INTERNATIONAL STANDARD

ISO 17427-1

First edition
2018-06

Intelligent transport systems — Cooperative ITS —

Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s)

Systèmes intelligents de transport — Systèmes intelligents de transport coopératifs —

Partie 1: Rôles et responsabilités dans le contexte des ITS fondés sur l'architecture

Reference number
ISO 17427-1:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/TC 204, *Intelligent transport*.

This first edition cancels and replaces ISO/TS 17427:2014 which has been technically revised.

A list of all the parts in the ISO 17427 series can be found on the ISO website.

Introduction

Cooperative Intelligent Transport Systems (*C-ITS*) (3.8) are a promising advancement of Intelligent Transport Systems (ITS). Numerous applications, made possible only, or most efficiently, by the cooperation of *actors* (3.2) (other vehicles, the *infrastructure* (3.12), *service* (3.25) providers, even bystanders), are being devised that open up new possibilities to make traffic safer, more efficient and smarter. Technologies are being developed and improved to realize and support those new *services* and *applications* (3.3). But, to finally implement *C-ITS* and to achieve the benefits of greater safety and better mobility, multiple *actors* will have to cooperate with each other in a completely new way. *Actors* that have to date worked in isolation, i.e. in so called "silos", will have to find a way to achieve these possibilities. New *actors* may also be required for the provision of some *services*. This requires a clear definition and assignment of *behaviours* (3.4), *responsibilities* (3.21) and liabilities. Therefore a general, abstract organizational architecture with the description of the single *roles* (3.22), their *behaviour*, and the corresponding *responsibilities*, is an essential prerequisite for the deployment of *C-ITS*.

The organizational relationships with the description of roles and responsibilities, is a crucial part of the whole *C-ITS* architecture. *C-ITS* is not an objective in itself, it is a means to achieve the potential of service provision through the cooperation of *actors* involved in the ITS sector. The architectural viewpoint comprising the organizational architecture has extensive influences on the deployment and implementation of *C-ITS*.

This document describes the high level roles and responsibilities of a *C-ITS* service provider and aligns it with other *C-ITS* standards and specifications.

Intelligent transport systems — Cooperative ITS —

Part 1:
Roles and responsibilities in the context of co-operative ITS architecture(s)

1 Scope

This document contains a detailed description of the (actor invariant) *roles* (3.22) and *responsibilities* (3.21) required to deploy and operate *Cooperative-ITS (C-ITS)* (3.8). The organization/organization of actors / roles described in this document are designed to be appropriate for any fully operational system that uses the *C-ITS* concepts and techniques in order to achieve its service provision. This document is presented in terms of an organizational or *enterprise viewpoint* (3.10) as defined in ISO/IEC 10746-1.

This document is for all types of road traffic of all classes, and for any other actors involved in the provision of applications and services which use *C-ITS* techniques to achieve service provision. The description of roles is technology agnostic and, in terms of *C-ITS*, agnostic in respect of communication modes and embraces vehicle-vehicle communications, vehicle-infrastructure communications and infrastructure-infrastructure communications.

This document provides a methodology for the identification of service specific roles and their corresponding responsibilities based on a process oriented approach. Additionally, the methodology is used to identify the roles and responsibilities for *C-ITS* in general. Both the methodology as well as the roles and responsibilities for *C-ITS* are deduced from ISO/IEC 10746-1, ISO/IEC 10746-2, ISO/IEC 10746-3, the reference model of Open Distributed Processing. Open Distributed Processing offers five viewpoints of which the *enterprise viewpoint* corresponds with the organizational architecture and its *roles* and *responsibilities*.

To limit the scope of the document to the core of *C-ITS*, the *roles* are separated into external and internal. Considered to be internal are all roles that are highly relevant for the purpose of achieving service provision by means of *C-ITS*. Considered to be external are all roles involved in *C-ITS*, but not set up only for the purpose of *C-ITS*.

This document provides a description of a high-level architectural viewpoint on *C-ITS*. It is designed to be used as a blueprint when implementing service provision systems that use *C-ITS*, and the corresponding organizational structures. The characteristics of *C-ITS* entail a huge number of data/information exchanges. Therefore the implementation stringently respects privacy and data protection as it is defined in ISO/TR 12859 and in national laws and regulations (where instantiated). Privacy and data protection affects all roles defined in this document due to these characteristics and all actors occupying roles in C-ITS respects the corresponding standards and regulations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/TR 12859:2009, *Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems*

ISO 14817-2, *Intelligent transport systems — ITS central data dictionaries — Part 2: Governance of the Central ITS Data Concept Registry*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
action
something which happens; the fact or *process* (3.18) of doing something

EXAMPLE Typically to achieve an aim.

[SOURCE: ISO/IEC 10746-2, 8.3]

3.2
actor
person or organizational unit playing a coherent set of *roles* (3.22) when interacting with the system within a particular use case

[SOURCE: ISO 24014-1:2015, 2.2]

3.3
application
app
software based mechanism of delivering some or all parts of a *service* (3.25)

[SOURCE: ISO 14813-1, 3.2]

3.4
behaviour
collection of *actions* (3.1) with a set of constraints on when they may occur

[SOURCE: ISO/IEC 10746-2, 8.7]

3.5
bounded secure managed domain
BSMD
ITS-S (3.15) *application* (3.3) *processes* (3.18) which function within a controlled environment comprised of an *ITS-S* facilities layer, *ITS*-S networking & transport layer, *ITS-S* access layer, *ITS-S* management entity and *ITS-S* security entity, which adhere to a minimum set of security principles and procedures so as to establish a level of trust between itself and other similar *ITS stations* (3.15) with which it communicates

3.6
client
party which instigates/authorizes the provision of an ITS *service* (3.14)

3.7
community
configuration of *objects* (3.17) formed to meet an objective

[SOURCE: ISO 10746-3, 5.1.1]

3.8
Cooperative-ITS
C-ITS
subset of overall ITS that communicates and shares information between *ITS stations* (3.15) to provide, exchange, or receive, data, give advice or facilitate actions with the objective of improving safety, sustainability, efficiency and comfort beyond the scope of stand-alone systems

Note 1 to entry: As an alternative to a "subset", Cooperative-ITS could be viewed as a "paradigm" in overall ITS.

