Elektrische Signalverarbeitung Dr. Fischer GmbH

ESF News

Issue 2015/1 **_Intelligent Transport Systems (ITS)_** August 2015

Editorial

Crystal ball — Soothsaying

Let us first have a look into the history of Cooperative Intelligent Transport Systems (C-ITS).

Development of standards for ITS in general started already in 1992 at the “one true advocate on ITS”, i.e. ISO TC204. The scope of TC204 is “*Standardization of information, communication and control systems in the field of urban and rural surface transportation, including intermodal and multimodal aspects thereof, traveller information, traffic management, public transport, commercial transport, emergency services and commercial services in the intelligent transport systems (ITS) field. TC 204 is responsible for the overall system aspects and infrastructure aspects of intelligent transport systems (ITS), as well as the coordination of the overall ISO work programme in this field including the schedule for standards development, taking into account the work of existing international standardization bodies.*” 26 countries are participating, and 27 countries are observing. About 200 ISO standards were published under the direct responsibility of TC204.

As an initiative of TC204 WG16 “Communications”, the car industry was heavily invited to contribute to the CALM (Communications Access for Land Mobiles) standards development, at least by providing functional requirements. An important event was the WG16 CALM conference at Castle Reisensburg (University of Ulm / Germany) in 2004 arranged by ESF GmbH. However, car industry did not contribute to standardization.

A further important step was the foundation of ETSI TC ITS in December 2007 by members of TC204 WG16, and the immediate action from the car industry to take over control of work done at ETSI TC ITS.

In 2009, the CALM WG16 had a big meeting in Ödenwaldstetten / Germany, where representatives from German car industry showed up as guests and tried to advice ISO what they have to do. Obviously they failed, and ISO continued the excellent work on the set of CALM standards as originally planned. Further on initiatives to harmonize standards with IEEE 1609 WG and ETSI TC ITS started, also supported by the US DOT and EC DGINFSO. This resulted in a set of standards that now is almost complete and consistent, and enables interoperability of IEEE WAVE devices with ITS station units operating at 5,9 GHz.

In October 2012 “*12 vehicle manufactures organised in the CAR 2 CAR Communication Consortium signed a Memorandum of Understanding (MoU) to commonly bring cooperative Intelligent Transport Systems and Services (C-ITS) onto European roads. Herewith they approved to follow a joint guideline to make traffic and transport even safer, more sustainable and more comfortable in the near future.*”

This MoU immediately was answered by a similar commitment of European ITS suppliers.

The idea was to have C-ITS “on the road” in 2015.

A Release 1 set of standards (http://release1.its-standards.eu/) was announced by ETSI and CEN (both working under the C-ITS mandate M/453 of the EC) as the basis for day one deployment of C-ITS on European roads, and it became very visible that work done in ETSI TC ITS (under major control of car manufacturers) was not at all aligned with work done in ISO TC204 (jointly with CEN TC278). Further on this “Release 1” was just a list of work items (read our news issue 2013/1).

Nevertheless the process continued, and The Netherlands, Germany, and Austria agreed to implement the European C-ITS corridor, using ETSI standards, especially the GeoNetworking protocol aiming on multi-hop forwarding for geo-dissemination of information. This is a pity, as at 5,9 GHz the multi-hop forwarding highly risks to flood the channel, and we have a harmonized IEEE/ISO short message protocol solution that serves the needs of car-to-car and car-to-roadside communications as proven in USA and in the EU.

Trying to figure out details on this C-ITS corridor, a lot of very valuable detailed technical information is available from Austria (ECo-AT — ASFINAG), some information is available from Germany (BASt), and almost no information could be gathered about the approach in The Netherlands, except that the technologies from TomTom are relevant (probably there is information, but we could not find it).

In the meanwhile, USA speeded up to run the NHTSA project with IEEE WAVE-based car-to-car communications (that is now in the final pro-

(Continued on page 3)

How to manage radio channel congestion?

