IEEE Communication Magazine, Vol. 53, Issue 12, pp.64–70, December 2015

Cooperative Intelligent Transport Systems Standards in Europe

Andreas Festag[*][†]

[*]Vodafone Chair Mobile Communication Systems, Technische Universität Dresden, Germany
andreas.festag@tu-dresden.de

[†]NEC Laboratories Europe, Heidelberg, Germany
andreas.festag@neclab.eu

***Abstract*—Information exchange among vehicles, and between vehicles and the roadside infrastructure is commonly regarded as a base technology to sustainably reduce road accidents and improve traffic efficiency. After more than a decade of research and development efforts, a technological basis has been established that applies WiFi-based, wireless communication in the 5.9 GHz frequency band, ad hoc communication and dedicated message sets, as well as management and security procedures. In Europe, Release 1 of standards for cooperative systems has been completed, indicating deployment of a basic system starting in 2015. This article provides a comprehensive overview of standards and complementary industry specifications for cooperative systems in Europe, covering relevant aspects of access technologies, network and transport protocols, facilities, applications, security, and management.**

I. INTRODUCTION

Vehicles are getting safer, cleaner, and more intelligent. Various sensors and assistant systems enable vehicles to monitor their environment. By means of information exchange among vehicles, as well as between vehicles and the roadside infrastructure, vehicles transform from autonomous systems into cooperative systems. Inter-vehicle communication is a cornerstone of intelligent transportation Ssystems (ITS), commonly referred to as cooperative ITS (C-ITS) or car-2-X communication. The development of C-ITS is primarily driven by applications for active road safety and traffic efficiency, which help drivers to be aware of other vehicles, disseminate warnings about road hazards, and provide real-time information about traffic conditions for speed management and navigation. Typically, these C-ITS applications rely on always-on connectivity among the vehicles in the vicinity, including the roadside infrastructure, and frequent data exchange. Additionally, Internet access and location-based services, such as for point-of-interest notification, road access control, and parking management, improve the driving convenience. Among the various possible communication technologies for ITS, a dedicated variant of IEEE 802.11, an allocated frequency band at 5.9 GHz for road safety and traffic efficiency applications, ad hoc networking, and C-ITS specific message sets have emerged as the current state of the art.

In Europe, the first research programs for cooperative ITS date back to the 1980s; the European project PROMETHEUS (1987–1994) marked the beginning of a cooperative driving system using inter-vehicle communication in the 57 GHz frequency band. By 2000, a new wave of research and development activities in academia and industry was initiated worldwide, triggered by the availability of GPS, embedded systems, and WiFi. In Europe, more than 40 different projects on C-ITS have been initiated since 2000. Starting with initial feasibility studies, such as FleetNet and NoW, projects greatly contributed to the current technology state and standardization, for example, SAFESPOT, GeoNet, SEVECOM, CoVeL, and COMeSafety. Finally, field operation tests (DRIVE C2X, SIM-TD, SCORE@F, etc.) validated and assessed the potential positive impact of C-ITS on safety and traffic efficiency at various test sites across Europe. Further projects have been initiated to study cooperative automated driving, such as the AutoNet2030 project.

C-ITS standards are essential to achieve interoperability among communication devices from different manufacturers for vehicles and roadside infrastructure. In Europe, standards are being developed by the European standardization organizations (ESOs) European Telecommunications Standards Institute (ETSI) and omit Europen de Normalisation (CEN) in their respective technical committees (TCs) ETSI TC ITS and CEN TC 278, Road Transport and Telematics, the latter in close liaison with International Organization for Standardization (ISO) TC 204. The standardization scope covers all types of transport, including rail, water, and air transport (ETSI) as well as tolling systems and road infrastructure (CEN); nevertheless, the focus in the past was clearly on cooperative road vehicles. ESOs produce standards of different types, from which the European Norm (EN) are approved by the national standardization organizations (NSOs) of the EU member and associated states and made legally binding. In 2010 the European Commission issued a mandate to the ESOs [1] for the development of a minimum and consistent set of standards for C-ITS. The mandate implied a common basis for national standardization in Europe and therefore prevented conflicting national standards. It was completed in 2013 with the announcement of Release 1 of the standards [2].