[SOURCE: ISO/TR 17465-1, 2.1]

3.9
enterprise object
object (3.17) in enterprise *viewpoint* (3.10)

3.10
enterprise viewpoint
viewpoint on an open distributed processing (ODP) system and its environment that focuses on the purpose, scope and policies for that system

[SOURCE: ISO/IEC 10746-3, 4.1.1.1]

3.11
external enterprise object
enterprise object (3.9) involved in C-ITS but not set up for the only purpose of C-ITS

3.12
infrastructure
system of facilities, equipment and *services* (3.25) needed for the operation of an organization

Note 1 to entry: C-ITS specific: static part of C-ITS incorporating sensors, actuators, static *ITS Station(s)* (3.15).

[SOURCE: ISO 9000:2015, 3.5.2]

3.13
internal enterprise object
enterprise object (3.9) within C-ITS set up only as an internal C-ITS mechanism to enable or support the provision of an *ITS service* (3.14) via C-ITS

3.14
ITS service
provides benefits to its *service recipient* (3.28)

3.15
ITS Station
ITS-S
entity in a communication network, comprised of *applications* (3.3), facilities, networking and access layer components that operate using regular wireless communications interface security, or may operate within a *bounded secure management domain* (3.5)

3.16
data lifecycle process
process (3.18) based on data element transformation

3.17
object
model of an entity, characterized by its *behaviour* (3.4) and dually by its state, distinct from any other object, encapsulated, i.e. any change in its state can only occur as a result of an internal *action* (3.1) or as a result of an interaction with its environment

[SOURCE: ISO/IEC 10746-2, 8.1]

3.18
process
sequence of *tasks* (3.32) or set of interrelated tasks which transform inputs into outputs

[SOURCE: ISO 9000:2015, 3.4.1]

3.19
process chain
sequence of processes (3.18) that wait in the background for an event, with some of these processes triggering a separate event that can start other processes in turn

[SOURCE: SAP Help Portal]

3.20
public key infrastructure
PKI
hierarchy of "certification authorities" to allow individuals and organizations to identify each other for the purpose of doing business electronically

3.21
responsible
responsibility
responsibilities
state of being accountable or answerable, as for an entity, function, system, security service or obligation

Note 1 to entry: A responsibility might be a legally backed assignment of *actions* (3.1) to a *role* (3.22).

3.22
role
described by *tasks* (3.32), a *behaviour* (3.4) and *responsibilities* (3.21) and to be associated with an actor

3.23
scenario
general description of activities between (possible) participating *actors* (3.2)

3.24
sequential process
process (3.18) based on sequence of *actions* (3.1) executed

3.25
service
defined functionality to the system which requires a defined set of data as input, processes this data and delivers a defined output

3.26
service in pull mode
ITS service (3.14) actively requesting the data that is required for the service operation

3.27
service in push mode
ITS service (3.14) operating on data delivered without request by an actor or its system

3.28
service recipient
user
actor (3.2) who receives a *service* (3.25)

3.29
stakeholder
individual or organisation having a right, share, claim or interest in a system or in its possession of characteristics that meet their needs and expectations

3.30
sub-role
subordinate *role* (3.22) consisting of a defined fragment of the superior *role* (3.22)

3.31
system
set of interacting or interdependent components forming an integrated whole

Note 1 to entry: Every system is delineated by its organizational and/or spatial and/or temporal boundaries, surrounded and influenced by its environment, described by its structure and purpose and expressed in its functioning.

3.32
task
action that is fulfilled by a role

4 Abbreviated terms

C-ITS	Cooperative ITS
GNSS	Global Navigation Satellite System
HMI	Human Machine Interface
ITS	Intelligent Transport Systems
ITS-S	ITS Station
LDM	Local Dynamic Map
PKI	Public Key Infrastructure
ODP	Open Distributed Processing

5 Compliance

It is recommended that any implementation of an organizational architecture for *C-ITS* (3.8) should comply with this document. Compliance with this document is achieved when all *roles* (3.22) and *sub-roles* (3.30) described in Clause 8 are assigned to corresponding *actors* (3.2) in *C-ITS*.

6 How to use this document

6.1 Roles and responsibilities in the context of Cooperative-ITS

In order for *C-ITS* (3.8) to work cohesively and interoperably, it shall be specified and implemented consistently.

The instantiations of *C-ITS* that will appear over the coming years and decades will vary according to their specific applications and requirements, and will vary in their technology, particularly over time, as the capabilities for these technologies evolve and develop.

While it is not possible today to predetermine future applications in precise detail, it is important that such applications will operate, and most importantly for *C-ITS*, interoperate, within a collaborative environment.

It is therefore necessary, and desirable, to understand the *roles* (3.22) and *responsibilities* (3.21) of *C-ITS* at a general abstracted level, (above that for any particular application) in order to be able to achieve

such consistency of approach, and by so doing, achieve interoperability and indeed, achieve the basic elements required for successful cooperation.

Clauses 7 to 8 provide an explanation of the methodology in this document. This is achieved using an architecture description and analysis technique known as open distributed processing (ODP) (the reasons for which are explained at the beginning of Clause 7).

Annexes A and B provide informative examples of the methodology and its sample application (Annex A), and profiles (Annex B) for different implementation *scenarios* (3.23) for the identified *roles* and *responsibilities*.

