CEN/TC 278 PT1605

Basics on ITS communications –
CEN deliverables from PT1605 –
Support of secure access to sensor and control networks

Presentation to DG GROW

Hans-Joachim Fischer

Leader PT1605

PT1605 deliverables

PT1605 is funded by DG GROW under the C-ITS mandate, and actively supported by stakeholders.
Experts from PT1605 developed 7 CEN deliverables in support of ITS:

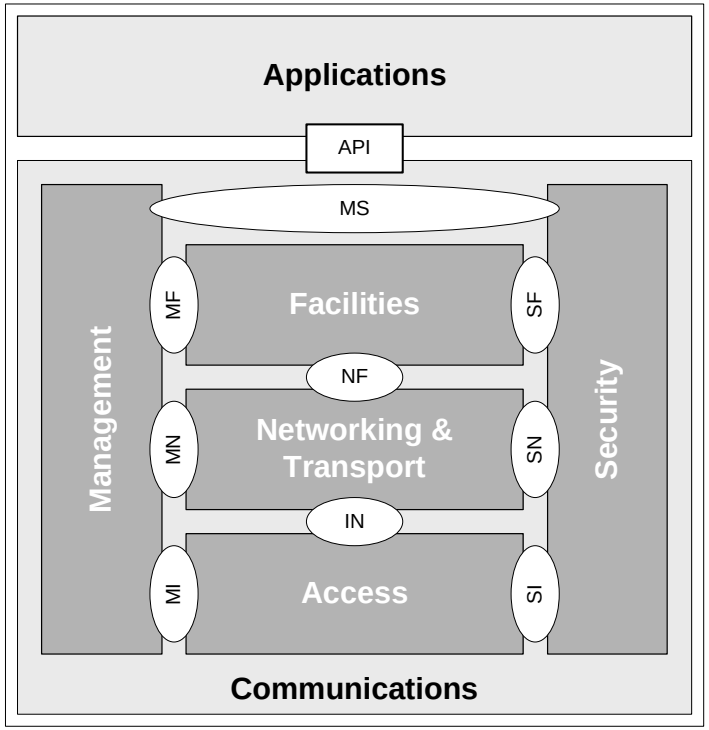
- ✓ *TS 21176: Position, velocity, time facility*
- ✓ *TS 21177: Session security (used in TS 21184)*
- ✓ *TS 21184: Global transport data management framework (including secure access to sensor and control networks)*
- ✓ *TS 17496: Communication profiles (for hybrid communications)*
- ✓ *TR 21186-x: Guidelines on the usage of C-ITS standards*
  1. *Standardization landscape and C-ITS releases*
  2. *Hybrid communications*
  3. *Cyber security (including improvements of TS 21177)*

All deliverables are either published or in the final ballot.

The presentation focuses on the basics of communications.

ITS station architecture

Many ITS standards were build around the abstract ITS station architecture (specified in ISO 21217), that describes functionality.



However, these ITS standards can be used also in different station contexts.

Networking modes

Communications between end-nodes (stations) can be performed as

- ✓ localized communications,
  i.e. communications between nearby stations without involving networking from a source station through nodes of a network to a final destination station – also referred to as "ad-hoc communications" (e.g. FSAP ISO 29281-1 / WSMP IEEE 1609.3), and
- ✓ networked communications,
  e.g. applying the Internet Protocol (ISO 21210).

These networking modes are not bound to a specific access technology. Each networking mode may support different end-node relations.

End-node relations

Each of the networking modes may support

- ✓ information dissemination,
  i.e. broadcast / groupcast communications (**one-to-many**) using *exactly only* one single technology per ITS service (ITS-G5 ISO 21215), and
- ✓ information exchange (sessions),
  i.e. unicast communications (**one-to-one**), probably based on a multiplicity of technologies per service (e.g. with session initiation performed during service announcement, or technology defined by choice of service provider).

