ETSI World Class Standards

THE STANDARD

News From ETSI · Issue 2, 2017

MADE IN EUROPE FOR GLOBAL USE

Smart Cities Deserve an Easier Task! Standards Will Help.

By Lindsay Frost, chairman of ETSI CIM ISG

The hard task for Smart City decision makers

Smart city managers are facing physical and social challenges which will transform communities for good or for ill: climate change, immigration, resource shortages, waste disposal, aging demographics, renewable energy. Cities are using digital technologies (sensors, IoT, Cloud computing, Big Data analytics) to help cope or even thrive. Their administrators and elected officials have the heavy responsibility of deciding on infrastructure (street lighting, buildings, high-tech industry parks, water works, safety systems, traffic flow systems, eGovernment access) which may take years to build and will be used for decades in order to succeed in a world with many billions of urban citizens.

Continued on page 6 >

An update on our Multi-Access Edge Computing ISG

Written by Alex Reznik, chairman of ETSI MEC ISG

MEC can enable Tactile Internet, Interactive Gaming, Virtual Reality and Industrial Internet

APIs: latest achievements

Recently, ETSI's Multi-Access Edge Computing ISG published its first set of API specifications. This was a culmination of two and a half years' of work and a key step towards enabling a dynamic, rich market of applications that take advantage of Edge Computing. What's the big deal here? Edge computing is widely recognized as a key enabling technology for 5G. One important reason is that edge presence is viewed as absolutely necessary to enable certain 5G classes of use cases. Moreover, MEC can enable many of these use cases with existing 4G technology – i.e. with MEC we don't have to wait for 5G RAN and network to start running 5G applications. Some important examples of use cases that MEC can enable today are Tactile Internet, Interactive Gaming, Virtual Reality and Industrial Internet. All these require extremely low-latency for some application components. As a consequence, physical limitations (i.e. speed of light) prohibit execution of these components in the traditional "deep" cloud and require edge presence. Another set of use cases which is likely to heavily rely on edge computing is "massive" IoT – i.e. IoT where a large number of devices such as sensors are sending a massive amount of data upstream. Market consensus is that pre-filtering of this data at the edge is necessary in order to make the overall system scalable without overloading network and deep cloud compute resources.

Continued on page 8 >

Compliance with the new EU Radio Equipment Directive

On 13 June 2017, the new Radio Equipment Directive became mandatory and the R&TTE Directive can no longer be used to access the European market. This major update of Europe's single market rules for radio equipment was published in May 2014. ETSI's Harmonised European Standards, developed in support of the Directive, are the preferred means for manufacturers to comply with the regulation. Equipment which complies with the Harmonised Standards for this Directive is presumed to comply with the requirements of the Directive. By 13 June 2017, 140 ETSI harmonised standards have been cited in the Official Journal of the European Union, covering most types of radio equipment.

The field of application of this Directive covers a large scope of equipment, ranging from satellite communications to radars to mobile phones, to products operating below 9 kHz such as telecoil hearing aids and sound and TV broadcast receivers. Further examples of equipment covered by the Directive include combinations of multiple radio products in one radio equipment, combinations of radio and IT or electro-technical equipment, RLAN enabled domestic appliances, radio controlled heating systems, radio controlled lighting systems, products including GPS, Wi-Fi, Bluetooth, etc.

Continued on page 2 >

Welcome to the World of Standards

Welcome to this second issue in 2017 of our newsletter, The Standard. We continue to bring you a round up of the recent news from ETSI, together with a mix of background articles.

5G will continue to be an important topic for ETSI and 3GPP for some time yet. So expect to see regular reports of the latest developments in this and future issues. We also have a collection of news from our other partnership project, oneM2M, which is achieving ever greater adoption and recognition in the world of IoT. We continue to hear news from our more recent committees: NFV and OSM, MEC, ENI and CIM among others. Find out what these acronyms mean by reading further!

Of course, the big story at ETSI in recent months has been the preparation of the Harmonised Standards required for the Radio Equipment Directive. We have written about this before, in these pages and elsewhere. We've also held two webinars on the topic. Now that the directive is fully in force standardization work doesn't stop, even if the vast majority of the Harmonised Standards required have now been delivered. So there is still plenty of opportunity to get involved!

Once again,
I hope you enjoy this edition.

Luis Jorge Romero,
Director General, ETSI

Berlin 5G Week

ETSI is pleased to endorse the Berlin 5G Week 2017. Join the tutorials, workshops and conference, hands-on live demonstrations and in-depth technical discussions with leading operators, manufacturers, integrators as well as various solution providers around the most recent 5G hot topics.

For more information visit http://www.berlin5gweek.org

Compliance with the new EU Radio Equipment Directive Continued (from page 1)

ETSI's Harmonised European Standards are developed by our members in our technical committees, with much of the work being done in our committee for Electromagnetic compatibility and Radio spectrum Matters (TC ERM). All of ETSI's Harmonised Standards, like all our other standards and specifications, are freely available from our website. Further information on ETSI's Harmonised standards, including links to download them, is available on our Harmonised Standards web page.

Key facts about the Radio Equipment Directive:

- Manufacturers of relevant equipment now have to comply with the requirements of the Radio Equipment Directive (2014/53/EU) which has replaced the Radio & Telecommunication Terminal Equipment Directive (1999/5/EC). In most cases, Harmonised Standards are available and cited in the Official Journal of the European Union. The latest list of cited standards (8 June 2017) can be found here: http://bit.ly/2vYelzq
- For Safety & EMC requirements (articles 3.1a & 3.1b), manufacturers do not need a cited Harmonised Standard to declare compliance with the Directive, although they still need them to benefit from formal presumption of conformity. If your product is a radio product, you can use the appropriate standards of the EN 301 489 series for EMC (article 3.1b), which are available without charge from the ETSI web site: http://www.etsi.org/standards-search#Pre-defined Collections
- Safety standards are produced by CENELEC: https://www.cenelec.eu/index.html
- If Harmonised Standards are not yet cited in the Official Journal, compliance with the Directive can also be achieved by drawing up a technical file and submitting it to a Notified Body. More details on this can be found in the European Commission's Guide to the RED, available from: http://ec.europa.eu/docsroom/documents/23321

5G is coming soon...

Riding the NB-IoT bicycle

By Matthew Webb, 3GPP rapporteur on Enhancements of NB-IoT (NB_IOTenh)

Participants at the 3GPP RAN (WGs 1, 2, 3, 4, 5, 6) and the SA2 Working Group meetings, hosted by Huawei in Hangzhou in May 2017, have joined an NB-IoT bicycle tour around Hangzhou's beautiful West Lake.

The equipment used is an example NB-IoT use case being deployed in a cellular network in China, as part of a bicycle sharing service 'ofo'. The bicycles are unlocked via a pin from a smartphone - by scanning a QR code on the bicycle. The pin code wakes up the NB-IoT module, which reports to the server then goes back to sleep until the user finishes the ride. When the customer locks the bicycle, the NB-IoT module re-activates to report the journey information and to generate a new pin for the next user. The NB-IoT module can also wake more often to provide other functions, such as periodic location reports.

By installing NB-IoT modules - which are pin-for-pin compatible with GPRS modules in the existing locks - power consumption is much improved, with the stand-by time extended by years, using the same battery.

The swift Release 13 standardization of the 'NB1' category device, followed by the Release 14 enhancements to NB-IoT, completed in March 2017, including multicast, positioning and a reduced 14 dBm power class, have all helped to bring this technology to LPWA (low-power wide-area) IoT products quickly.

With Release 15 now beginning, the evolution of NB-IoT will bring TDD support, increased small cell capability and a number of new techniques to optimize device power consumption for the Internet of Things.

Zhiqin Wang, director of the Institute of Communications Standards Research at the China Academy of Information & Communications Technology (CAICT), said: "With the maturing of the end-to-end ecosystem, since the start of 2017, there are now chipsets, modules, infrastructure, and applications - as the fruit of 3GPP's accelerated standardization of NB-IoT."

The largest of the RAN Working Groups attracts over 700 participants, with around 2000 registrations for the whole week in Hangzhou – meaning that the bikes had to be shared around!

5G-NR workplan for eMBB

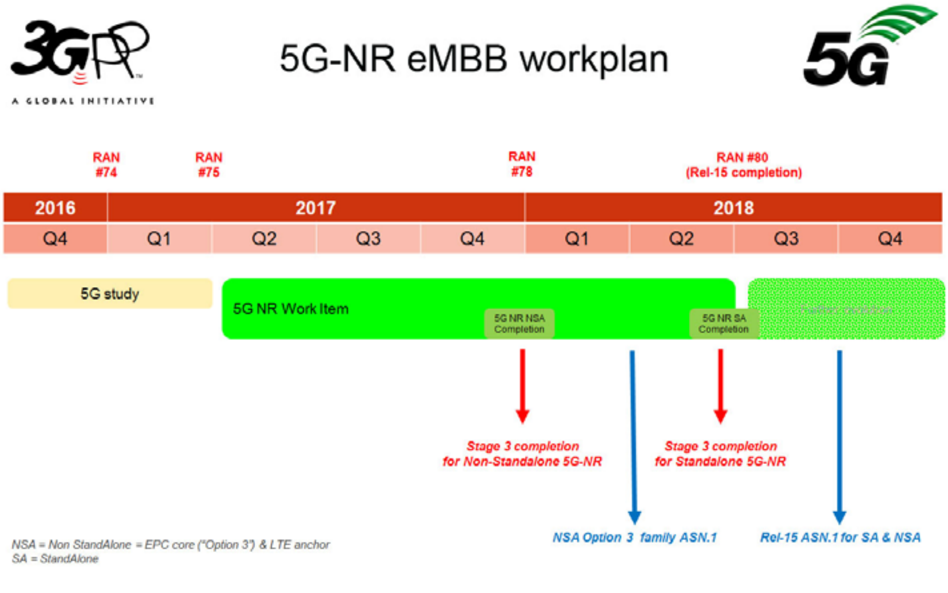
By Dino Flore, 3GPP Outgoing RAN Chairman

A major decision was taken at the beginning of March in 3GPP RAN on the 5G New Radio (NR) workplan. In particular, the group agreed to have an intermediate milestone for the early completion of the Non-standalone (NSA) 5G NR mode for the enhanced Mobile BroadBand (eMBB) use-case. In Non-standalone mode the connection is anchored in LTE while 5G NR carriers are used to boost data-rates and reduce latency.