This document should be read in concert with ISO/TR 17427-2 to ISO/TR 17427-10, which are a series of complementary Technical Reports which explain and debate the context of many specific aspects of C-ITS such as the "Core System", liability, privacy, risk management etc. These aspects are therefore not defined or explained in detail within this document.

Subclause 6.2 uses the context and roles and responsibilities determined in this document, and provides checklists that are recommended to be used when developing *C-ITS* standards deliverables, or when implementing a *C-ITS* application.

6.2 Guidance for developers and implementers of *C-ITS* application standards

When developing *C-ITS* application standards or implementing *C-ITS* applications and systems, an architecture should be prepared to ensure that all of the relevant *roles* and *responsibilities* involved in *C-ITS*, relevant to the application standards deliverable or the system under development have been considered, and, where appropriate, specified.

Such a process/recommendation does not imply or require any particular form or format to be imposed on a *C-ITS* (3.8) application standard, *C-ITS* application or system, but is designed to ensure that all of the relevant aspects of *roles* (3.22) and *responsibilities* (3.21) have been considered, and where appropriate are clearly identified and specified within that application standard's deliverable or system specification and implementation.

7 Introduction and theoretical framework

7.1 Use of ODP

For the description of an organisational architecture as one of the viewpoints of *C-ITS*, the concept and terminology of ODP according to ISO 10746 (Parts 1 to 3) is applied in this document.

The organisational architecture described corresponds with the *enterprise viewpoint* (3.10) in ODP, defining the purpose, scope and policies governing the activities of the specified system within the organization of which it is part.

Following the concept and terminology of ODP for the description of the *roles* and *responsibilities*, *C-ITS* can be described as a *community* (3.7) composed of *external* and *internal enterprise objects* (3.11/3.13) with the objective of providing *C-ITS* with its benefits regarding safety, efficiency, comfort and sustainability to the *user* (3.28) and minimization of pollution and other adverse ecological effects. *External enterprise objects* are involved in *C-ITS* but are not set up for the sole purpose of *C-ITS*. Therefore this document only includes aspects of *external enterprise objects* and their *roles* and *responsibilities* if they are relevant in respect of *C-ITS*. The *roles* (3.22) within the *internal enterprise objects* are specified in detail in this document.

The ODP reference model provides abstract language for the relevant concepts. It does not prescribe particular notations to be used in the individual viewpoints. The viewpoint languages defined in this reference model of *C-ITS roles* and *responsibilities* are abstract languages in the sense that they define what concepts should be used, not how they should be represented. Precise notations are not specified in this high level overview. The approaches of this deliverable are consciously defined in a notation- and representation-neutral manner, to increase their use and flexibility. However, it is recognized that

further bridging work will be required in the architecture specifications of the individual *services* (3.25) to enable the development of industrial tools for modelling the viewpoint specifications, the formal analysis of the specifications produced, and the possible derivation of implementations for their system specifications.

Within ITS and its projects, and as recommended in ISO 14814, UML (ISO/IEC 19501) is frequently used to describe architecture aspects of ITS for system modelling. However, while UML is proving to be very useful for the specification of specific *systems* (3.31), it proved unnecessarily challenging to present and succinctly analyse the overall *C-ITS roles* and *responsibilities*, and use UML views, for the overarching description of *C-ITS* roles and responsibilities.

For applications and standards which need to map between this ODP overview, and more specific UML application specifications, refer to ISO/IEC 19793.

NOTE ISO/IEC 19793 (usually referred to as UML4 (ODP) defines use of the Unified Modelling Language 2 (UML 2; ISO/IEC 19505-1 and ISO/IEC 19505-2), for expressing the specifications of open distributed systems in terms of the viewpoint specifications defined by the RM-ODP. It defines a set of UML Profiles, one for each viewpoint language and one to express the correspondences between viewpoints, and an approach for structuring them according to the RM-ODP principles. The purpose of UML 4 ODP is to allow ODP modellers to use the UML notation for expressing their ODP specifications in a standard graphical way; to allow UML modellers to use the RM-ODP concepts and mechanisms to structure their large UML system specifications according to a mature and standard proposal; and to allow UML tools to be used to process viewpoint specifications, thus facilitating the software design process and the enterprise architecture specification of large software systems.

7.2 Transferring ODP to roles and responsibilities for C-ITS

C-ITS features the characteristics of a distributed system with its partition of *service* (3.25) delivery via multiple *ITS stations* (3.15), therefore methodologies for the description of distributed systems are consulted when describing the overall architecture of *C-ITS* (3.8) and its different viewpoints. Conveyed to this standard, it is part of the organizational architecture for *C-ITS* and focuses on the description of *C-ITS* specific *roles* (3.22) and *responsibilities* (3.21).

Following the concept and terminology of ODP for the description of the *roles* and *responsibilities*, *C-ITS* can be described as a *community* (3.7) composed of *external* and *internal enterprise objects* (3.11, 3.13) (see Figure 1) with the objective of providing *C-ITS* with its benefits regarding traffic safety, traffic efficiency, comfort and ecological mobility to the user. *External enterprise objects* are involved in *C-ITS* but are not set up for the sole purpose of *C-ITS*. Therefore this document limits itself to the identification of *roles* and *responsibilities* of *external enterprise objects*.

