Practicable, workable, acceptable solutions for cybersecurity for connected vehicles through the use of CEN/ISO Standards

Bob Williams

Coordinator CEN TC278 WG17 / ISO TC204 WG19 Mobility Integretion

Convenor CEN TC278 WG15 eSafety

- The following slides summarise work in recent years by CEN and ISO concerned with the exchange of data between ITS-stations

  (V><V, V><I, I><I) in a flexible cybersecure paradigm
- This paradigm is independent of the wireless carrier medium

- The objective of this presentation is to summarise these documents to WP29 with the view that they may be useful tools for WP29 in its work
- Documents ISO 21217, ISO 21177, ISO 21184*, ISO 21185 have been made available by CEN to WP29.

*Note: ISO 21184 is still working its way through the approval process

ISO 21177, ISO 21184, ISO 21185

- The development of ISO 21177, ISO 21184, ISO 21185 were funded by EC via CEN PT 1605.
- and are consistent with European Commission's Joint Research Council "Certificate Policy For Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS") May 2018.
- ISO.EN 21184/ISO.EN 21185/ ISO.EN 21177 provide a secure framework for the definition and management of data that recognises and accommodates differences between OEM proprietary systems.
- Works within the communications reference architecture (ISO 21217) of nodes called "ITS station units" designed for deployment in intelligent transport systems (ITS) communication networks.
- Respects OEMs internal needs for private security of their EXVE's, provides secure bridging mechanism and cybersecure data access.
- Is independent of any one carrier medium and supports hybrid communications

CEN/TS 21177: Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices

- This document contains specifications for a set of ITS station security services required to ensure the authenticity of the source and integrity of information exchanged between trusted entities:
- devices operated as bounded secured managed entities, i.e. "ITS Station Communication Units" (ITS-SCU) and "ITS station units" (ITS-SU) specified in ISO 21217
- between ITS-SUs (composed of one or several ITS-SCUs) and external trusted entities such as sensor and control networks
- These services include authentication and secure session establishment which are required to exchange information in a trusted and secure manner.
- These services are essential for many ITS applications and services including time-critical safety applications, automated driving, remote management of ITS stations (ISO 24102-2), and roadside / infrastructure related services.
- This document is complemented by guidelines (contained in CEN/TR 21186-3) on how security for C-ITS can work in general for all communication types (broadcast information dissemination and unicast sessions), considering especially what is needed in the infrastructure in addition to the technical features implemented in ITS station units.

CEN/TS 21184: *Cooperative intelligent transport systems* — Global transport *data management (GTDM) framework*

- This document specifies a "Global Transport Data Management" (GTDM) framework composed of
- a global transport basic data model
- a global transport function monitor data model
- a global transport access control data model
- to support data exchange between ITS-S application processes and correct interpretation of these data.
- This document defines standardized data classes in a "Global Transport Data Format" (GTDF), and means for managing them.
- Data exchange between ITS stations is specified based on messages composed of a global unique identifier and the associated data part. The format of the data part is specified by a globally unique identifier pointing to a configuration including instructions for correct interpretation of the data part.
- Application and role-based access control to GTDF resources are specified in conformance with IEEE 1609.2 certificates.
- The set of ITS-S facility layer services is described as an ITS-S capability conformant with ISO 24102-6, which is an optional feature.