With the updated workplan, NSA 5G NR will be finalized by March 2018.

At the same time, the group re-stated its commitment to complete the Standalone (SA) 5G NR mode by September 2018 and put in place a plan to achieve that.

To know more about 5G new radio, watch the chairman of 3GPP RAN, Balazs Bertenyi, talk about it: http://bit.ly/2wp6kWm


5G-NR eMBB workplan

3GPP A GLOBAL INITIATIVE
5G
RAN #74
RAN #75
RAN #78
RAN #80 (Rel-15 completion)
2016
2017
2018
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
5G study
5G NR Work Item
5G NR NSA Completion
5G NR SA Completion
Further evolution
Stage 3 completion for Non-Standalone 5G-NR
Stage 3 completion for Standalone 5G-NR
NSA Option 3 family ASN.1
Rel-15 ASN.1 for SA & NSA

NSA = Non StandAlone = EPC core ("Option 3") & LTE anchor
SA = StandAlone

Power Set to be Key Battleground for 5G

By Erik Guttman, 3GPP TSG SA Chairman

As we seek to provide standards for integration with a growing range of 'vertical' business sectors, 3GPP has initiated a new area of API specification work.

At our March 2017 Plenary meeting (SA#75) a new Study on a Common API Framework for 3GPP Northbound APIs was approved and now the SA6 Working Group – responsible for application layer functional elements and interfaces - has started investigating the topic.

In order to provide mobile end-to-end services, 3GPP interfaces exist throughout the system:

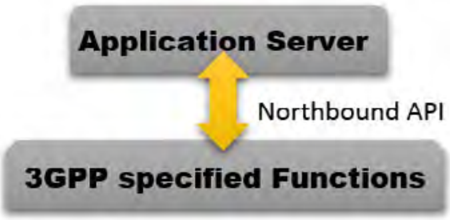
- Between the mobile device and the Radio Network
- Between the Radio Network and the packet core network
- Within the core network
- To external networks
- For management and orchestration, etc.

These interfaces have facilitated the development of a range of diverse equipment, providing a broad range of functionality and services.

Going North

Providing a broader range of standardized services with a wide range of partners has been a goal from the earliest days of 3GPP.

An area where 3GPP has not actively developed standards to achieve this goal is at the 'Northbound Application Programming Interface' level, since the transfer of the Open Service Architecture (OSA) API work to the Open Mobile Alliance (OMA), in 2008.



A Northbound API is an interface between an Application Server (either in a mobile operator's network or external to it - operated by a third party) and the 3GPP system via specified functions in a mobile operator's network.

The new SA6 Study on Common API Framework for 3GPP Northbound APIs will consider their development, specifying common capabilities so that all Northbound APIs function similarly. The figure below, from draft TR 23.722, proposes how this may be achieved.

To realize standardized integration of services with diverse service providers, northbound APIs provide for interaction at the application layer. This makes it possible for mobile network operators to offer a wide range of services beyond prevalent teleservices - voice calls, SMS and data service. Those services can be exposed within the operator network or to third parties in other networks. The figure below is a simple model to illustrate how the Common Framework will develop as the study progresses. The blue lines are defined for all services accessed by northbound APIs – a common framework. The red lines are specific interfaces to deliver a particular service.

The Opportunity

3GPP has actively worked over the past decade to provide additional services in the area of 'machine type communication' (MTC) which delivers the mobile communications part of some important new sectors, including;

- The Internet of Things (IoT)
- Media Broadcast
- Vehicle to Everything (including Vehicle to Vehicle, and other use cases)
- Critical Communications

These activities, particularly those related to broadcast and IoT, have led to an increased interest in standardization of northbound APIs. In Release 14, the "eMBMS Delivery of Media and TV Services" feature provides broadcasters with the ability to directly integrate their services with mobile network operators over standardized interfaces to the 3GPP system. In Release 15, to correspond with oneM2M release 2, 3GPP will include functionality to directly expose Cellular IoT and MTC capabilities via northbound APIs.

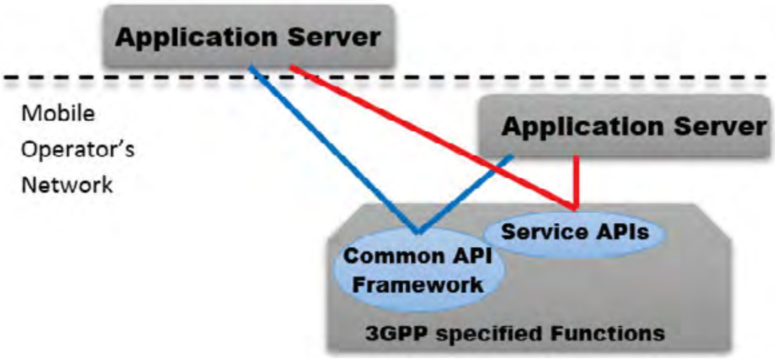
This expanding activity across 3GPP has provided the impetus for this new Study on Common API Framework (FS_CAPIF), which has begun to consider common aspects of northbound APIs. The study will focus on architectural aspects such as registration, discovery and identity management that generally apply to all services. Common API Framework functions could be achieved uniformly for such capabilities as Service API discovery, monitoring and charging.

FS_CAPIF takes into account both the work ongoing within 3GPP as well as frameworks defined by other organizations. It aims to provide recommendations for specific architectural solutions that can subsequently be standardized. At this stage, requirements and issues have been identified and a gap analysis of existing solutions has begun.

While the scope of the study is general to all northbound APIs it is important to support the specific needs of individual vertical service offerings as well. For example, work on broadcast interfaces has benefited from the participation of 3GPP member organizations actively providing broadcasting services. Similarly, MTC–related service exposure is coordinated directly with oneM2M and involves a wide range of other participants.

Looking to 5G

3GPP currently focusses significant resources on developing 5G standards. 5G aims to provide distinctive performance and capabilities to meet the needs of specific services. This will intensify the existing focus on integration with service providers in different service domains (often called 'vertical industries'). One aspect of this may be a broadening range of northbound APIs designed to expose the capabilities and resources of 3GPP operators' networks and the broad range of devices communicating over them.



Mission Critical Services in 3GPP

By Yannick Lair and Georg Mayer

A platform for Mission Critical (MC) Communications and MC Services has been a key priority of 3GPP in recent years and is expected to evolve by taking more requirements on board from different sectors of the global critical communications industry.

This article provides an overview of what was achieved so far in the MC domain within 3GPP and also gives an outlook of what can be expected in the near future. We plan to create a more detailed paper on MC Services, which will summarize the use cases and functional aspects of Rel-13, Rel-14 and upcoming Rel-15, later this year.

Driven by the 3GPP release schedule, the mission critical related functionalities have been phased across them, each release encompassing a complete set of standards for equipment vendors and operators to phase their implementations and deployments, based on market demands.

Early Mission Critical Enablers

Prior to Rel-13, 3GPP standardized functionality that was later to serve as an enabler for MC Services. For example, MC Services benefit from the use of multicast bearers in LTE due to the standardization of eMBMS and Group Communication System Enablers (GCSE). Additionally, D2D Proximity Based Services (ProSe) was enhanced to support public safety use.

This allows public safety operators to determine whether critical communications occur on-network using the LTE network infrastructure, or off-network without the use of the LTE network infrastructure, or both.

Mission Critical Push to Talk in 3GPP Rel-13

3GPP entered the application domain by standardizing Mission Critical Push to Talk (MCPTT) in Rel-13, completed in 2016. To provide organizational support and focus, a new working group - SA6 - was established in order to complete the new application related work in concert with other 3GPP working groups in less than one and a half years - by March 2016.

By achieving this challenging goal, 3GPP not only honoured its commitment to the mission critical industries but also demonstrated its ability to take on new, application related work and to complete it within a set timeline.

Mission Critical Services in 3GPP Rel-14

MCPTT was the first major step in a series of MC Services and functionalities demanded by the market. In Rel-14, completed in 2017, 3GPP added additional MC Services and enhancements to its repertoire of standardized applications, specifically:

- Enhancements to MCPTT
- MC Data
- MC Video
- General framework which facilitates standardizing additional MC Services

The Rel-14 work on MC Services required not only a large set of new protocol additions and new security functionality, but also enhancements to the MCPTT Rel-13 specifications to enable reuse of common functionality across MC Services. Given the tight timeline for Rel-14 and with an eye on the upcoming 5G work, the MC Services were split into smaller, self-contained features in order to allow 3GPP to finish the majority of them in Rel-14, by September 2017, and to complete the remaining features in Rel-15, due to be completed in June 2018.

The MC Services introduced in Rel-14 offer stand-alone functionality that enriches the existing base of MC Services. The set of features included was carefully chosen so that implementers need not have to wait for the completion of additional standardized functionality in Rel-15. The Rel-14 MC Video and MC Data specifications therefore offer equipment vendors as well as network operators a consistent and fully specified set of standards, ready for initial implementation and deployment.

A detailed list of the functionalities completed in Rel-14 and Rel-15 respectively, can be found on 3GPP website.

Mission Critical Services and Industry Specific Requirements in 3GPP Rel-15 and beyond

All 3GPP working groups have already started work on Rel-15, the first release of the 5G system. In addition, 3GPP is also working on service requirements for Rel-16, the second release of the 5G system.

In Rel-15, the MC Services are further evolved. In addition to that, 3GPP is currently evaluating and studying further MC related topics for Rel-15 and beyond, in particular:

- Interconnection between 3GPP defined MC systems
- Interworking between the 3GPP defined MC system and legacy systems such as TETRA or P25, for voice and short data service
- MC Service requirements from railway industries
- MBMS APIs for MC Services
- MC Service requirements from maritime industries

Conformance test standards for MC Services are also being developed within 3GPP. The initial set of test specifications on conformance testing Rel-13 MCPTT is expected to be available by the end of 2017. Subsequently, conformance test specifications for Rel-14 and Rel-15 feature sets will be developed.

Smart Cities Deserve an Easier Task! Standards Will Help.

Continued (from page 1)

By Lindsay Frost, chairman of ETSI CIM ISG

Not only do the new technologies have a "steep learning curve", the interactions between the various systems are hard to predict (improved traffic flow may increase air pollution in some areas, reduce it in others; electrical vehicle charging may overload the power grid or - properly managed - help optimize for short-term solar-energy fluctuations). Not only are the technologies complex, the variety of options is enormous (dozens of wireless communication technologies, hundreds of IoT specifications) and the advantages/disadvantages of each depend on the use case(s).