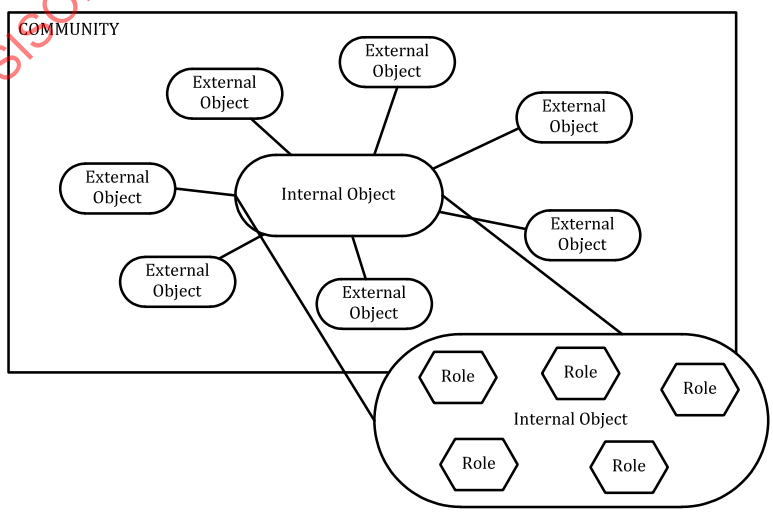


Figure 1 — Relationship between community, internal and external enterprise objects and roles

Internal enterprise object is connected with various *external enterprise objects*. The diagram (Figure 2) illustrates both the *external enterprise objects,* and *internal enterprise objects* in a similar representation

as described in Figure 1, and shows the key relationships in the context of *C-ITS* between the *internal enterprise object* and the *external enterprise objects.*

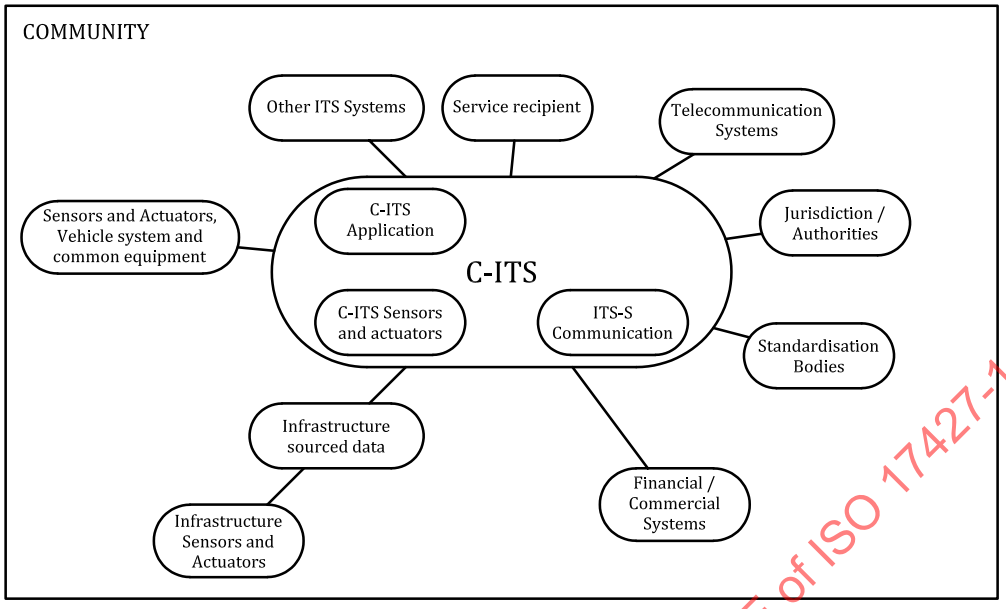


Figure 2 — External and internal enterprise objects in a C-ITS community

C-ITS "enterprise" role and responsibilities

The large oval in the centre of Figure 2 represents the "enterprise" domain of C-ITS (in Figure 1, the "internal object").

C-ITS Sensors and actuators

This term comprises equipment specifically installed to support C-ITS service provision (examples might be lidar, radar, video sensing equipment, etc.).

In the context of ODP, these are "internal objects".

C-ITS applications

These are the specific application services that use C-ITS information to provide their service (examples might be cooperative ice alert, obstacle alert, blind spot warning, ramp access, collision avoidance, etc.).

In the context of ODP, these are "internal objects".

ITS-Station communications (wireless or wired)

This is the means by which one ITS-station interacts with another ITS-station. In the case of communications between vehicles or between vehicles and the infrastructure, this is a wireless communication. In the case of an infrastructure-to-infrastructure C-ITS service provision, this may be wired or wireless.

As these are the essential functions of the "internal object" which enables it to communicate with other objects, in the context of ODP, these communications capabilities are "internal objects".

7.3 External enterprise objects

The following are *external enterprise objects* (3.11) and must meet and pass through the *C-ITS* (3.8) security firewall before their data can be used. In some cases this may be simply the security provisions of the wireless medium, but in some cases will require full BSMD security:

a) **ITS service recipient**

This is the actor who receives the service.

In the context of Figure 1, the service recipient is by definition an external object.

b) **Other ITS systems**

These are other ITS systems, which may well use the vehicle's communications capabilities, but do not provide or use *C-ITS* data or processes (examples might be, service monitoring/reservation, temperature monitoring, fleet management etc.).

In the context of Figure 1, other ITS applications are an external object.

c) **Sensors, actuators, vehicle systems and common equipment**

This ODP object comprises common equipment in the vehicle that may be used for *C-ITS* or non-C-ITS service provision (for example gyroscopes, accelerometers, clock, GNSS etc. are used both for non-C-ITS service provision, such as advanced driver assistance systems, and for *C-ITS* service provision, location based services).

In the context of Figure 1 sensor, actuators, vehicle systems and common equipment are an "external object".

d) **Infrastructure sensors and actuators/infrastructure sourced data**

Many *C-ITS* services may rely on infrastructure sourced information, much of which may come from embedded sensors and actuators (but could also come from the output from other systems, e.g. temperature gauges and received meteorology service information).

In the context of Figure 1, infrastructure sensors and actuators as well as infrastructure sourced data are an external object.

e) **Jurisdictions/authorities**

C-ITS service provision has to take place within the legal framework of a jurisdiction.