In Europe, the standardization efforts are driven by the European Car-2-Car Communication Consortium (C2C-CC) [3],

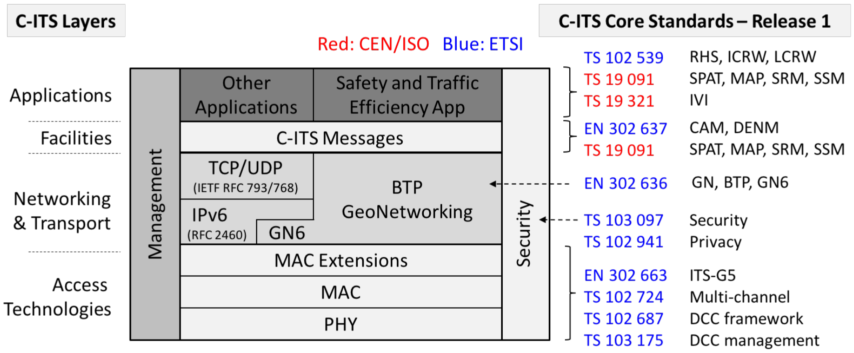

Fig. 1. Protocol stack and Release 1 core standards for C-ITS in Europe.

an industry consortium of automobile manufacturers, suppliers and research organizations, ERTICO, an European organization of stakeholders with public and private partners, as well as by ETSIs Center for Testing and Interoperability, ETSI CTI. In 2013, automobile manufacturers in C2C-CC signed an agreement for the introduction of the system in Europe starting in 2015. Deployment plans are being developed in the Amsterdam Group [4], a strategic alliance of stakeholders of C-ITS in Europe, CEDR, ASECAP, POLIS, and C2C-CC.

This article gives a comprehensive overview of Release 1 C-ITS standards in Europe and their profiling by industry consortia for initial deployment by 2015. The second section gives an overview about the standards set and briefly compares it with the IEEE 1609 standard family. The following sections provide details about standards for access layer, networking and transport, facilities, applications, and security and management. The final section concludes and provides an outlook on deployment and standardization beyond Release 1.

II. OVERVIEW OF C-ITS STANDARDS

The C-ITS standards follow a general architecture, specified in ETSI EN 302 665 and ISO 21217, with the ITS station as the core element, representing vehicle, personal (mobile personal devices), roadside (infrastructure), and central (back-end systems and traffic management centers) subsystems [5]. For C-ITS, the ISO OSI reference model was adapted to cover horizontal layers for access technologies, networking and transport, facilities and applications, and vertical entities for management and security.

Figure 1 illustrates the protocol stack for vehicle and roadside ITS stations, and lists the Release 1 core standards with their shorthand names for the European C-ITS Release 1. The access technologies layer primarily utilizes a specific set of options of the IEEE 802.11 standard, that is, ITS-G5 (where G5 stands for the 5 GHz frequency band). In the United States, this set is named Wireless Access in Vehicular Environment (WAVE), formerly referred to as the IEEE 802.11p amendment and now integrated into the IEEE 802.11-2012 standard release. The European variant, ITS-G5, is derived from WAVE and adapted to European requirements. Other access technologies, such as cellular networks, are not excluded, but are out of the scope of this article. The networking and transport layer has two columns: GeoNetworking and Basic Transport Protocol (BTP). The other column employs the Internet protocols, in particular IPv6 with UDP, TCP, or potentially other transport protocols such as SCTP, and IP mobility extensions (Mobile IPv6 and its extensions for network mobility, NEMO). The choice of the communication profile, whether GeoNetworking or IPv6, lies in the application. Typically, the GeoNetworking stack is used for ad hoc communication over ITS-G5 utilizing geo-addressing, and IPv6 for communication with an IP-based infrastructure over cellular networks. IPv6 packets can also be transmitted over GeoNetworking, for which the adaptation sublayer GN6 has been designed.

On top of the network and transport layer, standards for facilities layer protocols enable application functionality. The CAM protocol conveys critical vehicle state information in support of safety and traffic efficiency application, with which receiving vehicles can track other vehicles positions and movement. The DENM protocol disseminates event-driven safety information in a geographical region. Further message types are being standardized for vehicle-to-infrastructure communication. Applications are not fully standardized; instead, standards specify the minimum requirements for three groups of applications: road hazard signaling (RHS) comprises ten different use cases for initial deployment, including emergency vehicle approaching, hazardous location, and emergency electronic brake lights. The other two groups, intersection collision risk warning (ICRW) and longitudinal collision risk warning (LCRW), refer to potential vehicle collisions at intersections and rear-end/head-on collisions. Security- and privacy-related standards enable asymmetric cryptography and changing pseudonyms. Management standards mainly cover support for decentralized congestion control and communication profile management. A series of test standards provide specifications to verify the conformance of an implementation to the base standards and enable plug-tests for the testing of interoperability among implementations from different vendors. Further industry specifications for profiling and missing standards complete the set.