An easy approach to understand the problem of channel congestion is to arrange for a telephone conference. Repeat the trial with increasing number of participants. You can do a listen before talk to avoid collisions, and you will have the advantage to listen whilst you are talking (an 802.11 radio does not have this advantage!). Hopefully I do not need to say more — just try it!

Channel congestion can be managed (never totally avoided!) by the following means:

- keep the number of talkers in communication distance small
  - talk at low voice (power)
  - reduce the sensitivity of listening
- as much as possible avoid talking (use a priority scheme)
- keep your talks short (fair time-sharing of available channel capacity)
- use a supervisor to organize channel access (difficult or impossible with only mobile stations)
- use different radio channels for different "types" of information services
- ... there may be others and more complex ones.

Well, once a radio channel is filled up, no more additional communications can happen. A quite simple estimate on the theoretical capabilities with typical road traffic situations (Frankfurt Autobahn during rush-hour) and a given radio channel (e.g. at 5,9 GHz with 6 MBit/s) will provide a first feeling on what is feasible.

Beside the fact, as implemented in the US LIMERICS algorithm, to share the available bandwidth in a fair way amongst the WAVE devices being in a vicinity, and to arrange for this without the need to exchange channel congestion control information, the most important approach is at the appropriate design of the applications that exchange protocol data units, which includes an optimized design of the messages themselves with the aims to avoid communications, and to minimize message length. Message length significantly is increased by adding "security". Thus intensive research work is needed to identify suited security approaches to achieve a sufficient level of trust (see ISO 21217 and ISO 17419 on the subject of a trusted ITS station unit).

Further on with a given radio channel there are always limitations such that some networking modes are either impossible or very unfavourable. An example is ETSI GeoNetworking in multi-hop mode for geo-dissemination of information, or even the single-hop mode with a 40 (unused) octet header that would only be needed to prepare for multi-hopping.

We need to accept that the 802.11 technology used at 5,9 GHz was designed for operation with a master device that organizes channel access. This fits perfectly to roadside to car communications with the capability to use a multitude of orthogonal channels upon registration of vehicles via a default channel. For car-to-car communications, only the single-hop mode remains.

Some considerations on security?

Technical systems dealing with human properties or life need a sufficient level of security in order to efficiently protect the property or life. The technical means to achieve security however never should go beyond what typically is achieved and acceptable in ordinary life.

This is especially true when "security" is interpreted as "privacy". Applying strictly policies and regulations on privacy in a system design phase can always completely disable the introduction of the system to the market. "Privacy" thus can be used as a tool to avoid introduction of a new technology. That seems to be the case in C-ITS with the intention to promote existing cellular phone technologies and stop introduction of new ad-hoc communication technologies such as 802.11 at 5 GHz (ISO 21215), 60 GHz communications (ISO 21216), or Infrared communications (ISO 21214). We should note that for cellular networks the privacy regulations and policies never were strictly applied. A user of a mobile phone just accepts this by switching on his mobile phone; the same could be done for dedicated C-ITS communications, and there are even procedures possible in case of "mandatory applications" operated over such dedicated communication links.

The other issue with "security" is "trust". The question of trust is: "Can I believe in the content of a message that I received from another station, or can I trust in general messages from an other station?" At least two basic technical means are feasible, i.e. authenticate every message, or authenticate a station. The first approach is intensively considered in standardisation at IEEE 1609 WG and at ETSI TC ITS WG5, the second approach is not yet standardized although it is indicated in the ITS communications architecture ISO 21217 by means of the term "Bounded Secured Managed Domain" indicating a trustable ITS station, and further detailed in ISO 17419 on "Classification and Management of ITS applications".

It is recommended that the security experts start work on the second approach, and also investigate in alternative solutions compared to those standardized at IEEE and ETSI. Authorities might not accept the current approach.

Security developments also have to consider the capabilities of stations. ITS station units can be portable devices, e.g. a smart phones, or optimized microcontroller-based vehicular stations with limited computation power, and C-ITS application designs may require periodic transmissions of messages (e.g. CAM or BSM) at high repetition rate; applying crypto-algorithms to every received message might require more resources than available in such stations, and communications finally will fail. Workarounds open new doors for threats and thus are not acceptable.