Furthermore, the constraints on public procurement (limited funds, need for transparency and "paper trails" which all consume time/money) are in contrast to the great urgency in solving huge social, economic and resource-efficiency issues fast enough so as to actually benefit citizens. There is even the painful constraint of too few trained experts for writing the RFQs and for analysing both the "state of play" for competing standards and the validity of commercial offerings.

Standards can help in overcoming all of these issues, as described below.

Standards improve interoperability, help avoid "vendor lock-in", improve economies of scale and provide cost savings

How standards can help

Standards are consensus agreements on specifications of technical solutions, so they automatically improve interoperability, help avoid "vendor lock-in", improve economies of scale and provide cost savings. If market or regulatory forces recommend or require certain standards, it helps create a common market, which also improves global market access for products, reduces risk of obsolescence and of cost explosions. Additionally, standardization helps in bringing experts together and aligning interests of stakeholders, dissemination of knowledge and creation of an ecosystem.

The speed of reaching consensus depends on the breadth and impact of the topic, as well as the importance of ensuring interoperability of all systems. ETSI Industry Specification Groups are set up to allow a wide selection of stakeholders to reach consensus quickly.

How ETSI, CEN, CENELEC and ITU are collaborating to provide the standardization tools

The three European Standardization Organization (ESOs) are CEN, CENELEC and ETSI and they each are tasked by the EU to create (harmonized) standards referenceable in government regulations and procurement. They have separate topics of responsibility which however overlap strongly for use cases in the Smart Cities domain. Therefore a joint collaboration committee has been set up, called Sector Focus for Smart and Sustainable Cities and Communities (SF-SSCC), which held its second meeting on 4 June in ETSI headquarters. One of its first tasks is to combine several existing "standardization landscape" overviews from ETSI, CEN/CENELEC, EU projects like ESPRESSO (http://espresso.ru.uni-kl.de) and industry bodies like AIOTI (www.aioti.eu) into one updateable categorized reference list of those EU standards relevant to smart city solutions.

ETSI ISG CIM chairman recently went to the first regular meeting of the new ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities. That focus group now has 5 working groups, is open to many organizations, such as oneM2M, IEC/ISO, the UN, NIST, etc. and is tasked to recommend what further standardization is needed to help smart cities realize a vibrant interoperable data ecosystem.

ETSI work on Information Management for Smart Cities

ETSI is a founding (Type 1) partner of oneM2M, which has for some years been consolidating IoT functions in one platform and has in the last year begun work on semantic interoperability between various device access protocols and cloud applications.

ETSI has begun focused work in the area of data processing and management by establishing in February an Industry Standardization Group for cross-domain Context Information Management. This was in response to a perceived lack of other activities supporting interoperability and integration of data from multiple different "verticals" e.g. from the IoT domains, the city administration and/or open data domains and the 3rd-party application developer domains.

The launch of the ISG CIM was reported here in February. The key goal of the group (supported by 24 organizations so far) is to collaborate with stakeholders from all parts of the smart city ecosystem (EuroCities, SharingCities, FutureCatapult, OASC), from various IoT areas (oneM2M, TMForum, GSMA), from key players in knowledge management (OGC, W3C, various academic institutions) and of course from within ETSI itself (ETSI TC SmartM2M, ETSI TC CYBER, ETSI TC ATTM), to recommend how to achieve information integration (preferably with minimal new specifications).

Re-use of (Context) Information by various applications, different from the one(s) collecting the original data, is a persistent weakness in the open data and open government movement of the last decade. Part of the problem is that the "hidden assumptions" about the provenance, quality, timeliness and ownership/licensing of data is seldom available to external users. And even if it is in principle available, it is seldom fully machine-readable, which is a requirement for data manipulation by machine learning and AI-recommendation systems.

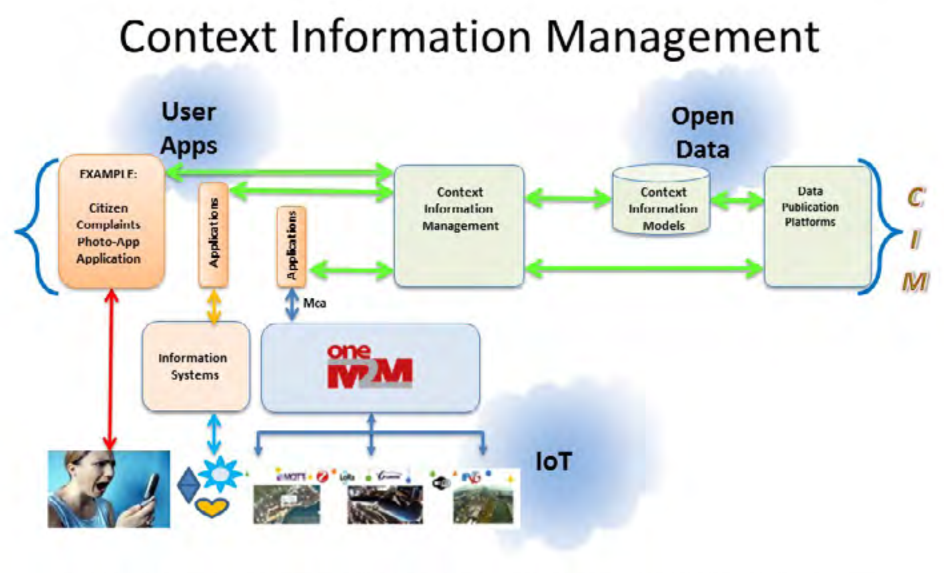
What is ETSI ISG CIM, what are the benefits, what influence should Smart Cities exert?

The mission of ETSI ISG CIM is basically to "see how to make collected information more useful", i.e. to identify mechanisms (protocols) to publish, discover, and re-use data from diverse domains. The figure shows the currently discussed domains of User Applications, Smart City databases and Internet-of-Things.

There is already substantial material about the forms of information to be shared arising from the Internet of Things. Likewise there are substantial examples and analyses of the forms of information which are, or might be, "published" by 3rd party applications in the Cloud or installed on mobile phones. Combining these two forms of information has become quite common, using various proprietary approaches. Missing from the combinations,

Smart Cities Deserve an Easier Task! Standards Will Help.

Continued (from page 6)


Context Information Management
User Apps
Open Data
EXAMPLE:
Citizen Complaints Photo-App Application
Applications
Applications
Context Information Management
Context Information Models
Data Publication Platforms
C
I
M
Mca
Information Systems
oneM2M
IoT

Goal = interoperable exchange of data & metadata between systems

however, are many practical examples from Smart Cities about integrating the existing/installed databases and their contents. Some examples exist, particularly from the Geospatial data (e.g. INSPIRE Directive) and Linked & Open Data domains (e.g. OpenAIRE www.openaire.eu), but again the integration with other domains has been proprietary.

How Smart Cities can guide the SDOs

ETSI ISG CIM is collaborating with other SDOs and organizations, meeting with many relevant EC H2020 projects, and has contacts with several Smart City alliances, however the "street level" expertise and critique from smart city technicians and elected officials is still desperately needed. Amongst the many successful (or partially successful) smart city trials is a wealth of knowledge which must be taken into account. Readers who have such experience (or can recommend others) are strongly encouraged to contact ISGsupport@etsi.org to find out how their use cases can be taken into account.

ETSI is encouraging the creation of further technical groups to promote such knowledge exchange and Smart City employees should please "watch this space" in the next few months.

“Making Smart Cities Sustainable”: ETSI workshop in Bordeaux

> ***“As a city, it was important to be involved in the standardization process as we foresee long term implementation and investment.”***
>
> - Christophe Colinet, Bordeaux Metropole chairman ETSI ATTM SDMC

With over 50% of the world’s population living in urban areas, making smart cities sustainable is a key urban development goal. To tackle this challenge, ETSI organized a workshop, together with showcases and demonstrations, in partnership with Bordeaux Metropole, eG4u and the Sharing Cities Project in June 2017. This two-day event was hosted by Bordeaux Metropole and the City of Bordeaux and supported by the European Commission and Eurocities, a network of over 140 European cities. Speakers and participating organizations originated from both public and private sectors. They looked into key global implementations and examined major technology and social challenges that need to be faced in order to roll out smart city services.

Offering sustainable and resilient new services for citizens and cities implies huge investments on the long term. Therefore large scale deployments have to be standards-based to prevent vendor lock-in and need to include key indicators to evaluate and evolve technology maturity. The topics addressed during the workshop helped identify the main technology trends for smart cities, taking into account major industry initiatives.

“In Bordeaux, the mayor implemented the Bordeaux Digital City programme, aligned with COP 21 requirements”, said Christophe Colinet, chairman of the ETSI working group on Sustainable Digital Multiservice Cities. *“As a city, it was important to be involved in the standardization process as we foresee long term implementation and investment.”*

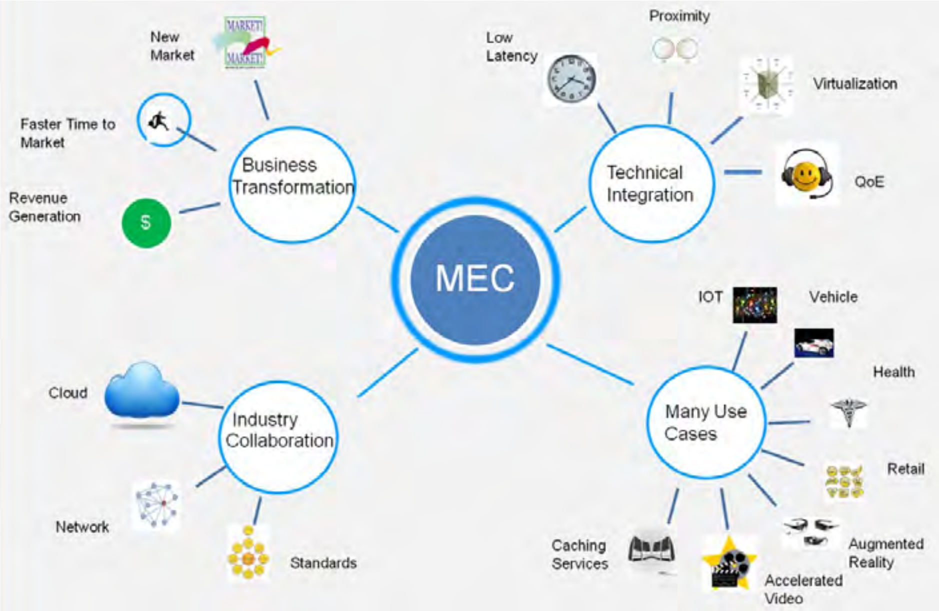
The first day of the event described trials and field developments in various locations including the cities of Bordeaux and Milan, ongoing projects in Eurocities, and projects funded by the European Commission. It also provided an overview of urban data platforms: the digital networking of various ICT solutions in urban areas.