A comparison of the European C-ITS with the U.S.

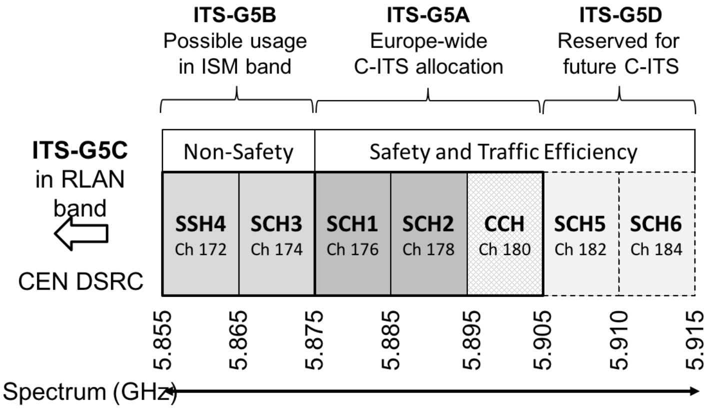

Fig. 2. European frequency allocation for road safety and traffic efficiency (ETSI EN 302 571).

dedicated short range communication (DSRC) standards in IEEE 1609 and SAE J2735 [6] reveals many similarities. Both approaches operate in the 5.9 GHz frequency band with several 10 MHz channels and rely on the OCB mode of IEEE 802.11, whereas the European variant ITS-G5 takes into account specific requirements for Europe and also incorporates service channels at the RLAN 5.4 – 5.7 GHz band for ITS applications. Also, the security and privacy approach is similar. Standards for higher protocol layers are different: the U.S. IEEE 1609 specifies a broadcast protocol for ad hoc routing optimized for short packet headers, called Wave Short Message Protocol (WSMP). The ETSI GeoNetworking standards specify an ad hoc routing protocol for single- and multi-hop communication with geographical addressing. Furthermore, the U.S. approach largely relies on the basic safety message (BSM) for collision avoidance applications. In contrast, C-ITS uses several safety message types including CAM for periodic and DENM for event-driven safety information. Both approaches are the subject of harmonization efforts at the governmental level between the United States and Europe, also including Japan, and at the industry level between C2C-CC and CAMP on the U.S. side. A major achievement is the alignment of the C-ITS Common Data Dictionary (CDD) in ETSI, which specifies the data elements for the CAM, DENM, and other messages, with the SAE 2735 message set. Overall, the similarities between the European C-ITS and U.S. DSRC standards prevail and enable multi-mode or dual stack implementations at reasonable costs, although major conceptual differences, particularly in information dissemination, still remain.

III. ACCESS LAYER STANDARDS

Three frequency bands in the 5 GHz band were allocated for ITS in Europe in 2008 (Fig. 2), aligned with similar efforts in North America and Japan: ITS-G5A has 30 MHz with 10 MHz channel spacing. The upper channel in ITS-G5A is named the control channel (CCH) and used as the primary safety channel. The others are additional service channels. ITS-G5B spans 20 MHz with two service channels of 10 MHz each and is dedicated to non-safety C-ITS applications. The 255 MHz wide band ITS-G5C is shared with the radio local area network (RLAN) band used by WiFi devices and can have 10 or 20 MHz channels. In ITS-G5C, devices must adhere to the dynamic frequency selection (DFS) method, well known for WiFi devices, which protects radar systems operating in the same band. As this method requires a DFS master, the usage of ITS-G5C is practically restricted to vehicle-to-infrastructure communication with a C-ITS roadside unit as a DFS master. However, up to now, the effectiveness of DFS with highly mobile devices in vehicles is not clear. Two more channels (ITS-G5D) are foreseen for future C-ITS systems.

In Europe, the usage of the allocated bands is regulated by harmonized standards, a specific form of European norms, which ensure the compliance of radio equipment with legislative directives. The harmonized standard for ITS-G5A EN 302 571 allows for up to 23 dBm/MHz transmission power and limits the emission to adjacent bands accordingly [7]. The spectrum mask is limited to -65 dBm in the 5.795 – 5.805 GHz band, in which CEN DSRC, the European tolling system, operates. The maximum transmit power is further restricted per service channel in order to protect the important CCH and restrict the out-of-band leakage to the CEN DSRC band: on the CCH and SCH1 a transmit power of 23 dBm/MHz is allowed, on the SCH2 and SCH3 only 13 dBm/MHz. Requests to spectrum regulators for extension of WiFi operation to the 5 GHz band for high data rate communication have triggered discussions about coexistence of C-ITS and WiFi in the same band. Although studies are still ongoing, effective protection of the ITS-G5 bands with low latency requirements is technically challenging.