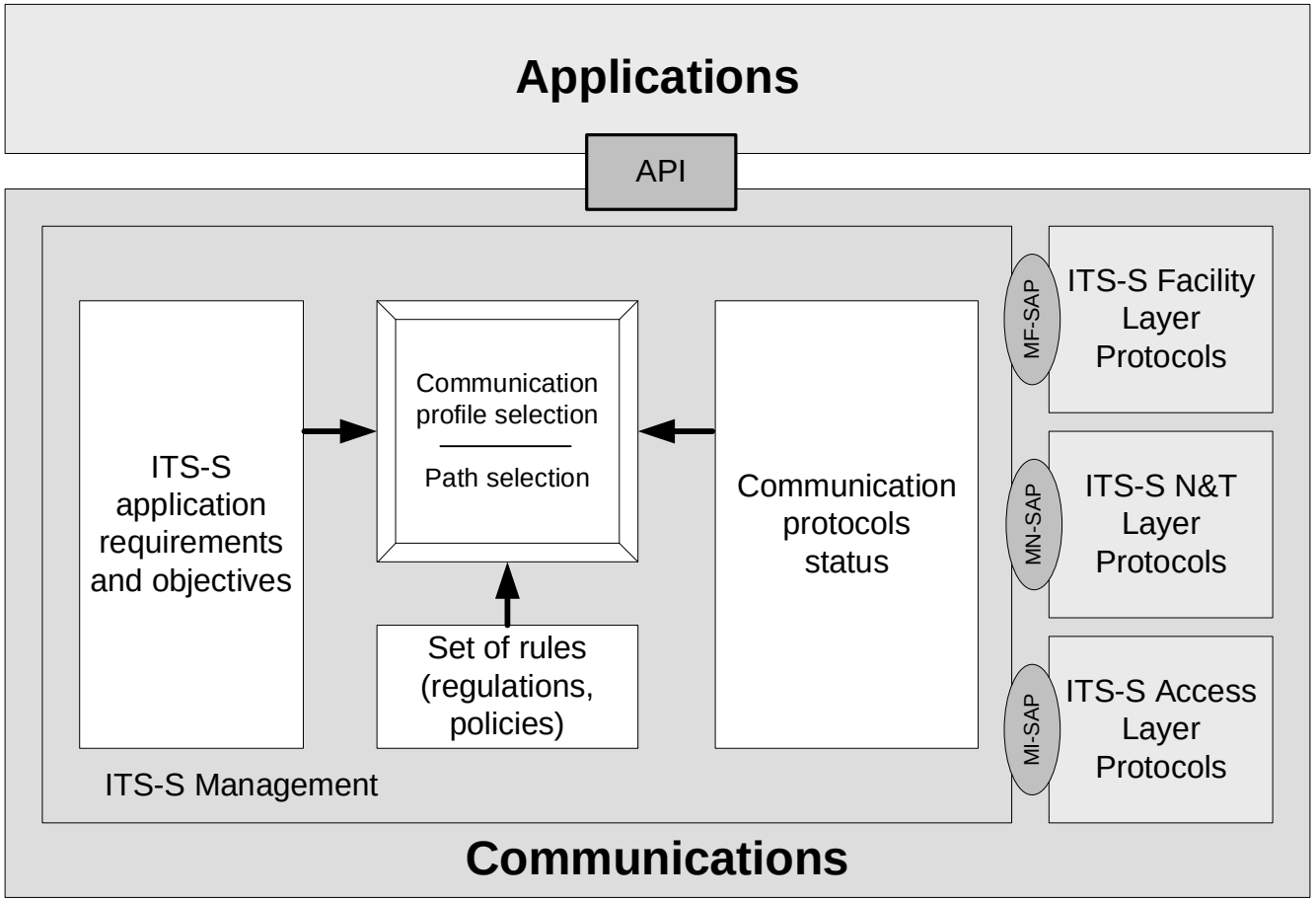
ITS application requirements

ITS applications are used to provide ITS services, and may have multiple and diverging communication needs per data flow.
Nevertheless, ITS applications should be agnostic to a specific communications technology (communication profile) to support *migration towards future technologies*.