Probably authorities like BSI in Germany will give a lesson to standardization on how to do it better.

Efficient communications in C-ITS

The essential basics of communications in ITS and C-ITS are presented in ISO 21217:2014. The architecture, for good reasons as confirmed e.g. by the German CONVERGE project, supports different communication protocols, a multiplicity of different access technologies, and a multiplicity of radios of a specific technology. This is one of the keys to efficient communications in C-ITS. C-ITS never can be based on just one (or two) communication protocol stacks. What is needed in general is the following

- ad-hoc short range communications
  - very short range "bumper to bumper" communications, e.g. for platooning, with one radio channel (ISO 21214, ISO 21216);
  - directed short range communications for roadside to vehicle communications, traditional service advertisement (ISO 24102-5) such as road tolling, with multiple orthogonal radio channels to serve several vehicles simultaneously (ISO 21215, ISO 21214);
  - almost omnidirectional short range communication, e.g. to support handheld devices and general car-to-car communications (ISO 21215);
- cellular networks for continuous communications and larger messages, e.g. file streaming, to connect to central stations (ISO 21213, ISO 17515);
- ...

with an efficient low-protocol-overhead short message protocol (e.g. ISO 29281-1 FNTP), and with the Internet protocol suite for ITS (ISO 21210 and others), and with a flexible protocol in the upper three OSI layers for message and data handling (ISO 17429, ISO 18750).

C-ITS applications should not need to know anything about communication protocol stacks except functional requirements for communications (ISO 17423), that are used by the station management together with location information, local regulations, and user policies to select an appropriate available protocol stack (ISO 24102-6), and to support various kinds of handover.

Not only in order to avoid self-interference, a local station-internal management is necessary (ISO 24102-1). Updates of protocols and applications, support of security means, and event handling requires a remote station management (ISO 24102-2) that connects the ITS station to its dedicated management center.

This all is available from ISO and CEN in a harmonized package developed by a small group of International experts.

Tutorials on the usage of these standards are offered by these experts. Please contact ESF GmbH to get more information and an offer for the kind of training you need.

Editorial — continuation

(Continuation from page 1)

cess of formal harmonization with ISO FAST). For well-understood reasons, USA does not support ETSI standards, but uses standards and specifications from IEEE and SAE. This highly optimized WAVE / FAST system seems to be well suited to achieve the goal of improving road safety and traffic efficiency. The NHTSA system specification is expected to be finished this year.

Intensive standardization work still is done at ETSI, IEEE, and SAE on two topics, i.e. algorithms to minimize the risk of 5,9 GHz radio channel congestion, and security algorithms to ensure a sufficient level of trust in received messages and corresponding transmitting stations. These two issues are a pre-requisite to introduce services that may impact on human life.

Implementing an ITS station in a conventional way that allows to update applications and protocols (software) remotely smoothens down the problem of insufficient trust and channel congestion, as initial "protocol bugs" easily can be fixed at reasonable cost. It could be noticed at ETSI TC ITS meetings that German car makers insist on an approach to implement an ITS station to a large extend in silicon. It was explicitly said that remote update of software is not acceptable. An update of an insufficient protocol or of protocol parameters (such as for mitigation techniques—coexistence with 5,8 GHz road tolling DSRC systems) thus would require a replacement of hardware.

Whilst the BSI (German federal authority on security in informatics) and other such authorities in Europe do not care about radio channel congestion, they will definitively care about security algorithms and the possibility to update protocols and protocol parameters.