In the context of Figure 1, jurisdictions are an external object.

f) **Standardization bodies**

C-ITS can only operate in an interoperable environment. Such interoperability is most commonly achieved by "standards" developed in standardization bodies to which all actors agree to/comply.

In the context of Figure 1, standards bodies are an external object.

g) **Commercial/financial systems**

Many *C-ITS* services will be paid for by service event or subscription (examples might be parking fees, route optimization, etc.).

In the context of Figure 1, commercial / financial systems are an "external object".

It is essential to understand that *C-ITS* is not an end objective in itself, but is a means of achieving application *service* (3.25) delivery.

NOTE The relations of external and internal enterprise objects for *C-ITS* as it is shown in Figure 2 could also be mapped to other ITS subsystems. This implies that the arrangement of objects and their assignment to internal and external might change in other paradigms.

7.4 Internal enterprise objects

C-ITS as *internal enterprise objects* (3.13), consist of a set of specific *roles* (3.22) identified and described in the subsequent clauses of this document. The methodology that describes how these *roles* and *responsibilities* (3.21) originally were identified and verified can be found in Annex A.

8 Roles and responsibilities

8.1 Introduction

All *roles* (3.22) and the corresponding *responsibilities* (3.21) identified through use of the methodology described in Annex A are described in the following paragraphs.

8.2 Generic description of organizational architecture

In the generic view of the organizational architecture four major *roles* (3.22) were identified (Figure 3):

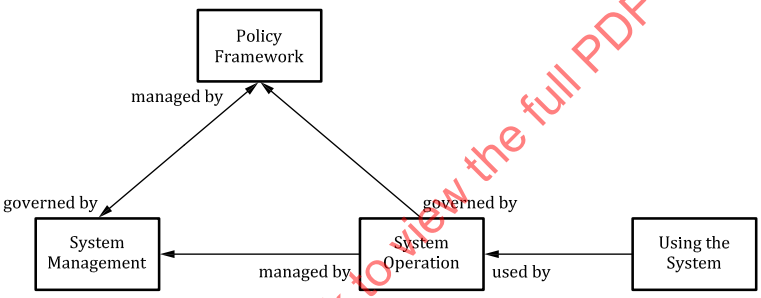


Figure 3 — Global description of organisational architecture

8.2.1 System operation

The *role* "system operation" is *responsible* for the proper execution of the *applications* (3.3) that provide the end-to-end *ITS service*(s) (3.14). This includes the reliability for the coordination, organization and execution of the whole *process* (3.18). One of the major interfaces of this *role* is with the *actor*(s) (3.2) of the *role* "functional operation" who uses the system.

Relationships with other *roles*:

The *role* system operation is connected with the *role* "system management". In this relationship denominated with the term "managed by" in Figure 3, the *actor*(s) with the *role* system management provides supporting functionalities to the *actor*(s) with the *role* "system operation". This mainly includes functionalities enabling and facilitating the "System management" *behaviour* (3.4) and *responsibilities*.

The *role* "system operation" is connected with the *role* "policy framework". In this relationship denominated with the term "governed by" in Figure 3, the *actor*(s) with the *role* policy framework provides policies and regulations as well as their enforcement to the *actor*(s) with the *role* system operation.

The *role* system operation is connected with the *role* "functional operation". In this relationship denominated with the term "used by" in Figure 3, the *actor*(s) (3.2) with the *role* system operation provides the system to the *actor*(s) with the *role* functional operation. The *role* functional operation uses this system.

8.2.2 Functional operation

The *role* (3.22) "functional operation" is *responsible* (3.21) for the proper functional operation of its particular *sub-role*. To perform an appropriate operation an *actor* (3.2) of the *role* functional operation uses the system provided by *actor*(s) of the *role* system operation.

8.2.3 System management

The *role* "system management" is *responsible* to fulfil all required management activities within the system. This especially includes activities supporting system operation. Additional *actions* (3.1) are the management of the policy framework activities.

Relationship with other *roles*:

The *role* "system management" is connected with the *role* policy framework. In this relationship denominated with the term "managed by" in Figure 3, the *actor(s)* with *role* system management provides supporting functionalities to the *actor(s)* with the *role* policy framework. This mainly includes functionalities enabling and facilitating the policy framework *behaviour* (3.4) and *responsibilities*. Additionally, the *actor(s)* with the *role* policy framework provide(s) policies and regulations as well as their enforcement to the *actor(s)* with the *role* system management. This is denominated with the term "governed by" in Figure 3.

8.2.4 Policy framework

The *role* "Policy framework" is *responsible* for all governing and institutional activities required in the *system* (3.31).

Relationship with other *roles*:

Relationships of *role* policy framework with *role* system operation and *role* system management have already been given in 8.2.1 and 8.2.3.

All main *roles* "system operation", "system management", "policy framework" and "functional operation" are detailed with *sub-roles*. Those are described in the following subclauses.

8.3 General responsibilities of actors involved in C-ITS

8.3.1 Registration and authorization

Prior to the use of the system each *role* and therefore each *actor* shall be *responsible* to participate in activities related to the request of access permission. This includes both registration and authorization:

— Registration — defined as registration to the system itself, necessary prior to the first use of the *system*:

  — issue request for registration to the *system*;

  — receive certificates for registered *ITS Stations* (3.15);

— Authorization — defined as authorization prior to every system usage:

  — issue request for authorization;

  — receive confirmation of authorization.

Details of the activities following the registration or authorization request and leading to the reception of a permission or confirmation shall be based on the standard registration and authorization mechanisms described in ISO 14817-2.

8.3.2 Privacy and data protection

The definition of C-ITS as stated in ISO/TR 17465-1 mentions two core characteristics of C-ITS:

— The distributed implementation of *ITS services* (3.14), which requires a huge number of data and information exchanges between *ITS Stations* (3.15) to realize the respective end-to-end *ITS service*.