The second day addressed IoT and sustainable ICT deployments and how to bring innovation to the eco system level with a focus on smart home, smart buildings and smart cities.

Attendees had the chance to view multi-vendor showcase projects, offering first-hand knowledge and insight about sustainable smart city technologies. These showcases helped strengthen strategic planning and decision-making, and identify which digital solutions may be more viable in the cities. Showcases covered technologies and solutions such as centralized energy or traffic controls as well as optical fiber home networks.

An update on our Multi-Access Edge Computing ISG

Continued (from page 1) Written by Alex Reznik, chairman of ETSI MEC ISG



MEC Market Drivers

A complex ecosystem

Notably, the edge computing ecosystem is more complex than a typical telecom ecosystem. It includes providers of user connectivity – which are often Communication Service Providers (CSPs), but can also be new players such as enterprises deploying private LTE networks; providers of edge platforms; and third party application developers. It may also include other players such as typical cloud service providers, enterprises, etc. Each one of these ecosystem participants has their own role. For example, CSPs provide the capability to deploy a "cloud" at the edge of their access networks. Additionally, CSP may expose certain information available in the access network as a value-added service to the applications. CSPs may also run certain key VNFs on their own edge cloud. Third parties develop applications which run on the edge clouds that CSPs deploy and create value from the information exposed via MEC services. Interaction between CSPs and application providers may be direct or may be facilitated by a typical cloud service provider. Finally, all of this is enabled by an edge platform that provides the required services to authorized applications.

Even ecosystems with lower complexity than that of multi-access edge computing can suffer from lack of interoperability. Given the complexity of the edge computing ecosystem and the critical importance of this technology to 5G, such a situation would create significant issues in our industry. ETSI ISG on Multi-access Edge Computing (MEC) was created 2.5 years ago precisely to address this problem. By defining and standardizing key edge computing interfaces, ETSI ISG MEC eases the path to interoperability and removes this key obstacle towards a broad industry adoption of edge computing. It should be noted here that while several industry groups and open source projects are currently focused on edge computing, ETSI ISG MEC remains the only standardization group in this space.

Main accomplishments of the only standardization group in this space

So what have we actually accomplished to date? Well, building on the use cases, requirements derived from these use cases and reference architecture (which defined, among other entities, what a MEC Platform is), we have published API specifications for a good portion of the APIs we identified as being in scope for Phase 1 of our work. These include specifications relating to the essential functionality of the application enablement platform (API framework), specific service-related APIs (Radio Network Information and Location Information) and management and orchestration-related APIs. The APIs are designed to be application-developer friendly and easy to implement so as to stimulate innovation and foster the development of applications.

The MEC application enablement is a generic framework which is applicable for every environment that aims to open up the network and expose information towards authorized third-party applications. Utilizing a unique API framework across the industry ensures common practices for developers when interfacing their applications with the operator's system. This can promote innovation and accelerate the development of third-party applications, enabling operators to capitalize their networks.

ETSI ISG MEC is the only standardization group in this technology

The MEC API principles provide generic guidance for the development of APIs. Compliance with these principles ensures consistency and an easy-to-implement set of APIs for the use of developers. Developing APIs across the industry in line with a common set of principles can accelerate the adoption of the APIs by the developers, encourage the creation of innovative applications and ensure the cost-efficient development of APIs.

We also released standard APIs for two key value-add services: Radio Network Information Service (RNIS) and Location Service. Notably, to complement the API definitions and offer increased accessibility to ETSI specifications, ETSI MEC ISG is providing supplementary machine-readable description files compliant to the OpenAPI Specification. The file for each API is available for download at ETSI's new Forge platform. Check them out here: https://forge.etsi.org/rep/gitweb.cgi

We further released information-model level specification of application life-cycle, rules and requirements management. These are essential to facilitate the running of applications at the optimal place at the right time and supporting relocation of an application instance as needed.

Clearly, we are not done. We still have some work to finish. API specifications for the user equipment-initiated operations, platform management as well as UE identity and Bandwidth Management services should be completed shortly. More importantly, we have already embarked on Phase 2 of our work which will expand applicability of our standards from mobile to all types of access. Phase 2 will also define how MEC integrates with NFV and address significant new use cases, such as connected cars. Phase 2 should also see an increased emphasis on our industry outreach with growing action to move towards adoption of our APIs by the key industry groups, certification and application developer outreach.

ETSI releases specifications for Licensed Shared Access

Enabling spectrum sharing and improved Quality of Service

The ETSI Technical Committee for Reconfigurable Radio Systems (TC RRS) announced the completion of the specification for the support of Licensed Shared Access (LSA) in April 2017. This provides a means to enable spectrum sharing coordination between LSA licensees and existing spectrum licensees, thereby ensuring Quality of Service (QoS).

The recently completed specification, ETSI TS 103 379 addresses information elements and protocols for the operation of Licensed Shared Access in the 2 300 MHz - 2 400 MHz band. The document defines the application protocol, also known as LSA1 protocol, on the interface between the LSA Controller and the LSA Repository, and the content of the information conveyed by this protocol.

With this new specification, ETSI TC RRS completes a set of specifications that opens the way for interoperable implementation of LSA Repositories and LSA Controllers to support LSA deployments in the initial target band (2 300 MHz - 2 400 MHz). Extensions to other bands are not precluded, in response to future regulatory requirements. It is the intention to take such future requirements as well as additional features into consideration when starting a new release of the LSA specifications.

The ETSI work was initiated in response to the European Commission's Mandate M/512 on RRS, and closely followed related CEPT work, particularly the ECC Report 205 on "Licensed Shared Access". It completes and complements existing ETSI specifications.

"Licensed Shared Access based spectrum sharing is expected to be a key element to address future 5G spectrum needs"

In addition, ETSI TC RRS has started new work to address the different technical possibilities for local high-quality wireless networks to access spectrum temporarily on a shared basis. A Technical Report will be finalized during this year.

ETSI Multi-access Edge Computing starts second phase and renews leadership team

Addressing current and future heterogeneous networks

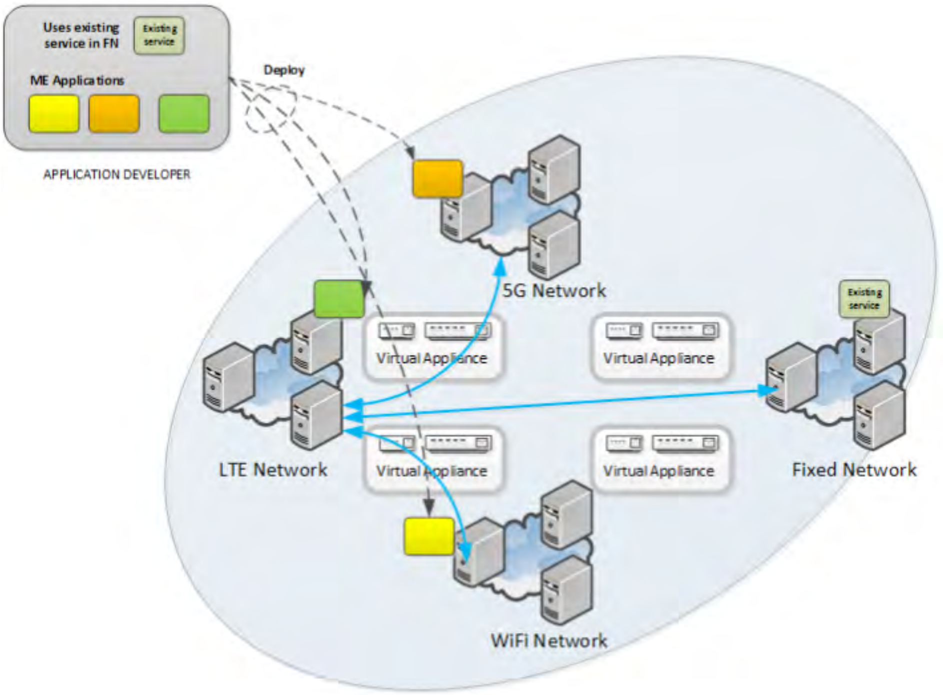
ETSI's Multi-access Edge Computing (MEC) Industry Specification Group has a new name, a new leadership team and a new scope that extends beyond its original focus on Mobile Edge Computing for mobile access networks.

At the 9th meeting of ETSI MEC, held on 13-17 March in Sophia Antipolis, France, Alex Reznik from Hewlett-Packard Enterprise was elected as the new chairman. Pekka Kuure and Sami Kekki, respectively from Nokia and Huawei, were elected as new vice chairs, while Adrian Neal, from Vodafone, was re-elected as vice chair.

ETSI's Mobile Edge Computing Industry Specification Group has been renamed to Multi-access Edge Computing to embrace the challenges in the second phase of work and better reflect non-cellular operators' requirements. The scope of the group has expanded to address multiple MEC hosts being deployed in many different networks, owned by various operators and running edge applications in a collaborative manner. Future work will take into account heterogeneous networks using LTE™, 5G, fixed and WiFi technologies. Additional features of the current work include developer friendly and standard APIs, standards based interfaces among multi-access hosts and an alignment with NFV architecture.

The MEC system will provide a standardized and open system able to support different virtualization techniques, with the capability for an application to discover applications and services available on other hosts, and to direct requests and data to one or more hosts. These features among others will lead to a system offering standard APIs, management interfaces with orchestrator and virtualized infrastructure, standardized interfaces between MEC hosts for traffic as well as service routing or application relocation, and standardized interfaces with transport networks.