The physical transmission in ITS-G5 is derived from IEEE 802.11a. It uses orthogonal frequency-division multiplexing (OFDM) with 52 subcarriers, of which 48 are for data and 4 for pilots. Compared to the typical 20 MHz channels in IEEE 802.11, with 10 MHz channels the sub-carrier spacing is halved, and the timing parameters are doubled, yielding an OFDM symbol duration of 8 ms including a cyclic prefix of

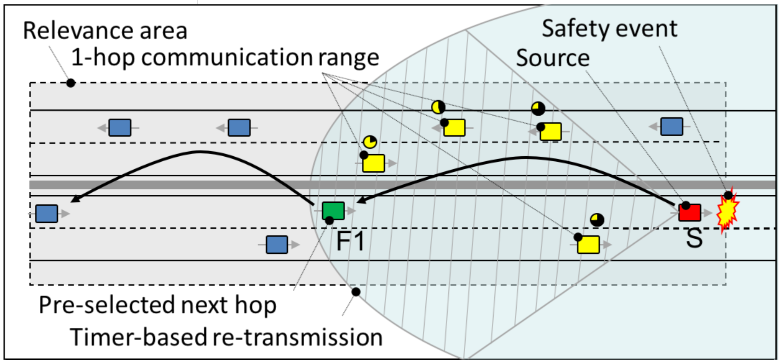

Fig. 3. Advanced forwarding algorithm for geo-broadcast (ETSI EN 302 636-4-1).

1.6 ms, which is aligned with the expected delay spread at a communication range of less than 1 km. The symbol duration in the 10 MHz channel configuration is also small enough to cope with inter-carrier interference caused by Doppler spread, that is, the coherence time is $T_C = f_d T_{OFDM} \approx 0.0134 \ll 1$ or a relative speed of 260 km/h between two vehicles. At a default data rate of 6 Mb/s the coherence time corresponds to roughly 400 bytes, which may result in variations of the channel estimation during the reception of a large frame in high-speed scenarios [8].

ITS-G5 applies a basic ad hoc mode, which is referred to outside the context of a BSS (OCB) in standards. The OCB mode simplifies operation compared to a wireless network known as the basic service set (BSS) in IEEE 802.11 terminology, disables management procedures, such as channel scanning, authentication, and association, and uses a wildcard BSS identifier. OCB-enabled ITS-G5 stations can transmit messages directly and immediately without time-consuming delays for the exchange of control frames.

For medium access, ITS-G5 introduces the same scheme as specified in IEEE 802.11, that is, carrier sense multiple access with collision avoidance (CSMA/CA), with one medium access control (MAC) entity per channel. The scheme is extended by quality of service (QoS) support from IEEE 802.11, known as enhanced distributed channel access (EDCA), which provides different priorities for channel access with specific parameters for contention window size and idle time (inter-frame spaces) per priority class. The ITS-G5 frames are assigned to EDCA queues based on the traffic class (TC) parameter chosen by the facilities layer with TC values for CAMs, high- and low-priority DENMs, and so on.

On top of the medium access entity with the EDCA queues, the MAC layer extensions for ITS-G5 provide two main functions: gatekeeper and multi-channel operation (MCO). The gatekeeper ensures that upper layer entities transmit packets within a maximum rate bound for a TC; it is essentially a set of on-off queues on top of the EDCA queues. MCO controls an ITS-G5 transceiver to tune to a specific service channel in a dual-transceiver ITS-G5 configuration, where the first transceiver is fixed to the CCH, and the other transceiver may dynamically switch among service channels. The standards for both functions, gatekeeper (ETSI TS 102 687) and MCO (ETSI TS 102 724), are currently under revision.

ITS-G5 uses the standard IEEE 802.2 protocol supplemented by the Subnetwork Access Protocol (SNAP). GeoNetworking uses LLC unacknowledged connection (Type 1) service with unnumbered information (UI) frames and Ethertype 0x8947.

IV. NETWORKING AND TRANSPORT LAYER STANDARDS

The networking and transport layer standards belong to the standard series EN 302 636 and cover requirements (part 1), scenarios (part 2), and the overall networking architecture (part 3). Part 4 specifies the networking protocol and is separated into media-independent (subpart 4-1) and media-dependent operations for ITS-G5 (subpart 4-2). Although split up in parts, both build a single protocol entity. The split allows for future media-specific extensions over wireless media other than ITS-G5. The transport layer standards for BTP and GN6 are specified in parts 5 and 6 of the series, respectively.