— The sharing of data and information between *ITS Stations* for purposes other than the original intent.

Both properties lead to serious consequences on C-ITS regarding privacy and data protection.

ISO/TR 12859 provides a detailed description of privacy and data protection issues for *C-ITS* as a whole. Additionally this important subject needs to be reflected in every single *C-ITS* standard including this document. It will be one of the major tasks of the *actors* (3.2) that claim one of the *roles* (3.22) defined in this document to respect the *responsibilities* (3.21) regarding privacy and data protection.

Much of the data/information collected and processed in C-ITS can be associated with an individual. This especially applies to any kind of data/information collected through a vehicle (Floating Car Data) including any *ITS Station* (3.15) that is moving, e.g. mobile devices. Therefore this content is subject to strict privacy and data protection regulations and the *roles* collecting or handling this content have to respect the corresponding privacy regulations.

Each *role* and therefore each *actor* is *responsible* to respect ISO/TR 12859 when participating in C-ITS.

In general this applies for the following *actions* (3.1):

— Collection of data/information (content) — each *actor* collecting data/information (including the hand-over of data/information from other parties) handles this data/information with care and respect for the originators privacy based on the principles advised and referenced in ISO/TR 12859 and the international agreements that it references.

— Processing of data/information (content) — each *actor* processing data/information handles this data/information with care and complies with the principles outlined in ISO/TR 12859 and the international agreements that it references.

— Deletion of data/information (content) after usage — each *actor* handling data/information ensures the proper deletion of data/information after usage based on the principles outlined and referenced in ISO/TR 12859 and the international agreements that it references.

— Transmission of data/information (content) — each *actor* providing a *service* (3.25) that transmits data/information respects the principles outlined in ISO/TR 12859 and the international agreements that it references.

Any *role* described in the following clauses will in some way utilize data/information collected or used in *C-ITS* and therefore needs to comply with these requirements.

8.4 Role — Functional operation

8.4.1 General

The *role* "functional operation" is *responsible* for all activities related to the functional operation of the *system*.

The *role* (3.22) "functional operation" has two different aspects modelled as *sub-roles* (3.30) "generic functional operation" and "specific functional operation". Each *actor* (3.2) with a *role* "functional operation" has at least one *sub-role* in generic functional operation and at least one *sub-role* in specific functional operation. The generic functional operation reflects the *process chain* (3.19) of the corresponding *services* (3.25) and the specific functional operation reflects the functional *sub-role* within a specific *C-ITS* (3.8) *scenario* (3.23).

The following figure shows the relation between the *sub-role* of the *role* functional operation. The dash-line oval shows an example where an *actor* has the generic *sub-role* "service provider" and the specific *sub-role* "roadworks operator" (Figure 4):

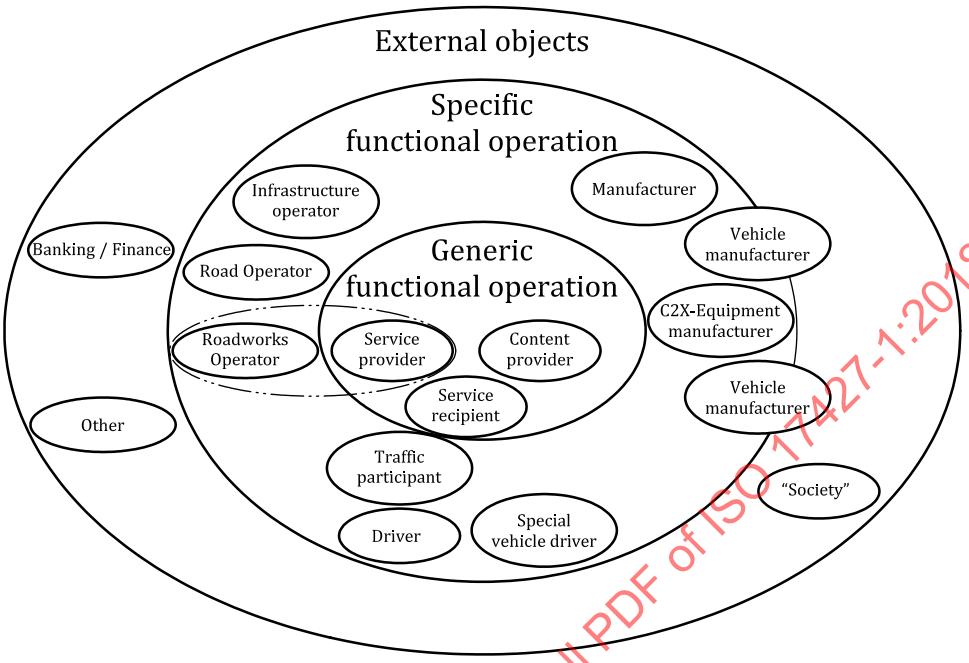


Figure 4 — Relation between generic and specific functional operation

8.4.2 Sub-role — Generic functional operation

The *sub-role* generic functional operation reflects the *process chain* (3.19) of the corresponding *services*.

The *sub-role* generic functional operation is composed of the *sub-roles* "content provider", "service provider" and "service recipient".

8.4.2.1 Sub-role — Content provider

The *sub-role* "content provider" shall provide various types of content. This includes every type of data between raw data and highly (pre-) processed information.

Prior to the provision of content, the *sub-role* shall be *responsible* (3.21) for the registration of itself as a content provider and the content that is provided. It responsible for

— subscribing the content provision activity,

— cancelling the content provision activity,

— the registration of content (data/information), and

— the cancellation/deregistration of content (data/information).

Details of content (data/information) registration related activities can be found in ISO 14817-2.

The *responsibilities* (3.21) associated with this *sub-role* (3.30) that have a tight relation to the service provider itself are

— receive content request,

— obtain content (data/information), and

— provide content (data/information).