"In phase 2, we are expanding our horizons and addressing challenges associated with the multiplicity of hosts and stakeholders. The goal is to enable a complete multi-access edge computing system able to address the wide range of use cases which require edge computing, including IoT," says Alex Reznik, chairman of MEC ISG. *"We will continue to work closely with 3GPP, ETSI NFV ISG and other SDOs as well as key industry organizations to ensure that edge computing applications can be developed to a standardized, broadly adopted platform."*



ETSI Open Source MANO announces Release TWO

Advanced interoperability, scalability and hybrid cloud capabilities to meet operators' needs

Continuing to meet operators' needs for predictable, high-quality open source MANO releases, the ETSI Open Source MANO group (ETSI OSM) announced OSM Release TWO on 27 April 2017. This release brings significant improvements in terms of interoperability, performance, stability, security, and resources footprint to meet operators' requirements for trials and upcoming RFx processes.

New features of Release TWO include:

- SDN assistance to interconnect traffic-intensive virtual network functions with on-demand underlay networks.
- Support for deployments in hybrid clouds through a newly developed Amazon Web Services plugin.
- OSM's plugin model for major SDN controllers has been extended with ONOS, which joins ODL and FloodLight in the list of supported controllers.
- Dynamic network services to scale resources on demand.
- Multiple installer options to ease OSM installation in different environments.

The new SDN capabilities enable advanced types of underlay connectivity that are often unavailable in a non-customized, virtualized infrastructure manager (VIM), thus avoiding performance degradation. This is transparent for operators, who only need to request the right type of connectivity in their virtual network functions or network service descriptors without concerns about the need for special hardware, server wiring or manual post-deployment intervention. This feature completes the first full implementation of the ETSI NFV specification on "NFV Performance and Portability Best Practices" (ETSI GS NFV-PER 001).

"The SDN assistance in Release TWO is a huge leap forward to enable full automation of key operators' use cases with the most popular VIMs on the market", says Francisco-Javier Ramón, chairman of ETSI OSM group.

"AWS support allows automation of NFV deployments in public clouds or in hybrid multi-site scenarios so that developers and testers of OSM and NFV orchestration will no longer need to set up a private cloud to run basic NFV use cases and tests," adds Andy Reid, vice chairman of ETSI OSM.

A comprehensive description of the new features that come with OSM Release TWO can be found in the new white paper from the OSM Community.

ETSI's Open Source MANO announced its newest members in February 2017, with Atos, CableLabs and Verizon joining the group making a total of 60 organizations working together to shape NFV networks in the largest open source MANO initiative. It has grown from eight founding members to a total of 60 organizations, including 8 network operators (Bell Mobility, BT, PT Portugal Telecom, SK Telecom, Sprint, Telefonica, Telenor and Verizon).

25-27 September 2017, Berlin

See MEC technology live in action!

https://tmt.knect365.com/meccongress/

ETSI Workshops – recorded

Two of our recent workshops have been recorded and made available online. As well as recording the presentations, we have also captured the panel sessions and concluding remarks at each event.

ETSI 5G Infrastructure Summit

This year's ETSI Summit, held on 6 April, was on the topic of 5G network infrastructure. This 2017 ETSI summit focused on the technological solutions that will be needed in order to enable true scalable mobility and to fulfil the ambitious 5G requirements, in terms of performance, reliability, energy efficiency and security.
Watch the videos: http://bit.ly/2i8V1iK
Full event details: http://bit.ly/2i9QjS7

Security Week - eIDAS workshop

The eIDAS workshop, held on 13 June during the ETSI Security Week, reviewed the state of play one year after the entry in application of the eIDAS Regulation.
Watch the videos: http://bit.ly/2w55PnZ
Full event details: http://bit.ly/2sznHFM

Webinars

Don't forget to follow the ETSI Webinar channel and watch our webinars on such topics as the Radio Equipment Directive or tutorials on NFV.
http://bit.ly/2fO7szT

Videos

View all of ETSI's videos online on our YouTube channel, or our Vimeo channel: www.youtube.com/etsiorgstandards, www.vimeo.com/etsi

Outstanding results for the first ETSI NFV interoperability test event

ETSI has just released the results of its two-week NFV Plugtests™ event that took place from 23 January to 3 February in Spain. For features such as network service on-boarding, instantiation and termination, 98% of the interoperability tests succeeded. For more complex operations like scaling and network service updates, very encouraging initial results were observed. The test plan, overall results and lessons learnt during the Plugtests are fed back to ETSI NFV ISG.

35 commercial and open source implementations were tested for interoperability, including 15 virtual network functions, 9 management and orchestration solutions and 11 NFV platforms. More than 160 engineers were involved in the preparation of the Plugtests, 80 of them on-site, coming from a diverse community of NFV implementers, including vendors and key Open Source projects such as ETSI OSM, Open Baton, OPEN-O and OPNFV.

In a pre-testing and remote integration phase launched in November 2016, 29 remote labs were connected to the ETSI Plugtests network to ensure interconnection and integration among the different Virtualized Network Functions (VNFs), Management and Orchestration (MANO) solutions and NFV platforms participating in the Plugtests.

During the two week intense testing phase, test sessions were organized in several parallel tracks, ensuring that all participants had at least one test session scheduled any time and that a maximum number of combinations could be tested. Each day 10 different combinations of MANO and VIM&NFVI (NFV platform) were scheduled, with up to 4 VNFs to be tested on each of them during the day. Overall, 160 different combinations of VNF, MANO and VIM&NFVI were tested for interoperability and over 1500 individual test results were reported.

The test plan developed by ETSI's Center for Testing and Interoperability, focused on validating ETSI NFV Release 2 end-to-end capabilities including management of descriptors and software images, as well as life cycle management of network services and virtual network functions. It consisted of 26 test cases, classified in several groups going from onboarding and instantiation, through different types of scaling and network service updates to terminate and teardown operations.

"The results for the setup and termination groups were near perfect, achieving almost 100% success for both", says Pierre Lynch, vice chairman of the NFV Testing, Implementation and Open Source working group. *"The results for the 3 other groups, while encouraging, showed that there is still work to be done on those areas. But this is to be expected, since the scale operations are quite complex, and the specifications have not been completed yet. Receiving feedback on the stage 2 specifications is valuable for the ETSI NFV ISG as they are currently working on data modelling and can take those into account."*

The first ETSI NFV Plugtests report is available on ETSI portal.

And if you missed this great event, have a glance at our video https://www.youtube.com/watch?v=MpWR4pu8FoE

Or come to our second ETSI NFV Plugtests event which will take place on 15-19 January 2018 at ETSI headquarters!

ETSI

First NFV Plugtests™ event

Leganes, Spain - January 2017

> ***"The results for the setup and termination groups were near perfect, achieving almost 100% success for both"***

SDN NFV World Congress 2017

SDN NFV WORLD CONGRESS
9-13 October 2017 The Hague, Netherlands
LAYER123
T
Accelerating Innovation for Networks

9-13 October 2017, The Hague, Netherlands

ETSI is pleased to endorse Layer123's SDN NFV World Congress, taking place in The Hague, Netherlands.

Members of the ETSI NFV leadership team will contribute to the conference programme. Don't miss the opportunity to obtain first-hand information on ETSI and how to contribute to its NFV standardization activities by visiting the ETSI exhibition stand.

For more information on the NFV World Congress visit the event website at: https://www.layer123.com/sdn

oneM2M's Interop 4 sees IoT standardization gain momentum

IoT interoperability and standardization has advanced significantly in Taiwan after oneM2M held its fourth interoperability testing event in Taipei, on 19 June 2017.

Interop 4 gave organizations implementing oneM2M standards the opportunity to check end-to-end functionality via oneM2M interfaces and validate interoperability, with a total of 13 companies taking part. A conference held the day before the event featured presentations from leading companies and members of oneM2M's leadership team to promote oneM2M to Taiwanese businesses in the IoT sector.

The event was held as the Asian Silicon Valley Development Agency (ASVDA) works to transform and upgrade Taiwan's industrial infrastructure with IoT technology. Taiwan aims to have a five percent stake in the global IoT market by 2025.

"Taiwan is looking to become a major player in the IoT and oneM2M Interop 4 helped drive this goal by giving organizations in the country and the wider Asia region the opportunity to test and improve their deployments," said JaeSeung Song, Associate Professor at Sejong University and Test Working Group Chair at oneM2M. *"Interop 4 was our second interoperability event of the year and its success highlights the continuous growth of oneM2M's standards."*

Hosted by TTA and ETSI – two of oneM2M's founding partners – along with the Taiwan-based Institute for Information Industry (III), Interop 4 allowed participants to take part in interoperability scenarios from oneM2M's testing specification, TS-0013. Testing at the event was based on oneM2M's Release 1 and Release 2 sets of standards, and covered functional architecture, service layer core protocol and CoAP, HTTP, MQTT and WebSocket protocol binding.

The event allowed companies to check interoperability levels of their implementations and ensure they had interpreted oneM2M's standards correctly. Conformance testing to help debug products was also available.

The full list of organizations which participated in this event is: Spirent Technologies, Institute for Information Industry, NTT, TTA, Sporton, DEKRA, KETI, C-DOT, ETRI, Sejong University, Easy Global Market, nTels Co., and Sensinov.

oneM2M's Interop events are open to all companies interested in testing their products for interoperability. For more information on upcoming events, visit www.onem2m.org.

> ***"The success of Interop 4 highlights the continuous growth of oneM2M's standards"***

oneM2M selects TTA as its global testing and certification organization

oneM2M has chosen the Telecommunications Technology Association (TTA) of Korea as its global testing and certification organization to help drive the certification of its standards.

As oneM2M's global certification body, TTA will provide certification and testing services to oneM2M members as well as to non-members that have implemented oneM2M solutions.

It has already developed test specifications, certification test equipment, certification logos and the official oneM2M certification homepage.

TTA has also secured the latest test certification technology through its interoperability event jointly held twice a year with the European Telecommunications Standards Institute (ETSI). With the launch, Korean companies KT Corporation, SK Telecom, KEPKO and NTELS, have been awarded the first official certification for four of their products.

Looking towards the future, TTA will continue to help to expand the certification services by testing new standards developed by the oneM2M working groups, which will benefit the IoT and M2M industry significantly.

TTA has been providing a oneM2M certification service since 2014 to ensure compatibility of oneM2M products and as the official oneM2M testing and certification organization, will continue to expand the testing and certification service by keeping up-to-date with oneM2M standards and further collaborate with overseas testing institutes to provide feedback on the standards.