CEN/TS 21185:
Cooperative intelligent transport systems — Communication profiles

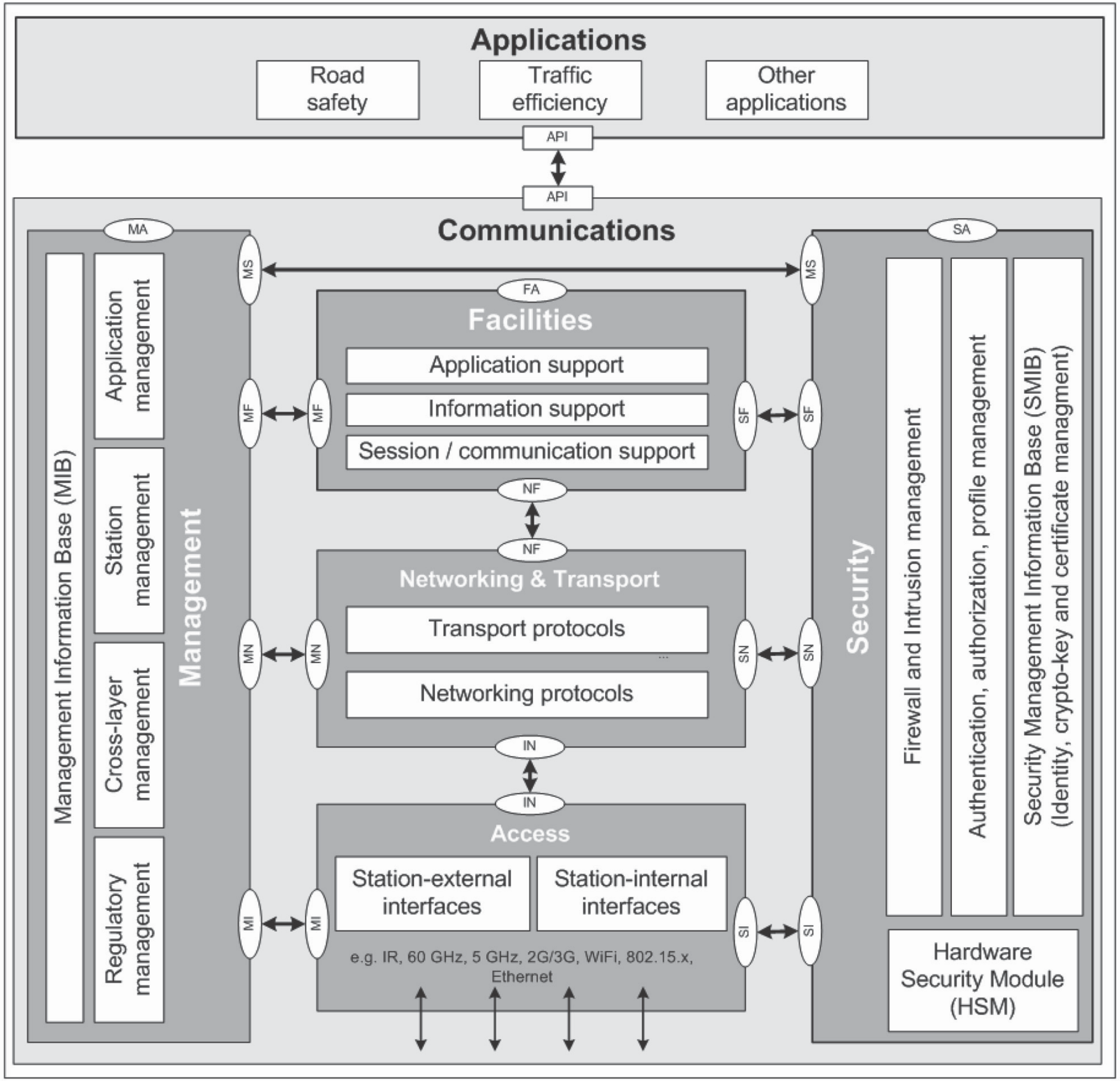
- This document specifies a methodology to define ITS-S communication profiles (ITS-SCPs) based on standardized communication protocols to interconnect trusted devices. These profiles enable information exchange between such trusted devices, including secure low-latency information exchange, in different configurations. This document also normatively specifies some ITS-SCPs based on the methodology, yet without the intent of covering all possible cases, in order to exemplify the methodology.
- Configurations of trusted devices for which this document defines ITS-SCP's include the following units according to ISO 21217:
- ITS station communication units (ITS-SCU) of the same ITS station unit (ITS-SU), i.e. station-internal communications specified e.g. in ISO 24102-4
- an ITS-SU and an external entity such as a sensor and control network, or a service in the Internet
- ITS-SUs
- The specifications given in this document can be applied to secured and to unsecured communications, both in unicast and groupcast communications mode

ISO 21217:2014 Intelligent transport systems — Communications access for land mobiles — Architecture

- This International Standard describes the communications reference architecture of nodes called “ITS station units” designed for deployment in intelligent transport systems (ITS) communication networks. The ITS station reference architecture is described in an abstract way. While this International Standard describes a number of ITS station elements, whether or not a particular element is implemented in an ITS station unit depends on the specific communication requirements of the implementation.