Additionally the *sub-role* content provision is responsible for ensuring data integrity.

8.4.2.2 Sub-role — service provider

The *sub-role* "service provider" shall connect the *sub-role* content provider with the *sub-role* "service recipient".

The *sub-role* service provider identifies which algorithm is suitable to fulfil the end-to-end *ITS service* (3.14). It determines the content that is required to run the *ITS service*, afterwards runs the *ITS service* and provides a suitable *service* (3.25) response. The content required to run the *ITS service* is requested and received from the *sub-role* content provider. The *service* results shall be delivered to the *sub-role* service recipient.

Prior to the provision of the *ITS service*, the registration of the *ITS service* with the *role* (3.22) "service catalogue management" shall be required. The *sub-role* service provider shall be responsible for the activities:

— subscribe new *ITS service*;

— cancel/deregistration of *ITS service*.

Details of these activities are described in ISO/TS 17419.

The *responsibilities* related to the *sub-role* service provider that have a tight link to the execution of the *service* itself are

— receive *service* request,

— select *ITS service/application* (3.3)/algorithm,

— operate *ITS service/application*/algorithm (service generation),

— request content (data/information) for *service* execution,

— receive content (data/information) for *service* execution, and

— provision of *service* (result).

8.4.2.3 Sub-role — Service recipient

The *sub-role* "service recipient" incorporates the triggering of *ITS services* available within the system. The entity occupying the *sub-role* therefore issues *service* requests and receives *service* responses.

The *responsibilities* (3.21) related to the *sub-role* (3.30) "service recipient" therefore have a tight relation to the "Service operation" itself:

— issue service request,

— recognition of service result presentation,

— judge the need for reaction,

— react accordingly,

— subscribe to service.

8.4.3 Sub-role — Specific functional operation

The *sub-role* "specific functional operation" reflects the functional *sub-role* within a specific *C-ITS* (3.8) *scenario* (3.23).

The *sub-role* specific functional operation is composed of the *sub-roles* "traffic participants", "infrastructure operator" and "manufacturer".

8.4.3.1 Sub-role — Traffic participant

The *sub-role* "traffic participant" summarizes traffic participants in a specific *C-ITS scenario*.

The *sub-role* "traffic participant" is composed of the *sub-roles* "driver" and "special vehicle driver".

8.4.3.1.1 Sub-role — Driver

The *sub-role* "driver" participates in a specific *C-ITS scenario* as a vehicle driver.

8.4.3.1.2 Sub-role — Special vehicle driver

The *sub-role* "special vehicle driver" participates in a specific *C-ITS scenario* as a driver of a special vehicle like police car or emergency car.

8.4.3.2 Sub-role — Infrastructure operator

The *sub-role* "infrastructure operator" summarizes any *infrastructure* (3.12) operator involved in a specific *C-ITS scenario*.

The *sub-role* infrastructure operator is composed of the *sub-roles* "road operator" and "roadworks operator".

8.4.3.2.1 Sub-role — Road operator

The *sub-role* "road operator" shall be *responsible* for the operation of a road.

8.4.3.2.2 Sub-role — Roadworks operator

The *sub-role* "roadworks operator" shall be *responsible* for the operation of roadworks.

8.4.3.3 Sub-role — Manufacturer

The *sub-role* "manufacturer" shall be *responsible* for the manufacturing of any products used in a specific *C-ITS scenario*.

The *sub-role* manufacturer is composed of the *sub-roles* "C2X equipment manufacturer", "vehicle manufacturer" and "infrastructure manufacturer".

8.4.3.3.1 Sub-role — C2X equipment manufacturer

The *sub-role* (3.30) "C2X equipment manufacturer" shall be *responsible* (3.21) for the manufacturing of C2X equipment.

8.4.3.3.2 Sub-role — Vehicle manufacturer

The *sub-role* "vehicle manufacturer" shall be *responsible* for the manufacturing of vehicles.

8.4.3.3.3 Sub-role — Infrastructure manufacturer

The *sub-role* "infrastructure manufacturer" shall be *responsible* for the manufacturing of infrastructure (3.12) products used in a specific *C-ITS* (3.8) *scenario* (3.23).

8.5 Role — System management

The *role* (3.22) "system management" is *responsible* for all management activities in the system. It supports both system operation and policy framework.

The *sub-role*s of the *role* system management are derived from the ones defined in ITIL V3 (Information Technology Infrastructure Library)[31]. Not all *role*s from ITIL V3 will be used in C-ITS — the appropriate ones regarding level of detail and *C-ITS* characteristics were selected. Where necessary *role*s were merged and renamed.

System management is a distributed role (multiple entities).

8.5.1 Sub-role — Service catalogue manager

This *sub-role* shall be *responsible* for up-to-date maintaining of the *service* (3.25) catalogue that lists all registered *ITS services* (3.14) and their status. This includes:

— add new *ITS service* to the *service* catalogue;

— remove any *ITS service* that are unsubscribed from the *service* catalogue.

A detailed description can be found in ISO/TS 17419.

8.5.2 Sub-role — C-ITS architect

This *sub-role* shall be *responsible* for maintaining the implemented *C-ITS* architecture, including architecture viewpoints.

8.5.3 Sub-role — Change manager

This *sub-role* shall be *responsible* for all change activities including collection of change requests, handling of change requests and application of changes.

8.5.4 Sub-role — Test manager

This *sub-role* shall ensure that deployed *ITS services* fulfil their specification.

8.5.5 Sub-role — Service level manager

This *sub-role* shall be *responsible* for negotiating *C-ITS service* level agreements and ensuring that these are met.

8.5.6 Sub-role — Homologation manager

This *sub-role* shall be *responsible* for product certification, test or authorization prior to deployment.