Following the announcement, TTA President Park-Jae-Moon said: *"TTA's cooperation with oneM2M has made the world's first global certification system in the IoT field. In the second half of this year, TTA will provide testing and certification services for various IoT technologies leading the global market by opening [the] Global IoT test Certification Centre."*

For more information, visit: http://www.onem2mcert.com

ETSI IoT week

23-26 October 2017
ETSI, Sophia Antipolis

ETSI's IoT Week - Standards & Technologies for the Smart World has become a must-attend event for anyone involved in IoT solutions, to appreciate the power and the value of the technologies enabled by the standards.

For more information, go to: http://www.etsi.org/etsi-iot-week-2017

IoT standards groups emphasized collaboration at oneM2M Industry Day

OCF, Zigbee Alliance, Thread, IIC, HPE, InterDigital, Qualcomm, iconectiv, AT&T and TTA highlight ways to accelerate IoT deployments

Leading technology companies from around the world gathered to advance adoption of the Internet of Things (IoT) through increased industry cooperation, as the global IoT standards initiative oneM2M held its second successful Industry Day on Wednesday, 13 July in Memphis, TN, USA.

HPE, InterDigital, Qualcomm, AT&T and iconectiv all took part in the conference that was hosted by oneM2M North American partner ATIS. oneM2M's goal is to further collaboration on IoT initiatives and accelerate adoption through a standards-based approach. Representatives of industry groups Open Connectivity Foundation (OCF), Zigbee Alliance, Thread and Industrial Internet Consortium (IIC), as well as one of oneM2M's founding partners TTA, presented ways in which their initiatives complement oneM2M activity.

"IoT is about device and application proliferation and oneM2M is working to lay the foundation of an IoT data economy through an interoperable approach to both domain-specific and cross-domain IoT," said oneM2M Technical Plenary Chair Dr. Omar Elloumi of Nokia. *"Interoperability is essential for the IoT to reach its full potential and this can only truly be achieved through collaboration among leading industry stakeholders."*

> ***"oneM2M is working to lay the foundation of an IoT data economy through an interoperable approach to both domain-specific and cross-domain IoT"***

"Nobody can do it alone. The industry and standards organizations must all work together to join the pieces of the puzzle together and our industry day highlighted that this is achievable," Elloumi added.

The event also featured demonstrations of oneM2M applications in different industries, as well as technical information on the latest requirements. Presentations on the oneM2M AppID registry managed by iconectiv, the global oneM2M certification programme run by TTA, and ATIS' open source initiative, which uses the oneM2M standard, were also given.

oneM2M's next Industry Day will take place in India on Wednesday, 20 September 2017 and interested parties can request an invitation from the Technical Plenary Chair.

For more information about the event and oneM2M, please visit www.onem2m.org.

"IoT Evangelist of the Year" prize for oneM2M's Omar Elloumi

The tireless work of oneM2M's Technical Plenary Chair Dr. Omar Elloumi was paid tribute to, as he collected a prestigious "IoT Evangelist of the Year" industry award recognizing his contribution to the progression of the Internet of Things (IoT) on 15 June in London.

Held at IoT World Europe, in London, the TechXLR8 awards celebrate outstanding contributions in converging technology areas, covering industries such as 5G, virtual and augmented reality, the IoT, cloud, connected automotive and artificial intelligence.

IoT Evangelist of the Year Award with Ana Matronic

"As the only representative of a standards organization to be shortlisted for this award, I am thrilled to have been named the winner," said Dr. Elloumi. *"Without interoperability, the IoT will not reach its full potential and progress to mass market adoption and we see this award as recognition of that fact. It is also a tribute to all of oneM2M's members, who are currently working on our next set of specifications, Release 3, as we continue to unlock the promise of the IoT."*

> ***"Without interoperability, the IoT will not reach its full potential and progress to mass market adoption and we see this award as recognition of that fact."***

Dr. Elloumi, of Nokia, heads up the Technical Plenary of oneM2M, the global standards initiative for Machine-to-Machine (M2M) communication and the IoT. Over the past year he has played a leading role in the ground-breaking work of the organization, which includes the launch of its Release 2 specifications to incorporate interworking, end-to-end secure information exchange and semantic interoperability. Dr. Elloumi is regularly invited as a panellist or keynote speaker and is recognized for evangelizing IoT advancements to the industry at large.

The judges highlighted how this has resulted in true advancement of the IoT, with companies such as Hewlett Packard Enterprise, InterDigital, Huawei, Sensinov and NEC using oneM2M's standards in real-world deployments.

For more information about oneM2M, please visit www.onem2m.org

Security: the impact of, and on, standards

By Scott Cadzow, Cadzow Communications Consulting, Ltd.

ETSI has a long and illustrious history of developing effective standards, something that all ETSI members hold as true. Whilst many of the successes of ETSI lie in radio and networks, through GSM and its successors, DECT and TETRA, underpinning those successes is a commitment to providing security capabilities.

Effective provision of security in a standard is backed up by consideration of risk and here ETSI has over a number of years led the world with its TVRA method. It is now extending this foundation work with TC CYBER moving towards publication of standards that address "Secure by Default" and "Privacy by Design" alongside the structural elements of successful security, in refining the Critical Security Controls (CSC) originally published by the SANS Institute and now available with an ETSI perspective as ETSI TR 103 305 (a multipart standard).

Misapplication of the CSC by human error, malicious or accidental, will lead to system vulnerabilities. The security domain has always sought input from users and human factors experts in addressing such errors. This is particularly important if the application or deployment of security measures relies on human users.

The first of the CSC requires that organizations make an inventory of authorized and unauthorized devices. It looks relatively simple - identify the devices you want to authorize and those you don't. However this introduces the Rumsfeld[1], conundrum *"… there are known knowns … there are known unknowns … there are also unknown unknowns …"*, and we have to assume that it is not possible to identify everything. The second of the CSC to prepare an Inventory of authorized and unauthorized software also has the Rumsfeld conundrum at the root of its problem.

The more flexible a device, the more likely it is to be attacked by exploiting its flexibility. We can also assert that the less flexible a device, the less able it will be to react to a threat by allowing itself to be modified. The nature of the devices, the mix of devices, and the connectivity of devices, are all critical elements in identifying where a system may be attacked and where the most effective defenses have to be placed. This is the world where you now find new and emerging technologies such as virtualization, led by ETSI's ISG NFV, M2M and IoT technologies, dealt with in oneM2M group and ETSI smartM2M, or autonomic and semi-intelligent networks, to name a few. Most of these technologies fall into the unknown unknowns' category at the beginning of their development which will be explored a little more in this article.

The role of standards in security is crucial here as standards have a primary role in giving assurance of interoperability. Opening up the threat model and the threats you anticipate, moving everything you can into box 1[2], in a format that is readily exchangeable and understandable is key. The corollary of the above is that if we do not embrace a standards' view we cannot share knowledge effectively. That means we grow our box 2, 3, 4 visions of the world. The lack of knowledge on the issue leading to the inability to defend our systems, and their users, gets ever more difficult and ultimately will act against us.

Standards enable and assert interoperability on the understanding that:

Interoperability = Semantics ⋃ Syntax ⋃ Language ⋃ Mechanics

Quite simply if any of the elements is missing then interoperability cannot be guaranteed.

Confidentiality Integrity Availability paradigm

Application of the CIA paradigm works for Box 1 problems and will work reasonably well to mitigate problems from Boxes 2 and 3. One of the big problems in the real world is that many of the problems are either in Box 4 or at the limits of Boxes 2 and 3. As systems become more complex how they react to stimuli become less certain and more problems will be hidden in box 4.

In the security domain, understanding that we need interoperability is considered a "by default" criterion but simply achieving interoperability is a necessary but insufficient metric for making any claim for security. The technical domain of security is often described in terms of the CIA paradigm (Confidentiality Integrity Availability) wherein security capabilities are selected from the CIA paradigm to counter systems' risks from several forms of cyber attacks. The common model is to consider security in broad terms as determination of the triplet {threat, security-dimension, countermeasure} leading to a triple such as {interception, confidentiality, encryption} being formed. The threat in this example is interception which puts confidentiality of communication at risk, and to which the recommended countermeasure (protection measure) is encryption.

"One pressing concern for security is the constant change of attackers' ability to break systems"

The challenge of quantum computers

One pressing concern for security but perhaps less so in other domains is the constant change of attackers' ability to break systems. As said above, whilst achieving interoperability is a necessary metric, it is insufficient unless it is continuously reviewed. In ETSI the technical groups have a good track record of review and refinement of all published standards and security is included. However whilst much of this work is careful evolution there is one domain which, for security, is causing a revolution in our thinking. It is the revolution represented by Quantum Computing and the impact this will have on our cryptographically protected systems. ETSI CYBER and the ETSI ISG QSC groups have published guides on this particular threat which may indeed destroy large chunks of our cryptographic toolkit. However one simple formula has been published in EG 203 310 which gives an understanding of the time to update an organization's computing and security base against attacks.

- Y = the time taken to patch the current system with one that is "safe" against all known vulnerabilities
- Z = the time taken to develop an attack against a system

If "Y > Z" then the system is vulnerable to the attack represented by Z.

Continued on page 15 >

[1] "Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones." Attributed to Donald Rumsfeld on 12 February 2002.

[2] The box 1, box 2 terminology arises from classifying the Rumsfeld conundrum to a Johari Window analysis and is addressed in more details later in the paper.

Security: the impact of, and on, standards Continued (from page 14)

By Scott Cadzow, Cadzow Communications Consulting, Ltd.

For the special case of the threat from quantum computing to public key cryptography the equation above is extended:

- X = the number of years the public-key cryptography needs to remain unbroken.
- Y = the number of years it will take to replace the current system with one that is quantum-safe.
- Z = the number of years it will take to break the current tools, using quantum computers or other means.

If "X + Y > Z" any data protected by that public key cryptographic system is at risk and immediate action needs to be taken. Thus if Z is estimated as 15 years then both X and Y have to be significantly less than 15 years, and the sum of X and Y also has to be less than 15 years, to be safe. With the increasing pace of development of viable quantum computers the value of Z is shrinking and there is a genuine challenge to ETSI to address this in a period less than our best knowledge of Z. This has to apply to all of ETSI's technologies - IoT, M2M, ITS, eHealth, cellular radio, NFV .... Quite simply nothing is exempt.