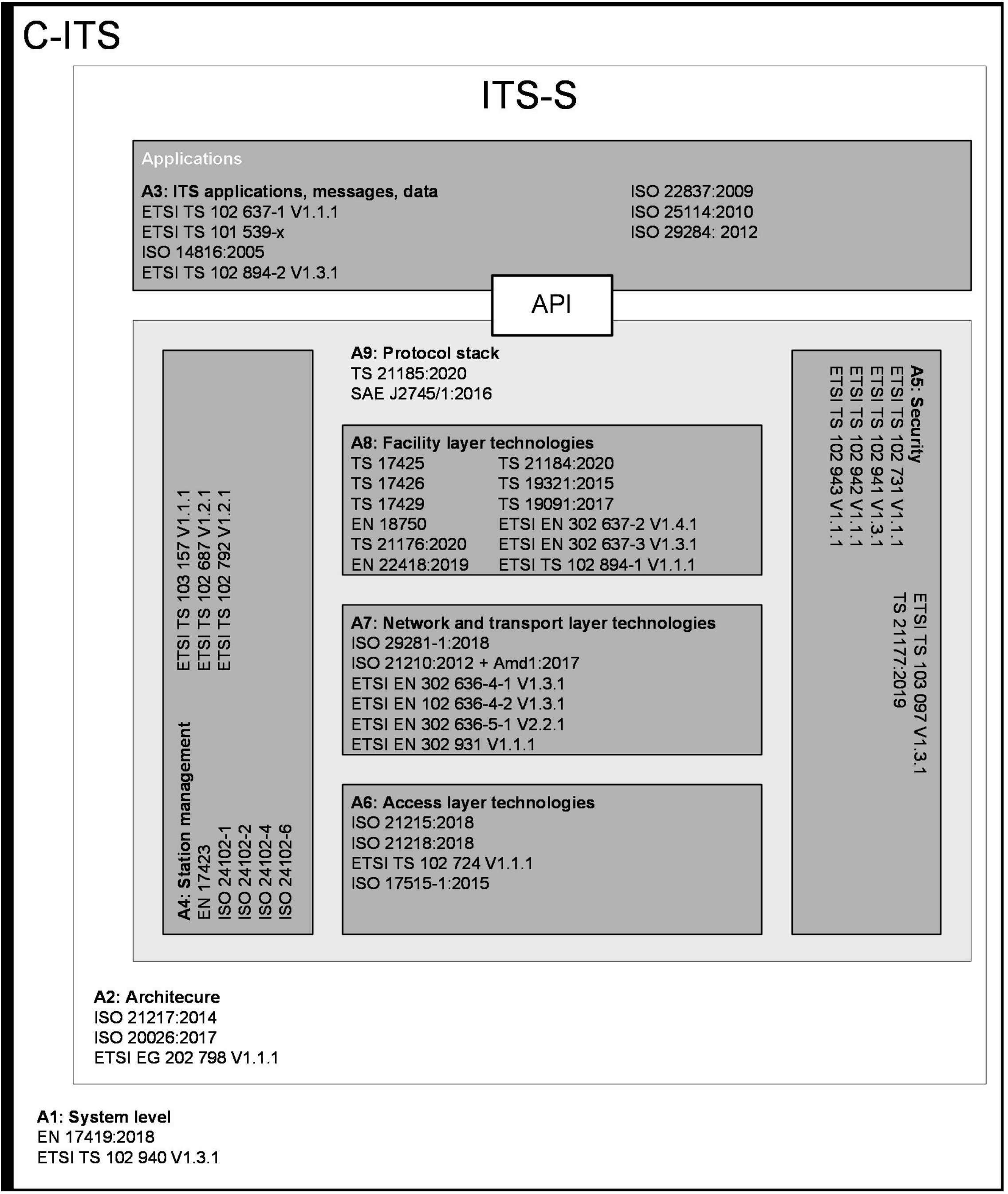
- This International Standard also describes the various communication modes for peer-to-peer communications over various networks between ITS communication nodes. These nodes may be ITS station units as described in this International Standard or any other reachable nodes.