EN 17423 (also funded under the C-ITS mandate) specifies

- ✓ how ITS application processes can present their communication needs to the station management, and
- ✓ the basis process of mapping communication requirements to the existing capabilities of a station (capabilities may depend on time and location of the station).

ITS application requirements



From ISO 21217 / EN 17423

Geo-fencing

Geo-fencing is a means (specified in CEN/TS 17380) to consider requirements (e.g. regulations and policies) that depend on the location (and time) of a station, e.g. regulations of radio matters, privacy, security, traffic rules.

The result of geo-fencing can be used e.g.

- ✓ to estimate the best choice of communication profile for a flow, i.e. the proper parameterization of the uppermost adequate communication protocol stack (see **CEN/TS 17496**);
- ✓ to inactivate an ITS station outside of an authorized area
- ✓ for the Management for Electronic Traffic Regulations (METR).

Cyber security

Information that is disseminated or exchanged must be secured. Whilst basically communications can be unsecured, end-to-end security between applications must be ensure:

- ✓ confidentiality (access control);
- ✓ data integrity (encryption of data);
- ✓ source authentication (signing of messages);
- ✓ non-repudiation (proof of integrity and origin of data).

Information dissemination applies "signing of messages" based on IEEE 1609.2 certificates (see ETSI standards). Information exchange is secured as specified in **TS 21177**; uses IEEE 1609.2 certificates for TLS.

Facilities

Facilities can be considered as tools (of the upper part of the OSI protocol stack) providing general functionalities to communications, to applications, and maybe to other entities:

- ✓ Message assembly:
  - the facilities service handler (specified in TS 17429), i.e. a functionality that can be ordered by applications to use facilities for e.g. adding a time stamp to a message.
- ✓ Sharing of data:
  - the local dynamic map (specified in EN 18750), i.e. a storage for location- and time-referenced data;
  - the content subscription handler (specified in TS 17429), i.e. a publish / subscribe mechanism useful to share data received from peer stations with local application processes.

Facilities

- ✓ Auxiliary functions:
  - the position - velocity - time service (specified in TS 21176 and EN 302 890-2), providing kinematic state information of an ego-station.
- ✓ Unique and secure access to data:
  - The global transport data management (GTDM) framework specified in **TS 21184**, providing e.g. necessary functionality for secure access to sensor and control network data with a precise and strict share of responsibilities and control for what is inside and outside the sensor and control network, offering a common data format (independent from the formats used in the sensor and control networks) to applications and facilities.

Service initiation

Beside the initiation of information dissemination services by

- simple pushing messages (broadcast / groupcast) – e.g. CAM and DENM, or
- polling an a-priori known URL,

an important distinction is between (push) service initiation

✓ by a central station for subscribed users,

typically based on cellular networks and the Internet Protocol, and

✓ using service announcement (specified in EN 22418)

Services are announced by means of the globally unique "ITS Application Identifier" (ITS-AID). Service announcement may be used to indicate a source of information for download, or to initiate a session between the service provider and the service user.

In both cases, part of the service initialisation phase is an optional change of communication profile for the service operation phase.

Hybrid communications

As explained before, due to the diverging communication requirements of already known and continuously emerging ITS applications, multiple communication technologies that may be fundamentally different can be supported in a specific station.

Supporting multiple access technologies and communication protocols is referred to as “hybrid communications”.

Hybrid communications can basically be defined as

composition of multiple access technologies and protocols with different characteristics combined to provide complementary or redundant communication channels.

Hybrid communications

Actually, this was a design principle of the ITS station architecture (specified in ISO 21217), which was developed in 2009 simultaneously with the activities of the EC-funded CVIS project. The urgent need for hybrid communications was also expressed by the German CONVERGE project in 2015, and in 2019 by the C-ITS deployment platform project C-Roads.