GeoNetworking is a routing protocol that provides packet delivery in an ad hoc network without a coordinating infrastructure. It utilizes geographical positions for addressing and forwarding. The addressing capabilities facilitate sending a packet to an individual ITS station with its geographical position or to a geographical target area described by geometric shapes (circle, rectangle, ellipse; see ETSI EN 302 931); the latter implies both broadcast and anycast to nodes inside the target area (area forwarding mode), as well as support for the transport of packets toward the area if the source is located outside (line forwarding mode). Altogether, GeoNetworking supports five packet handling modes: geo-unicast, geo-broadcast, geo-anycast, single-hop broadcast, and topologically-scoped broadcast, the latter two not having the geographical addressing. Geo-broadcast packets are used to distribute event-driven messages of type DENM, and periodically triggered CAMs are carried by single-hop broadcast packets.

GeoNetworking enables forwarding of packets on the fly without the need to establish and maintain routes. The GeoNetworking standard EN 302 636-4-1 specifies several forwarding algorithms with increasing protocol functionalities and efficiency. For geo-broadcast packets, three algorithms are specified: simple geo-broadcast applies a flooding scheme that restricts rebroadcasting by the geographical borders of the target area, and duplicate packet detection based on source ID and packet sequence numbers. With contention-based forwarding (CBF) a node broadcasts the packet to all neighbors, which buffer the packet and contend for packet forwarding: Each candidate forwarder starts a timer that is inversely proportional to its forwarding progress (i.e., the distance between the local and previous sender positions). The node with the shortest timer wins the contention and rebroadcasts the packet. When the other contending nodes overhear a forwarded packet, they stop the timer and remove the packet from their buffer. The advanced forwarding algorithm combines CBF with a sender-based selection of the next hop, where the neighbor with the most progress is chosen (also referred to as greedy forwarding, GF).

The advanced forwarding algorithm is illustrated in Fig. 3 in an example scenario. The source node S detects a safety event, creates a geo-broadcast packet, and selects F1 as the next hop using the GF algorithm. F1 then forwards the packet without buffering. The other nodes inside a defined sector of the sources direct communication range process and buffer the packet, and forward it if their position-dependent CBF timer expires. The advanced forwarding also allows for redundant retransmission by several different nodes up to a configurable threshold. The redundant transmission improves the reliability of geo-broadcast packet dissemination and controls the number of retransmissions, avoiding well-known broadcast storms. For geo-unicast, corresponding forwarding algorithms, that is, GF and CBF, are defined.

A GeoNetworking packet is composed of three headers; basic, common and extended. The basic and common headers carry fields that are needed by all packet types. The extended header is specific for geo-unicast, geo-broadcast, and so on, and covers, for example, fields for the definition of the geo-area. The separation of basic and common headers has security reasons: a digital signature and certificate is generated by the packet source over the common and extended headers (and payload), such that fields in the basic header can be modified by a forwarder (e.g., the hop-count value can be decreased by every forwarder without the need to regenerate the signature [9]).

On top of the GeoNetworking protocol, BTP (EN302 636-5-1) multiplexes/demultiplexes facility-layer messages and provides a connectionless, unreliable end-to-end packet transport similar to UDP. It adopts the concept of ports from the IP suite and assigns well-known ports for the relevant facility-layer message types. Alternatively to BTP, GN6 (EN 302 636-6-1) enables sub-IP multihop delivery of IPv6 packets without modifications of IPv6. It adapts the stateless address autoconfiguration known from IPv6 and extends the concept of an IPv6 link to geographical areas that are associated with an IPv6 point of attachment. GN6 introduces an adaptation sublayer, referred to GN6ASL that presents a flat network topology to IP [10, 11].

V. FACILITIES LAYER STANDARDS

The facilities layer standards specify requirements and functions supporting applications, communication, and information maintenance. The standards cover messaging protocols, position and time management, location referencing, sensor data fusion in a local dynamic map (LDM), and others. The most relevant standards are those for the C-ITS messaging, which are presented below.

CAM is a periodic message that provides status information to neighboring ITS stations. Its transmission is activated when a vehicle is in a safety-relevant context (basically, when the engine is running). A CAM is composed of an ITS PDU header and several containers (Fig. 4) that group the data fields by the role of the sender and frequency of their appearance in the message. The ITS PDU header carries protocol version, message type, and sender address; the basic container has station type and its position. In order to reduce the size of the CAM, the high-frequency container carries mainly highly dynamic data (e.g., vehicle heading, speed, and acceleration) and is sent in every CAM. The low-frequency container has data with less safety relevance (e.g., vehicle role) or may have a large size (e.g., path history) and is therefore not always added to the CAM, but sent. The special vehicle containers are optionally added if needed for the senders role, such as for public transport, dangerous goods, road works, or rescue. The container concept ensures a flexible message format that can be adapted to the needs of the sending and receiving vehicle, while minimizing the load on the wireless channel.