- This International standard specifies the minimum set of normative requirements for a physical instantiation of the ITS station based on the principles of a “bounded secured managed domain”.


Applications
Road safety
Traffic efficiency
Other applications
API
API
Communications
MA
MS
MS
SA
FA
Facilities
Application support
Information support
Session / communication support
MF
MF
SF
SF
NF
NF
Networking & Transport
Transport protocols
...
Networking protocols
MN
MN
SN
SN
IN
IN
Access
Station-external interfaces
Station-internal interfaces
MI
MI
SI
SI
e.g. IR, 60 GHz, 5 GHz, 2G/3G, WiFi, 802.15.x, Ethernet
Management
Management Information Base (MIB)
Application management
Station management
Cross-layer management
Regulatory management
Security
Firewall and Intrusion management
Authentication, authorization, profile management
Security Management Information Base (SMIB) (Identity, crypto-key and certificate managment)
Hardware Security Module (HSM)

Overview of relevant standards for C-ITS

T



C-ITS

ITS-S

Applications

A3: ITS applications, messages, data
ETSI TS 102 637-1 V1.1.1
ETSI TS 101 539-x
ISO 14816:2005
ETSI TS 102 894-2 V1.3.1
ISO 22837:2009
ISO 25114:2010
ISO 29284: 2012

API

A9: Protocol stack
TS 21185:2020
SAE J2745/1:2016

A8: Facility layer technologies

TS 17425	TS 21184:2020
TS 17426	TS 19321:2015
TS 17429	TS 19091:2017
EN 18750	ETSI EN 302 637-2 V1.4.1
TS 21176:2020	ETSI EN 302 637-3 V1.3.1
EN 22418:2019	ETSI TS 102 894-1 V1.1.1

A7: Network and transport layer technologies
ISO 29281-1:2018
ISO 21210:2012 + Amd1:2017
ETSI EN 302 636-4-1 V1.3.1
ETSI EN 102 636-4-2 V1.3.1
ETSI EN 302 636-5-1 V2.2.1
ETSI EN 302 931 V1.1.1

A6: Access layer technologies
ISO 21215:2018
ISO 21218:2018
ETSI TS 102 724 V1.1.1
ISO 17515-1:2015

A4: Station management
EN 17423
ISO 24102-1
ISO 24102-2
ISO 24102-4
ISO 24102-6
ETSI TS 103 157 V1.1.1
ETSI TS 102 687 V1.2.1
ETSI TS 102 792 V1.2.1

A5: Security
ETSI TS 102 731 V1.1.1
ETSI TS 102 941 V1.3.1
ETSI TS 102 942 V1.1.1
ETSI TS 102 943 V1.1.1
ETSI TS 103 097 V1.3.1
TS 21177:2019