So if we accept the very broad view that security functions are there to protect user content from eavesdropping (using encryption) and networks from fraud (authentication and key management services to prevent masquerade and manipulation attacks) then where is ETSI going with security standardization now and in the future?

The Rumsfeld conundrum

The use of the Johari Window method to identify issues is of interest here and is illustrated using the phrasing of Rumsfeld in Table 1.

Table 1. Security concerns in Johari window style with Rumsfeld phrasing.

	Known to self	Not known to self
Known to others	Known knowns BOX 1	Unknown knowns BOX 2
Not known to others	Known unknowns BOX 3	Unknown unknowns BOX 4

The target of security designers is to maximize the size of box 1 and to minimize the relative size of each of box 2 and box 3. In doing so, the possibility for box 4 to be of unrestrained size is hopefully minimized (it can never be of zero size).

We can consider the effect of each "box" on the nature of the security we can offer:

BOX 1: Knowledge of an attack is public and resources can be brought to bear to counter the threat by determining an effective countermeasure

BOX 2: The outside world is aware of a vulnerability in your system and will distrust any claim you make if you do not address this blind spot

BOX 3: The outside world is unaware of your knowledge and cannot make a reasonable assessment of the impact of any attack in this domain and the countermeasures applied to counter it

BOX 4: The stuff you can do nothing about as, as far as you know, nothing exists there.

The obvious challenge is therefore to bring tools such as the 20 critical security controls to bear to maximize box 1 while at the same time as using education and dissemination to minimize the size of boxes 2 and 3. Box 3 is characteristic of the old, mostly discredited, approach of security by secrecy, whereas Box 1 is characteristic of the open dissemination and collaborative approach of the world of open standards and open source development. Box 1 approaches do not guarantee never having a security problem. Generally speaking we expect problems to migrate from box 4 to boxes 2 and 3 before reaching box 1 and, hopefully, mitigation.

Main threats

In the security domain we can achieve our goals both on a technical and procedural stand point. This also has to be backed up by a series of non-system deterrents that may include the criminalization under law of the attack and a sufficient judiciary penalty (e.g. interment, financial penalty) with adequate law enforcement resources to capture and prosecute the perpetrator. This also requires proper identification of the perpetrator as traditionally security is considered as attacked by threat agents, entities that adversely act on the system. However in many cases there is a need to distinguish between the threat source and the threat actor, even if the end result in terms of technical countermeasures will be much the same, although some aspects of policy and access to non-system deterrents will differ. A threat source is a person or organization that desires to breach security and will ultimately benefit from a compromise in some way (e.g. nation state, criminal organization, activist) and who is in a position to recruit, influence or coerce a threat actor to mount an attack on their behalf. A Threat Actor is a person, or group of persons, who actually performs the attack (e.g. hackers, script kiddy, insider such as an employee, physical intruders). In using botnets of course the coerced actor is a machine and its recruiter may be a machine itself. This requires a great deal of work to eliminate the innocent threat actor and to determine the threat source.

Continued on page 16 >

Security: the impact of, and on, standards Continued (from page 15)

By Scott Cadzow, Cadzow Communications Consulting, Ltd.

The relative simplicity, the lack of connectivity and the relatively low reconfiguration capability of many IoT/M2M devices, offer an attractive class of devices for mounting attacks. Their large number makes defense somewhat more challenging than devices with strong authentication and control models built in.

Application of the CIA paradigm works for Box 1 problems and will work reasonably well to mitigate problems from Boxes 2 and 3. One of the big problems in the real world, is that many of the problems are either in Box 4 or at the limits of Boxes 2 and 3. Our easy to solve problems are almost always in box 1 but challenges are nearly everywhere.

The very broad view is thus that security functions are there to protect user content from eavesdropping (using encryption as the known counter to eavesdropping) and networks from fraud (authentication and key management services as the known counters to masquerade and manipulation attacks). What security standards cannot do is provide a guarantee of their security function out of the context for which that function was designed. Technical security measures give hard and fast assurance that, for example, the contents of an encrypted file cannot, ever, be seen by somebody without the key to decrypt it. In other words you don't lock your house and hang the key next to the door in open view, you must take precautions to prevent the key from getting into the wrong hands. The French mathematician Kerchoff has stated *"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge".*

In very crude terms the mathematics of security, cryptography, provide us with a complicated set of locks and we need to apply locks to a technical system with the same degree of care as the one we use when we choose where to lock up a building or a car. Quite simply we don't need to bother installing a lock on a door if we have an open window next to it - the attacker will ignore the locked door and enter the house through the open window. Similarly for a cyber system, if crypto locks are put in the wrong place the attacker will bypass them.

ETSI Security Week addresses cybersecurity standardization challenges

In order to help tackle the serious threats posed to network security, ETSI staged a comprehensive week-long event devoted to this increasingly crucial subject. Many respected cybersecurity experts from around the world participated in the 2017 ETSI Security Week, which took place from 12-16 June at ETSI's headquarters in Sophia Antipolis, southern France. This is the third year in succession that ETSI has staged the Security Week.

This year's event saw representatives from a broad range of sectors involved in the presentations and panel discussions. Among these were BNP Paribas, Bosch, Deutsche Telecom, Ericsson, Ernst & Young, Gemalto, Huawei, Intel, ISO, NEC, Nokia Bell Labs, NTT Docomo, and Thales. The agenda covered the numerous preventative measures that need to be taken and detail sophisticated mechanisms which must be put in place to protect valuable data from cybercrime and industrial espionage.

Much of the activity focused on addressing issues that are being raised by the latest technological advances - such as the expected massive increase in the number of connected devices and how security procedures will be impacted by the roll-out of 5G mobile technology. A particular focus was given to the new types of threats made possible by the virtualization of network functions with the adoption of NFV, and the means to mitigate them. Attention then turned to the pivotal role that standardization is going to have in supporting international legislative guidelines and interoperability. There was also an opportunity to share experiences one year after the eIDAS regulation has entered force.

> ***"The event underlined the proactive stance being taken by ETSI in the area of cybersecurity"***

"Building on the success of the previous two gatherings, in 2015 and 2016, the core objective of the ETSI Security Week was to provide a platform for detailed dialogue on how best to safeguard the telecom and data communication networks of the future from security breaches. The event underlined the proactive stance being taken by ETSI in this area and how our vision of a standards-based structural framework will help encourage collaboration and alleviate the financial impact that cyberattacks have on the digital economy," states Charles Brookson, chairman of ETSI TC CYBER. *"It offered an ideal opportunity for attendees to converse with leading authorities in cybersecurity, exchange ideas and gain real insight into the challenges that lie ahead – and their potential solutions."*

ETSI/IQC Quantum Safe workshop

13-15 September 2017, London, UK

This three-day workshop will feature a special executive track and in depth technical tracks. This event will bring together diverse players in the quantum-safe cybersecurity community to facilitate the knowledge exchange and collaboration required to transition cyber infrastructures and business practices to make them safe in an era with quantum computers.

http://www.etsi.org/news-events/events/1173-etsi-iqc-quantum-safe-workshop-2017

First ETSI LTE Mission-Critical Push to Talk interoperability tests achieve 85% success rate

TCCA to deliver vendor certification process for LTE mission-critical products and applications

The first ETSI Mission Critical Push to Talk (MCPTT) Plugtests™ event – interoperability test sessions for mission-critical LTE equipment – concluded on Friday, 23 June 2017, with 140 participants from 19 vendors. The event was held at the ETSI headquarters in Sophia Antipolis, France, in partnership with the TCCA, the representative body for the global critical communications community. The test sessions were observed by seven government and public safety network operator organizations from Belgium, Finland, France, Norway and the UK.

More than 1000 tests were conducted, with a success rate of 85%. The tests are based on 3GPP, ETSI and IETF standards. For this first session, a test specification has been developed for the 3GPP Release 13 MCPTT, comprising 47 test cases.

As commercial products are developed, the TCCA will implement the vendor certification process for mission-critical products and applications, including MCPTT. *"Our key goal is to have one global standard for MCPTT,"* said Phil Kidner, former CEO of the TCCA.

"Our key goal is to have one global standard for MCPTT"

The participating companies and tested equipment are as follows:

- MCPTT Application Servers from Airbus, Alea, Genaker, Harris Corporation, Hytera, Nemergent, TASSTA and ZTE
- MCPTT Clients from Airbus, Alea, Armour Communications, Etelm (included in TETRA Base Station), Frequentis (included in Control Room), Funkwerk, Genaker, Harris Corporation, Hytera, Nemergent, Spirent, TASSTA and ZTE
- User Equipment (UE) from Bittium and Funkwerk
- LTE network components Evolved Packet Core (EPC), Evolved Node B (eNB) and Multimedia Broadcast Multicast Service (eMBMS) from Athonet, Ericsson, Expway, Huawei and one2many
- IP Multimedia Subsystem (IMS) from Athonet

The final tests of the MCPTT Plugtests event included pre-arranged and chat mode Group Calls, which involved several MCPTT clients, a Control Room, a LTE cab radio and a TETRA radio.

"This first event demonstrates the commitment of the industry to ensuring that mission-critical LTE equipment adheres to open standards and will be thoroughly tested to ensure complete user confidence once commercial products are available," said Harald Ludwig, chair of the TCCA's Technical Forum.

Adrian Scrase, ETSI CTO, said during the event that *"the value of the Plugtests is not only for the vendors in testing their implementations, but also in finding issues in the 3GPP specifications, which will be fed back to the 3GPP working groups."*

Supported by the European Commission, these sessions are the first in the world to test the interoperability of MCPTT products and services, and are conducted to ensure that equipment from different vendors designed to support mission-critical users will work together. The full report on these Plugtests has been posted on the ETSI portal. The next MCPTT Plugtests sessions are planned for Q2 2018.

"The value of the Plugtests is also in finding issues in the 3GPP specifications, which will be fed back to the 3GPP working groups"

Push-to-Talk (PTT) is a standard feature of narrowband Professional Mobile Radio (PMR) technologies developed specifically for mission-critical communications. PTT enables near instantaneous group communications – a critical requirement in an emergency situation. To ensure that such capability is built in to LTE services, 3GPP has been catalyzed by the work of the TCCA to ensure that LTE supports mission-critical communications, with MCPTT now specified in 3GPP Release 13.