The CAM rate is determined by CAM generation rules and can vary between the lower and upper limit of the CAM period $T_{Min} = 100\,\text{ms}$ and $T_{Max} = 1\,\text{s}$ (corresponds to a CAM rate of 1 to 10 in 1 s), controlled by the vehicle dynamics, application, and congestion status of the wireless channel. As illustrated in Fig. 5, the conditions are sampled at small intervals (minimum 10 Hz). If the vehicle dynamics exceed the predefined thresholds for heading, movement, and acceleration, a CAM is generated. The minimum and maximum time period between two CAMs can then further be restricted by the needs of DCC and the applications to TDCC and TAPP, respectively: If the load on the wireless channel is high, the minimum time period is increased, whereas the application is able to decrease the maximum time period if required by the safety situation. A low-frequency container and special vehicle container are included if at least 500 ms has passed since the last CAM generation.

DENM is an application-controlled, safety event-triggered message. When a vehicle detects a safety situation, the DENM protocol assigns an action identifier that is unique for the detecting ITS station. Unlike the CAM broadcast over a single ITS-G5 hop, the DENM gets assigned a relevance area for dissemination and can be transported over several

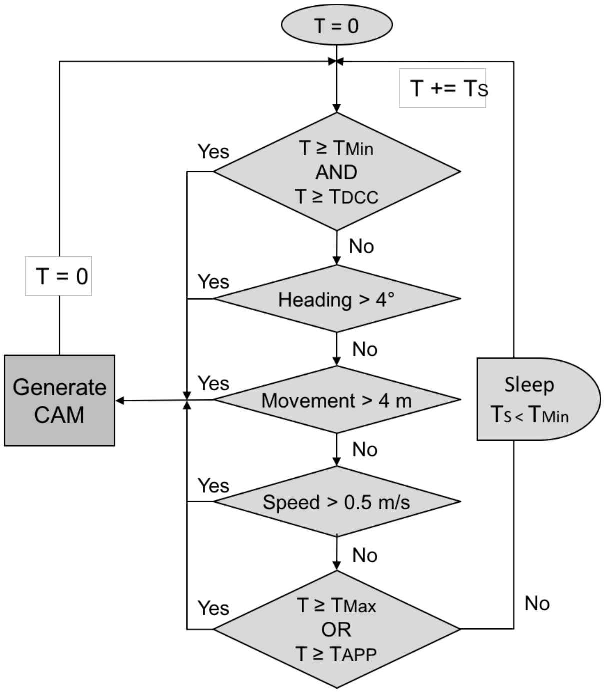

Fig. 4. CAM structure (ETSI EN 302 637-2).

wireless ITS-G5 hops, typically through the geo-broadcast mode of the GeoNetworking protocol. Similar to the CAM, the DENM is organized in containers with a prepended ITS PDU header (Fig. 6). The management container – with fields for action identifier, detection time, event position, and so on – is mandatory, all other containers are optionally added if needed by the application. The situation container has fields to describe the event by a predefined code for the causing event as well as related events (e.g., linked events or an event history). The location container carries fields for the event speed, heading, and traces. An a la carte container can be added to transmit application-specific contents, such as for lane position, impact reduction, and road works, among others.

The DENM protocol can handle an event life cycle: an event with a specific action ID can be triggered and then updated by the originator of the DENM; the event updates are distinguished by an increasing value of a data version field. An event can also be canceled by the originator or negated by a third ITS station.

The DENM protocol specification has several mechanisms for information dissemination to keep the safety information in the relevant area during the event lifetime. The originator can repeat a DENM, typically at a lower frequency than a CAM, to ensure that vehicles entering the relevant area later can receive the information. Optionally, another ITS station than the originator can overtake the repetition of the DENM message in case the originator fails to repeat the DENM (e.g., if it is broken or has left the relevant area).

In addition to CAM and DENM standards, further messages are being standardized in CEN TC 278/ISO TC 204 for static road topology data (MAP), dynamic traffic light data (signal phase and timing, SPAT), priority and preempted access of special vehicles (SRM, SSM), probe vehicle data (PVD, PDM), and in-vehicle information (IVI).

