In particular, several white papers and group specifications have been published and made available on the web portal of the ISG mWT on the worldwide regulations for the v-band (57 to 66 GHz) and e-band (71 to 86 GHz), technology maturity, applications and use cases of millimetre-wave transmission. Other, more technological publications covered antennas and semiconductor technology.

After the first phase, activities have focused on several other topics:

•Exploitation of the much wider spectrum available above 90 GHz, allowing link capacities up to100 Gbps that led to a Group Report on the spectrum management of the W-band (92 - 114,5 GHz) and the D-band (130 – 174,8 GHz) and describing anticipated scenarios and related channel arrangements. The successful cooperation within the industry led CEPT to recently release the Recommendation on D-Band, with W-Band to follow soon.

•Change of regulations and standards through a Group Report with a detailed interference analysis for systems in the V-Band employing Wireless Gigabit Alliance (WiGig) technology. Realistic approach-based 3D ray-tracing tools can take into account the typical geometry of a high, dense urban environment.

•Extension of the scope of work of the ISG to lower frequency bands used by wireless transmission for backhaul for the purpose of introducing new higher spectrum efficiency concepts and related implications on spectrum regulations, like band and carrier aggregation systems and use cases of Software-Defined Networking as related to microwave and millimetre-wave transmission.

## ETSI Rail Communications Standardization

Robert SARFATI, SYSTRA, Chairman of ETSI Railway Telecommunications Technical Committee; Ingo WENDLER, SBB CFF FFS, UIC Representative at 3GPP

Rail communication, essential for operations, will play an extraordinary role in the digitization and automation of railway production over the next decade. The "Future Railway Mobile Communication System - FRMCS" is a Union Internationale des Chemins de Fer (UIC), the Railroads International Organization set up in 2015 that will play an important role. FRMCS will provide approaches that allow it to follow the different evolutionary speeds in the 3GPP transport system as well as non 3GPP access technologies, e.g., satellite and the necessary functions for communication. Thus, new technologies in radio access can be used for the railway application, without the need for a complete overhaul of the FRMCS concept. This approach is also consistent with the vehicle equipment, also in the sense that new applications are available faster and no major adjustments in the communication architecture are necessary. In general, the aspects of the Service Based Architecture (SBA) are considered in the design of FRMCS, by virtue of SBA being designed to operate virtually, in which different functions can be composed into an end-to-end service over standardized application programming interfaces (APIs).

Another essential aspect is the localization of vehicles and staff. In the future, one would like to do without balises rolled out on the tracks. Accordingly, FRMCS must allow, in addition to the positioning by the radio and/or satellite, other high-precision sources.

FRMCS communication needs rely mainly on the current position of the vehicle or staff. Therefore, FRMCS is strongly oriented to the functions/roles and train number system. For this, the addressing of the users is provided by means of functional aliases.

With the increasing need for mobility of people, the different speed ranges of the available means of transport have to be considered. The railway today stretches on 0-500 km/h. Accordingly, the radio access systems need to cover

the entire speed range. Direct communication between rail vehicles, e.g., virtual coupling, will become increasingly important in the future. FRMCS considers these requirements and will provide a contribution to flexible communication transport solutions. Standardization work started with 3GPP release 15, it will include essential requirements within 3GPP release 16 and continue with additional features such as virtual coupling with 3GPP release 17. The current plan is to have the proof of concept (PoC) and first on site trials by 2022. Rollout of FRMCS is planned within rail by 2025 onward.

## 50 Gigabit Ethernet and Beyond

John D'Ambrosia, Senior Principal Engineer, Futurewei; Chair, IEEE 802.3 Beyond 10 km Optical PHYs Study Group

Ethernet's tale is one that has no end, as it undergoes a seemingly never-ending story of evolution. In December 2017, two new Ethernet standards were ratified. The first standard, IEEE Std 802.3cc-2017, expanded the 25 Gigabit Ethernet (25 GbE) family, as it defined 25 GbE operation over single-mode fiber for reaches of 10 km and 40 km. The other standard, IEEE Std 802.3bs-2017, introduced the 200 Gigabit Ethernet (200 GbE) and 400 Gigabit Ethernet (400 GbE) families, as well as defined 4 level pulse amplitude modulation (PAM4) at 50 Gigabit per second (Gb/s) electrical and optical signaling, as well as 100 Gb/s optical signaling.

Four new efforts are already underway within the IEEE 802.3 Ethernet Working Group, leveraging the 50 Gb/s and 100 Gb/s PAM4 signaling for other applications and physical layer specifications. This work will complete the breadth of the Ethernet families at 50 Gigabit Ethernet (50 GbE), 100 Gigabit Ethernet (100 GbE), 200 GbE, and 400 GbE.

•**IEEE P802.3cd 50 Gb/s, 100 Gb/s, and 200 Gb/s Ethernet Task Force.** In the same manner that 25 GbE evolved from the 25 Gb/s signaling developed to support 100 Gigabit Ethernet (100 GbE), 50Gb/s and 100 Gb/s PAM4 electrical and optical signaling will be leveraged to introduce the new 50 GbE Ethernet rate, as well as expand the 100 GbE and 200 GbE families. For the 50 GbE, 100 GbE, and 200 GbE families, physical specifications, based on 50 Gb/s PAM4 signaling, will be defined for operation over backplanes, copper twin-axial cables, and multi-mode fiber. Additionally, 100 Gb/s PAM4 will be leveraged to define a new single-mode-fiber specification for 100 GbE.

•**IEEE P802.3ck 100 Gb/s, 200 Gb/s, and 400 Gb/s Electrical Interfaces Task Force.** This effort will focus on developing 100 Gb/s electrical signaling and will target electrical interfaces that interconnect chips or to active modules, as well as for backplane and copper twin-axial cables.

•**IEEE P802.3cm 400 Gb/s over Multimode Fiber Task Force.** There are two aspects to this effort. One part will seek to leverage the work of the IEEE P802.3cd project, and define 400 Gb/s operation over multi-mode fiber by using 50 Gb/s over eight parallel muti-mode fibers. The other part of this effort will seek to leverage WDM technology and reduce the eight parallel fibers down to four.

•**IEEE 802.3 Beyond 10 km Optical PHYs Study Group.** While still a study group at the time this article was written, two distinct efforts are emerging. The first effort, which targets mobile backhaul networks, will seek to expand the 50 GbE, 200 GbE, and 400 GbE families by extending their reach to 40 km, assuming PAM4 signaling. The second effort is of particular interest to the cable/multiple system operators (MSO), mobile backhaul networks and DCI application spaces, as the 100 GbE and 400 GbE families will be extended to reaches of 80 km over DWDM systems

The efforts mentioned above represent Ethernet's expansion in a number of ways: expanding the breadth of a given family, developing and leveraging new technologies across multiple rates of Ethernet for new physical layer specifications, and expanding the application spaces and developing new physical layer specifications for them. Also, this work only represents one tangent of Ethernet's tale, as other application spaces, such as building automation, industrial, and automotive Ethernet, are creating entire new Ethernet solutions targeting entirely different physical layer specifications that are needed at relatively lower signaling rates than currently discussed here, but nonetheless, just as important for their respective application spaces.