Although the PMR market shows no signs of slowing, mission-critical broadband LTE will offer complementary capabilities, and its market is expected to grow at a compound annual growth rate of 20 per cent, from $1.1 billion in 2015 to $2.6 billion in 2020, according to IHS Markit. Planned nationwide rollouts in the United States, South Korea, the UK, the Middle East and Asian countries are expected to trigger significant large-scale investments in mission-critical LTE.

Ultra Reliable Low Latency Wireless Networks Conference (URLLC)

14-15 November 2017, London, UK

ETSI is pleased to endorse the Ultra Reliable Low Latency Conference 2017. The event is a platform for network operators, verticals, solution providers and standards bodies to come together and explore the drivers, challenges and performance parameters required to deliver competitive, low latency, high reliability wireless connectivity. **ETSI's CTO, Adrian Scrase, will speak at the event.**

For more information, please visit:
http://urllc2017.executiveindustryevents.com/Event/home

ETSI awards three ETSI Fellowships

Award granted for outstanding contribution to ETSI's work

On 4 April, during the 69th General Assembly, ETSI awarded three ETSI Fellowship awards to Frede Ask, Nuno Encarnação and John Phillips. All three awards were granted in recognition of outstanding contribution to the work of ETSI.

Frede Ask was elected in 1988 as ETSI Deputy Director, and served in that capacity and Deputy Director General until his retirement in 1996. Frede was also ETSI's legal advisor, secretary to the ETSI IPR Steering Committee and was instrumental in shaping the IPR policy of the Institute at its beginnings. Thanks to his negotiation with the European Commission, he helped achieve recognition of ETSI as an official European Standards Organization, alongside CEN and CENELEC. Frede Ask is fondly remembered as a great personality and as one of the individuals who helped define what ETSI is. This award, granted posthumously, was received by Frede's son Henrik Ask on his behalf.

Nuno Encarnação has participated in ETSI since 1992. From 1997 to 2000 he served as chairman of the Analogue Terminals and Access committee, and then as chairman of the Access and Terminals committee until 2006. He led the development of a range of TBR specifications for regulatory requirements for fixed network access, and later the Harmonised Standards under the Radio & Telecommunications Terminal Equipment (R&TTE) Directive. These included in particular TBR 21 for analogue non-voice access requirements. From 1999 to 2006 he was vice-chair of the ETSI group coordinating the implementation of the range of Harmonised Standards required for the R&TTE Directive. As chairman of TC AT Nuno also oversaw the introduction of cable network standardization at ETSI, which has now resulted in the creation of a dedicated committee, TC Cable.

John Phillips has been active in ETSI since 1989 through different leadership, technical and strategic roles. As the Chairman of ETSI General Assembly from 2006 to 2010 he led ETSI through a number of changes, putting in place the financial reporting structure and contributed to the EC's Future Landscape of European Standardization. He also served as vice-chair of the General Assembly from 2002 to 2006 and as a member of the ETSI Board from 1999 to 2006.

The ETSI Fellowship programme rewards individuals who have made an outstanding personal contribution to ETSI, to building the work of ETSI, or raising its reputation in specific sectors of standardization. Any individual representative of an ETSI member may propose a candidate for an ETSI Fellowship. Fellowships are awarded each year by an Award Committee composed of the ETSI General Assembly chairman and vice-chairmen, the ETSI Board chairman and the ETSI Director General.

BROADBAND WORLD FORUM

Broadband World Forum
24 – 26 October 2017
3 DAYS
4,000 HANDSHAKES
ENDLESS OPPORTUNITIES
RUB SHOULDERS WITH ALL THE LEADING PLAYERS
AN AGENDA THAT PACKS A PUNCH
INSPIRATIONAL C-LEVEL KEYNOTES
THE FUTURE OF CONNECTIVITY IS HERE. WILL YOU BE?
FIND OUT MORE AT TMT.KNECT365.COM/BBWF
HUAWEI
angie
NOKIA
ZTE

24-26 October 2017, Berlin, Germany

Endorsed by ETSI, Broadband World Forum is renowned as one of the world's largest telecoms, media & technology events. From the core to 5G enablement, the conference addresses timely issues being faced by operators and telcos. ETSI's CTO, Adrian Scrase, will be one of the key speakers at the event.

For more details go to: https://tmt.knect365.com/bbwf

6th eCall TESTFEST

9-13 October 2017 Kranj, Slovenia

ERTICO in partnership with ETSI and with the support of ITS Europe is organizing the sixth eCall TESTFEST event, which will take place from 9 to 13 October 2017, in Kranj, Slovenia. This event will be hosted by SINTESIO in cooperation with Iskratel, Public Administration and Telekom Slovenije.

http://www.etsi.org/news-events/events/1205-6th-ecall-testfest

Future Evolution of Marine Communication

7-8 November 2017 at ETSI, Sophia Antipolis

This ETSI workshop will investigate how the e-navigation concept and the evolution of GMDSS affect marine radiocommunication and navigation standardization in the mid/long term, also taking into account future requirements in terms of capacity/rate for data transmission as well as security aspects which are essential for improving maritime safety.

http://www.etsi.org/news-events/events/1206-workshop-future-evolution-of-marine-communication

Follow us #ETSIMarineComs

ETSI Experiential Networked Intelligence group elects leaders during kick off meeting

> "The purpose of the group is to improve operators' experience regarding network deployment and operation, by using AI techniques"

The elections of the chair and vice chair of the new ETSI Industry Specification Group on Experiential Networked Intelligence (ISG ENI) took place during their kick off meeting on 10 April. The purpose of the group is to define a Context Aware System using Artificial intelligence (AI) based on the "observe-orient-decide-act" control model. This enables the system to adjust offered services based on changes in user needs, environmental conditions and business goals.

Dr. Raymond Forbes of Huawei Technologies UK was elected as chairman and Ms. Haining Wang, of China Telecom, was elected as vice-chair.

Dr. Raymond Forbes explained: *"The purpose of the group is to improve operators' experience regarding network deployment and operation, by using AI techniques"*.

Ms. Haining Wang emphasized that: *"By introducing technologies such as SDN, NFV or network slicing, the network becomes more flexible and powerful. Nevertheless, the complexity of the future network is not reduced, but transferred from hardware to software, from the network itself to management and operation, from equipment to people. Experiential Networked Intelligence is expected to help operators to solve these problems"*.

Ten companies and organizations participated in this first meeting and defined the schedule to collect essential use cases and requirements, and carry out analysis of the potential gaps in the next eight months.

The ETSI ENI Industry Specification Group has resolved to work with major standards developing organizations such as ETSI NFV, ETSI MEC, ETSI NGP, IETF, MEF, 3GPP and BBF. New members are invited to join the group and participate in future meetings and standardization work.

The full list of organizations supporting ISG ENI can be found at:

https://portal.etsi.org/TBSiteMap/ENI/ListOfENIMembers.aspx

New ETSI Brochures

ETSI Annual Report

The ETSI Annual Report of 2016, published in April 2017, provides an overview of the activities of the institute during the course of the year.

The Annual Report April 2017 can be downloaded from the ETSI website: http://www.etsi.org/about/annual-report

Hardcopies are available from the ETSI Secretariat upon request at info@etsi.org

ETSI Work Programme

ETSI Work Programme 2017-2018 provides an overview of the ongoing work in our technical bodies and ISGs, structured according to our clusters. It presents the full extent of our forthcoming standardization activities to readers who may not wish to navigate our online database. Since ETSI's work never stops and our work programme is never frozen, the electronic format of the brochure contains links to the online work programme on the portal, for the latest status of our work.

You may download the ETSI Work Programme 2017-2018 now at: http://www.etsi.org/images/files/WorkProgramme/etsi-work-programme-2017-2018.pdf

Hardcopies are available from the ETSI Secretariat upon request at info@etsi.org.

ETSI 2017 EVENTS CALENDAR - What's on?

13-15 September	4th ETSI/IQC Workshop on Quantum-Safe Cryptography	London, UK
14-15 September	IoT India Congress	Bengaluru, IN
19-20 September	RAN World	Barcelona, ES
20 September	Telecom Security India Summit	Mumbai, IN
25-27 September	MEC Congress	Berlin, DE
26-29 September	NFV and Carrier SDN	Denver, US
9-13 October	SDN & OpenFlow World Congress	The Hague, NL
9-13 October	6th eCall TESTFEST	Kranj, SL
11-13 October	UCAAT 2017 - ETSI User Conference on Advanced Automated Testing	Berlin, DE
17-18 October	SON – Self-Organising Networks World	London, UK
23-26 October	ETSI IoT Week	Sophia Antipolis, FR
24-26 October	Broadband World Forum	Berlin, DE
6-8 November	IEEE NFV-SDN - IEEE Conference on Network Function Virtualization and Software Defined Networks	Berlin, DE
6-10 November	Berlin 5G Week	Berlin, DE
7-8 November	ETSI Workshop on Future Evolution of Marine Communication	Sophia Antipolis, FR
9-10 November	ICT Proposers' Day 2017	Budapest, HU
14 November	URLLC 2017 - Ultra Reliable Low Latency Communications	London, UK
4-5 December	ETSI Seminar	Sophia Antipolis, FR
4-8 December	5th oneM2M Interop Event	Pangyo, KR

Please visit the events section of our website for further details

Register now for UCAAT!

5th UCAAT
User Conference on Advanced Automated Testing
Berlin, 11-13 October 2017
Hosted by: Fraunhofer FOKUS

Full Details including tutorials and conference programme available at https://ucaat.etsi.org/

Follow us with #UCAAT

Not yet subscribed to the ETSI Newsletter?

Subscribe free of charge at www.etsi.org/newsletter

Hardcopies of the newsletter are available on demand. We are happy to consider contributions from ETSI Members.

For further information: newsletter@etsi.org

About ETSI

ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, aeronautical, broadcast and internet technologies and is officially recognized by the European Union as a European Standards Organization. ETSI is an independent, not-for-profit association whose more than 800 member companies and organizations, drawn from 68 countries, determine its work programme and participate directly in its work. **For further information, please visit: www.etsi.org**

World Class Standards

Follow us on: ETSI etsi.standards @ETSI_STANDARDS ETSIOrgStandards ETSIstandards

ETSI, 650 Route des Lucioles,
06921 Sophia Antipolis Cedex, France.
Tel: +33 (0)4 92 94 42 00