VI. APPLICATIONS, SECURITY, AND MANAGEMENT STANDARDS

For the initial deployment of C-ITS, a basic set of applications (BSA) has been identified (ETSI TR 101 638) and classified into four application groups: active road safety, cooperative traffic efficiency, cooperative local services, and global Internet services. Applications are not fully standardized; instead, the standards specify the minimum requirements for three groups of applications: RHS, ICRW, and LCRW. Road hazard signaling (RHS) comprises 10 different use cases that are relevant for initial deployment, including emergency vehicle approaching, hazardous location, and emergency electronic brake lights. The other two groups, intersection collision risk warning (ICRW) and longitudinal collision risk warning (LCRW), refer to potential vehicle collisions at intersections and rear-end/head-on collisions, respectively. In addition to the requirements from SDOs, the C2C-CC has defined triggering conditions for its day 1 applications that specify the behavior of use cases for the sender, including pre-conditions, process flow, message parameters, and information quality requirements for the specific use case.

C-ITS standards specify mechanisms for security and privacy protection [12]. Based on the security architecture in ETSI TS 102 940, ETSI TS 102 097 specifies private key infrastructure (PKI) enrollment and authorization management protocols, ETSI TS 102 941 confidentiality, and

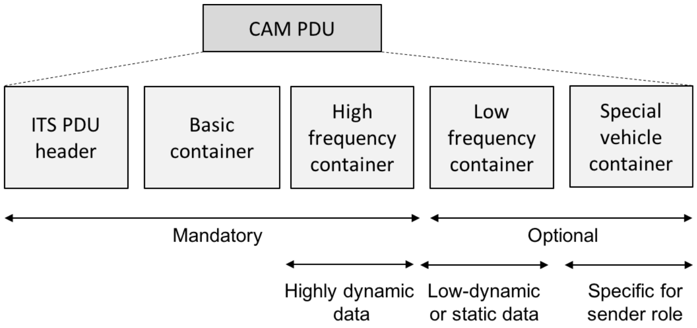

Fig. 5. CAM generation rules (ETSI EN 302 637-2).

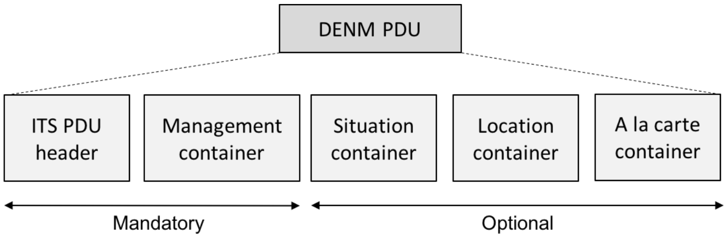

Fig. 6. DENM structure (ETSI EN 302 63-3).

ETSI TS 102 942 data integrity. The core security standard is ETSI TS 103 097 for the security header and certificate format for asymmetric cryptography with elliptic curves. The standards are complemented by C2C-CC specifications for PKI, TAL, and PP. The PKI specifications define the protocols among the certificate authorities and with the ITS stations, including root, long-term, and pseudonym certificate authorities. The trust assurance levels (TALs) define security levels of an in-vehicle C-ITS system, from a basic TAL protecting the software up to a very high TAL with a tamper-resistant hardware model, and shielding the involved in-vehicle sensors and control units. The protection profile (PP) then comprises all measures for security and privacy of a given TAL.

For DCC management, ETS ITS 102 687 defines a toolbox-like framework to control the channel load by transmit power, message rate, and other parameters. The standard introduces a state machine for DCC with relaxed, active, and restrictive states depending on the actual channel busy time. Every channel state enforces a predefined set of parameters for the upper or lower threshold of DCC parameters, but does not specify the exact DCC algorithm. ETSI TS 103 175 defines an ITS station-internal management entity that evaluates the congestion status for the ITS-G5 channels based on information from different layers. The DCC-related specifications are currently being revised. It is expected that message rate control is being applied as the main DCC mechanism together with additional mechanisms to ensure coexistence of C-ITS and the CEN DSRC road tolling system that operates in the adjacent 5.8 GHz frequency band. As an alternative to the state-based DCC approach, algorithms with linear control of parameters are considered, in particular LIMERIC [13] and PULSAR [14].

VII. CONCLUSIONS AND OUTLOOK

C-ITS has developed into a mature technology that can enable a wide range of innovative applications. To achieve interoperability, standards are essential. Release 1 of C-ITS standards was completed in early 2014, covering base standards for ITS-G5 radio, ad hoc networking and transport with GeoNetworking and BTP, facilities layer standards, in particular the messaging protocols CAM and DENM, security, privacy, and requirements for applications. The base standards are complemented by a set of test specifications. The maturity of the standards has been validated by conformance tests and plug-tests for interoperability with prototype implementations from different vendors. Field operational tests across Europe (DRIVE C2X, SIM-TD, and SCORE@F) have implemented and validated the standards in large-scale studies to assess the impact of C-ITS on safety and traffic efficiency.