That was a little of history of C-ITS. Now the "look into the crystal ball" is needed to figure out the future. Will C-ITS start in 2015, or will it start a bit delayed, or not at all? Will C-ITS come with non-standardized specifications — and what will be the services provided by C-ITS then? Will C-ITS be introduced by road authorities with "after-sales ITS station units" in vehicles, because car industry is not willing to support C-ITS? What about the frequency bands reserved in Europe for road safety — for which purpose will these be used? Well, I don't have a crystal ball, and I cannot do this magic job, but I can offer some considerations for discussion:

- Activities from road operators and vendors proof that they are preparing the introduction of C-ITS. As an example, ECo-AT already published version 3 of their well-developed system specification (note that Austria does not have a car industry as Germany has).
- ECo-AT does not mandate GeoNetworking, but has to mandate communication technology implemented in car maker's ITS station units. Car makers and the C2C-CC refer

(Continued on page 4)

Editorial — continuation

(Continuation from page 3)

to ETSI standards.

- Promotion of C-ITS is not visible in any news, whilst promotion of a similar technology (M2M) is even on the TV screens in airport lounges, and in ordinary news papers.
- The latest press release on the C2C-CC web was in 2012 on the MoU (see above).
- The multi-hop approach of ETSI is nicely called GeoNOTworking to indicate the related channel congestion problems that will become visible once a significant number of ITS stations is active in a vicinity (some of the readers may also remember the disaster at the demo given at the Vienne ITS world congress). ESF GmbH proposed a way out of this problem (draft ISO 16460).
- Although Vehicle Probe Data (data from the CAN bus) were identified by the traffic ministries of The Netherlands, Germany, and Austria as extremely relevant in the C-ITS Corridor to improve significantly traffic management, PVD are no more really visible in the specifications and discussions. Just evaluation of CAM and DENM (as a replacement for real PVD) is indicated to improve traffic management. Who objected and why?
- There are ongoing intensive discussions on privacy of data.
- Car makers are not willing to accept access to the in-vehicle CAN bus by an ITS station unit via a secured in-vehicle gateway, although such a gateway would definitively protect the CAN bus. This technical feature was intensively discussed in ISO TC204 WG17 and WG18, and in ISO TC22. There is no progress towards a standard. My question: “Who really owns these PVD?” I would say: “The car owner — not the car maker!”
- For obvious liability reasons, car makers aimed on using autonomous systems with on-board sensors in order to make driving in their cars reasonably save.
- An increasing number of C-ITS test sites is used in Europe.
- Books on VANETs (C-ITS) are published, e.g. http://www.springer.com/gp/book/9783319154961.
- http://www.faz.net/aktuell/technik-motor/auto-verkehr/car-to-x-kommunikation-abschied-von-der-zukunft-zurueck-zur-telematik-12514670.html (08/2013)

Content:

My personal vision is that C-ITS will come soon, largely using ISO and IEEE standards. ITS station units will be built according to ISO 21217:2014 principles, with after-sales units for German cars mounted on the dashboard. C-ITS stations will be used for many different services, not just for road safety.

Dr. Hans-Joachim Fischer
Managing Director

ESF GmbH

ESF GmbH is an independent engineering service provider and consultant for communications and radar with long-lasting experience in ITS and Road Tolling. ESF GmbH was founded in 1997 by Dr. Hans-Joachim Fischer. Dr. Fischer is still the owner and the only Managing Director. An introduction to ESF GmbH, its services, its projects, and a choice of customers is presented at http://fischer-tech.eu.

ESF GmbH is part of a virtual factory (set of small companies with complementary expertise) that can even offer quite complex activities (hardware, software, small series production, field trials, ...).

ESF GmbH opened a second office in Wannweil / Germany for Microsoft Windows SQL software development, and for Microsoft Back Office installation and support.

ESF GmbH is reactivating software development in C / C++ (and other languages as demanded by the customers) for microcontrollers and signal processors.

ESF GmbH will intensify activities on TTCN-3 based conformance testing, and development of conformance test suites in cooperation with relevant Standard Development Organizations.

Imprint

Company:	Elektrische Signalverarbeitung Dr. Fischer GmbH Fichtenweg 9, 89143 Blaubeuren, Deutschland, +49 7344 175 340
Managing Director:	Dr. Hans-Joachim Fischer
Registration:	Ulm, HRB 3433
Copyright:	Reprint permitted only without changes.