A2: Architecure
ISO 21217:2014
ISO 20026:2017
ETSI EG 202 798 V1.1.1

A1: System level
EN 17419:2018
ETSI TS 102 940 V1.3.1

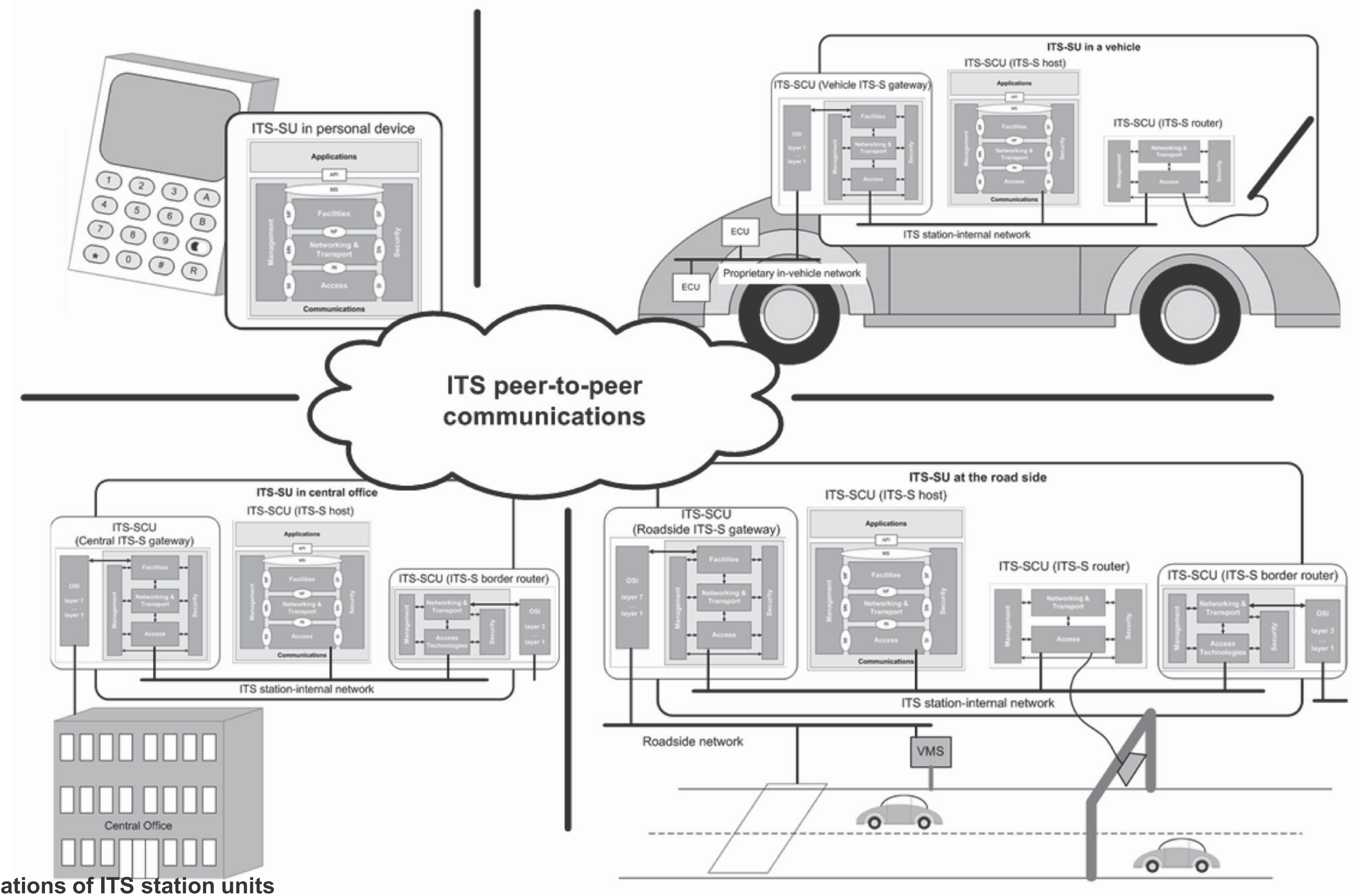


Figure 25 — Typical implementations of ITS station units

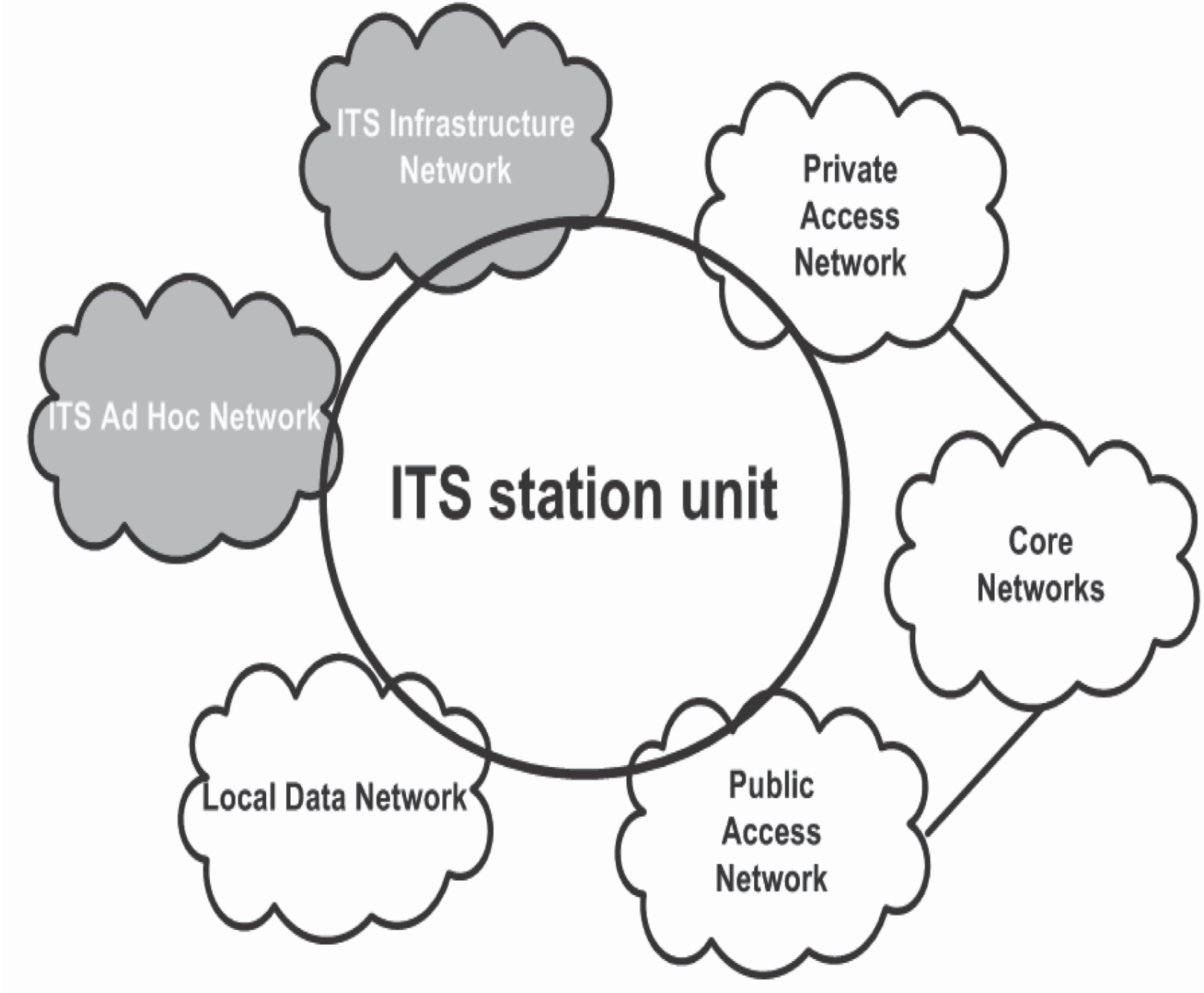
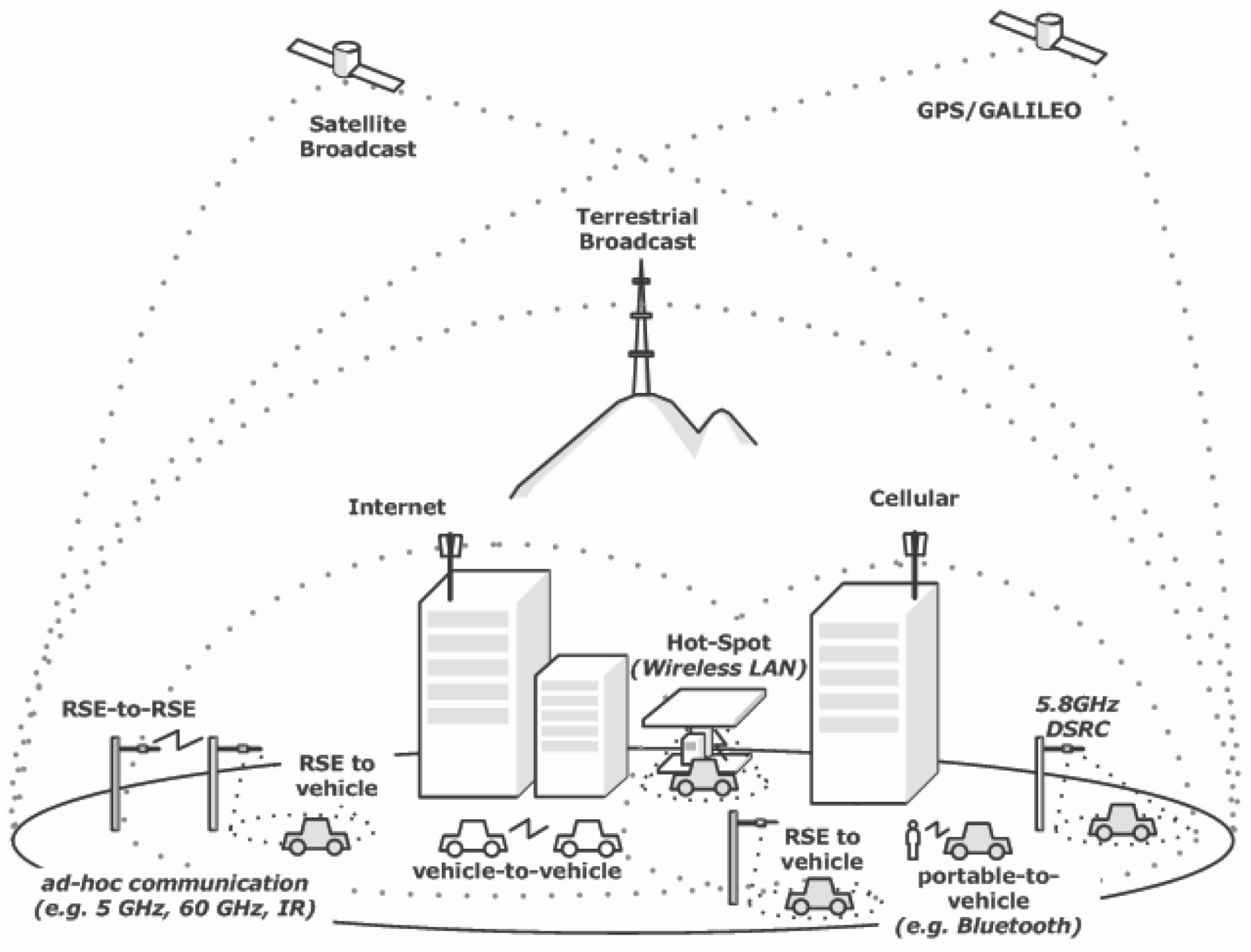


Figure 2 — Networking view of ITS communications



- Examples of ITS communications

Conclusion

- ISO.EN 21184/ISO.EN 21185/ ISO.EN 21177 provide a secure framework for the definition and management of data that recognises and accommodates differences between OEM proprietary systems.
- supported and funded by EC via CEN PT 1605 -consistent with EC Joint Research Council "Certificate Policy For Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS") May 2018
- Respects OEMs internal needs for private security of their EXVE's, provides secure bridging mechanism and cybersecure data access

Questions

- Bob Williams & Scott Cadzow
- bw_csi@fastmail.fm
- scott@cadzow.com