This can arise in multiple situations:

- ✓ Localized communications is combined with networked communications, e.g. the V2X communication stack from ETSI is combined with TCP/IP;
- ✓ Technology-agnostic applications are served with dynamic determination of the most appropriate communication profile;
- ✓ Safety critical communications, e.g. for platooning, requires physically independent redundant communication channels.

Hybrid communications

Benefits of hybrid communications are:

- ✓ redundant communications, e.g. simultaneous usage of physically different links to increase reliability;
- ✓ enabling mixed communications, e.g. to support multiple flows of the same ITS-S application process with different communication needs;
- ✓ serving a multiplicity of applications with diverging needs;
- ✓ smooth migration from one technology to an upcoming new one ensuring backward compatibility;
- ✓ support of different architectures for service provisioning.

Station management

Reliable and sustainable service provisioning requires station management:

- ✓ station-internal management (specified in ISO 24102-1) for e.g.
  - hybrid communication management including
    - selection and management of communication profiles per flow;
    - radio interference mitigation (e.g. DSRC for road tolling);

- ✓ remote station management (specified in ISO 24102-2) for e.g.
  - lifecycle management
  - certificate management.

PT1605 webinars

PT1605

✓ is offering a series of webinars on C-ITS technologies, and

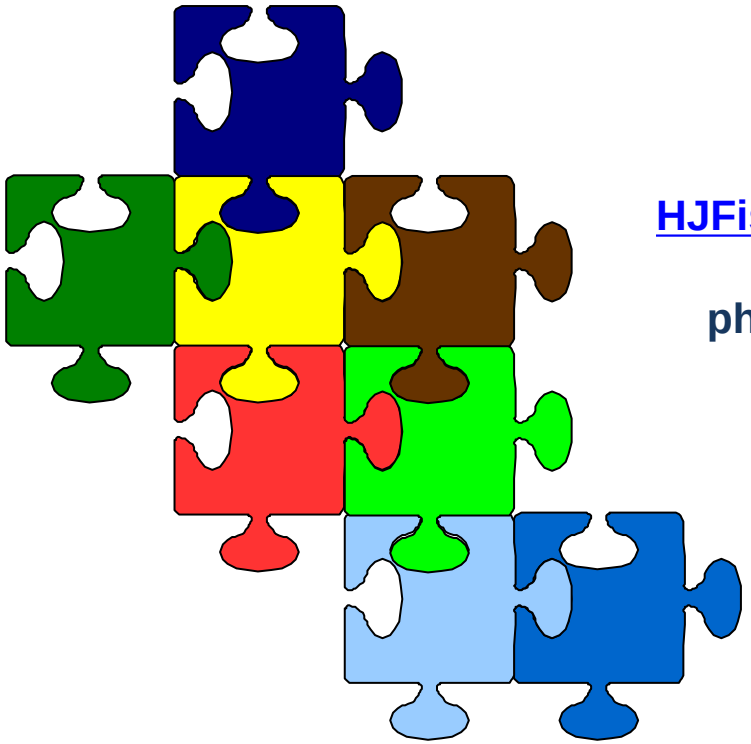
✓ contributes to webinars:

1. General presentation of PT1605 deliverables (April 2020)
2. C-ITS deployment in Israel (June 2020)
3. C-ITS deployment in Australia (under preparation)
4. Hybrid communications (scheduled for October 2020)
5. Cyber security – TS 21177 (under preparation)
6. GTDM framework – TS 21184 (under preparation)

Interested parties can contact PT1605 at webinar@its-standards.eu to get updates on these webinars.

PT1605

CooperativeSecureITS@its-standards.info
http://its-standards.eu/PTs/PT1605/



ESF GmbH
Hans-Joachim Fischer
Fichtenweg 9
D-89143 Blaubeuren
Germany
HJFischer@fischer-tech.eu
https://fischer-tech.eu
phone: +49 7344 175 340
fax: +49 7344 919 123