Based on Release 1 of C-ITS standards, the C2C-CC has derived a profile that restricts the large list of standards and parameters to a practical set, and complementary missing specifications for security, management, and applications. It is expected that the deployment of the C-ITS profile will start in Europe in 2015. To ease the system introduction, corridor pilots are planned that will provide C-ITS services on major European highways. The forerunner is the trilateral C-ITS corridor interconnecting Vienna – Frankfurt – Rotterdam starting in 2015. Further corridor pilots are planned in France, Sweden, and other countries, as well as in selected cities. It is important to note that the developed C-ITS message sets are media-agnostic and expected to be reused for media other than ITS-G5, in particular 4G and future 5G cellular networks.

Future standardization will go in two main directions. First, existing Release 1 standards will be revised, for example, to improve DCC, specify performance requirements, enhance data dissemination concepts, and enable other communication media in addition to ITS-G5. Second, future C-ITS applications will introduce new, more demanding requirements beyond those of the safety warning and awareness applications in Release 1. Some Release 2 activities have already started, such as standards for electro-mobility support. It is foreseen that future standardization activities in ETSI TC ITS will focus on cooperative advanced cruise control (C-ACC), platooning, and protection of vulnerable road users such as pedestrians.

Acknowledgment

This work was also supported by the European Commission under AutoNet2030 – Co-operative Systems in Support of Networked Automated Driving by 2030, a collaborative project part of the Seventh Framework Programme for research, technological development and demonstration (Grant Agreement NO. 610542, URL http://www.autonet2030.eu). The author would like to thank all partners within AutoNet2030 for their cooperation.

References

1) Car-2-Car Communication Consortium, http://www.car-2-car.org.
2) Amsterdam Group, http://www.amsterdamgroup.eu.
3) CEN and ETSI, Final Joint CEN/ETSI-Progress Report to the European Commission on Mandate M/453; http://www.etsi.org/technologies-clusters/technologies/intelligent-transport, July 2013.
4) EC, New Connected Car Standards Put Europe into Top Gear, http://europa.eu/rapid/press-release_IP-14-141_en.htm, Feb. 2014.
5) T. Kosch et al., Communication Architecture for Cooperative Systems in Europe, IEEE Commun. Mag., vol. 47, no. 5, May 2009, pp. 116–25.
6) J. B. Kenney, Dedicated Short-Range Communications (DSRC) Standards in the United States, Proc. IEEE, vol. 99, no. 7, July 2011, pp. 1162–82.
7) E. Ström, On Medium Access and Physical Layer Standards for Cooperative Intelligent Transport Systems in Europe, Proc. IEEE, vol. 99, no. 7, July 2011, pp. 1183–88.
8) C. F. Mecklenbräuker et al., Vehicular Channel Characterization and Its Implications for Wireless System Design and Performance, Proc. IEEE, vol. 99, no. 7, July 2011, pp. 1189–1212.
9) A. Festag, P. Papadimitratos, and T. Tielert, Design and Performance of Secure Geocast for Vehicular Communication, IEEE Trans. Vehic. Tech., vol. 59, no. 5, Mar. 2010, pp. 2456–71.
10) M. Gramaglia et al., IPv6 Address Autoconfiguration in GeoNetworking-Enabled VANETs: Characterization and Evaluation of the ETSI Solution, EURASIP J. Wireless Commun. and Networking, vol. 2012:19, Jan. 2012, pp. 1–17.
11) V. Sandonis et al., Vehicle to Internet Communications Using the ETSI ITS GeoNetworking Protocol, Trans. Emerging Tel. Tech., Oct. 2014.
12) P. Papadimitratos et al., Secure Vehicular Communications: Design and Architecture, IEEE Commun. Mag., vol. 46, no. 11, Nov. 2008, pp. 100–09.
13) J. B. Kenney, G. Bansal, C. E. Rohrs, LIMERIC: A Linear Message Rate Control Algorithm for Vehicular DSRC Systems, Proc. ACM VANET, Las Vegas, NV, Sept. 2011, pp. 21–30.
14) T. Tielert et al., Design Methodology and Evaluation of Rate Adaptation based Congestion Control for Vehicle Safety Communications, Proc. IEEE VNC-Fall, Amsterdam, Netherlands, Nov. 2011, pp. 116–123.