8.5.7 Sub-role — Compliance manager

This *sub-role* (3.30) shall be *responsible* (3.21) to ensure that standards, guidelines, laws and regulations for *C-ITS* (3.8) are followed and applied.

8.5.8 Sub-role — Financial manager

This *sub-role* is optional depending on the type of *ITS service* (3.14) (e.g. free safety related traffic information versus commercial services). The financial manager is *responsible* for managing budgeting, accounting and charging in the context of the *ITS service*.

8.5.9 Sub-role — Service owner

This *sub-role* shall be *responsible* for designing and delivering a particular *C-ITS* end-to-end *ITS service* within the agreed *service* (3.25) levels. *Service* ownership shall as well occur on a per-process step (content provider, service provider) level.

8.5.10 Sub-role — Project manager

This *sub-role* shall be *responsible* for planning and coordinating the resources (including software, hardware) to deploy, operate and maintain *C-ITS*.

8.5.11 Sub-role — Information security manager

This *sub-role* shall be *responsible* for ensuring the confidentiality, integrity and availability of the system, data, information, *C-ITS services* and the *service recipient* (3.28).

8.5.12 Sub-role — Privacy manager

This *sub-role* shall be *responsible* for the compliance with the regulations defined by the privacy body.

8.6 Role — System operation

The *role* "System operation" shall be *responsible* for all activities related to the operation of the system.

The *sub-roles* of the *role* system operation are derived from the ones defined in ITIL V3 (Information Technology Infrastructure Library)[31]. Not all *roles* from ITIL V3 will be used in C-ITS — the appropriate ones regarding level of detail and C-ITS characteristics were selected. Where necessary *roles* were merged and renamed.

8.6.1 Sub-role — Capacity manager

This *sub-role* shall be *responsible* for ensuring that *ITS services* and *infrastructure* (3.12) are able to deliver the agreed capacity and performance targets.

8.6.2 Sub-role — Availability manager

This *sub-role* shall be *responsible* for defining, analysing, planning, measuring and improving all aspects of the availability of a system being cooperative.

8.6.3 Sub-role — Technical analyst

This *sub-role* shall be *responsible* for providing technical expertise and support for the technical management of the C-ITS *infrastructure*.

8.6.4 Sub-role — Configuration manager

This *sub-role* shall be *responsible* for maintaining information about *infrastructure*/equipment/hardware required to deliver C-ITS *services* (3.14).

8.6.5 Sub-role — IT-operations manager

This *sub-role* (3.30) shall be *responsible* for the proper operation of the IT-system.

8.6.6 Sub-role — Access manager

This *sub-role* shall be *responsible* (3.21) for granting the right to use a *C-ITS service* (3.14) to authorized *service* (3.25) recipients and preventing access to non-authorized *service recipients* (3.28).

8.7 Role — Policy framework

The *role* (3.22) "Policy framework" shall be *responsible* for all governing and institutional activities in the system and governs the management and system operational activities.

8.7.1 Sub-role — Non-regulatory policy institution

This *sub-role* shall be *responsible* for the definition of non-regulatory policies (e.g. agreements between *stakeholder*s (3.29), regulations) regarding the design, implementation, deployment or operation of *C-ITS* (3.8).

8.7.2 Sub-role —Cooperative ITS Credential Management system (CCMS)

This *sub-role* is a high-level aggregate representation of the interconnected systems that enable trusted communications between mobile devices and other mobile devices, roadside devices, and centres and protect data they handle from unauthorized access.

8.7.3 Privacy body

This shall be responsible for the definition of privacy policies.

8.7.4 Information security body

This shall be responsible for the definition of information security policies.

8.7.5 Sub-role — Authority

This *sub-role* shall be *responsible* to define the regulatory policies regarding the design, implementation, deployment or operation of *C-ITS*.

A description can be found in national documents describing the goals.

8.7.5.1 Sub-role — Legislative

Legislative is defined as an institution, which is *responsible* for enacting laws within a state.

8.7.5.2 Sub-role — Jurisdiction

Jurisdiction is defined as the right, power, or authority to administer justice by hearing and determining controversies.

8.7.5.3 Sub-role — Executive

Executive is defined as the executive authority of a state.

8.8 Profiles

A profile provides a set of one or more base assignment of *role*s and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base *role*s (or in the case of ITS systems, standards or otherwise defined systems), necessary to accomplish a particular function/ *service* (3.25) with its characteristics.

The different profiles demonstrate key characteristics of an organisational architecture:

— one *role* (3.22) can be assigned to multiple *actor*s (3.2),

— one *actor* can occupy multiple *role*s.

Annex A
(informative)

Methodology and its sample application

A.1 Methodology to identify Cooperative-ITS (C-ITS) roles, behaviour and responsibilities

A.1.1 Introduction

To identify the *roles* (3.22) and *responsibilities* (3.21) in the context of *C-ITS*, based on architecture(s) for cooperative systems, an abstract methodology is defined. This methodology can be applied to any *C-ITS service* (3.14). It starts from the identification of the *ITS service* specific *stakeholder*s (3.29) and *actor*s (3.2), identifies their *behaviour* (3.4) and *responsibilities* with the support of an abstract *process* (3.18) description of the *service* operation and finally transforms the results into a basic organisational model for this *ITS service*.

A.1.2 Stakeholders

For the implementation of C-ITS, various players from different industries that did not collaborate so far will have to cooperate to realize one or more of the numerous implementation *scenario*s (3.23) of *ITS service* (3.14).

*Stakeholder*s are not necessarily active participants in C-ITS – they only have an occasional interest in the deployment and/or operation of *C-ITS* itself. Hence the group of *stakeholder*s incorporates the following entities:

— national/regional authorities (e.g. government, ministry);

— interest groups [e.g. user (3.28)];

— lobby groups (e.g. industry);

— industry associations.

A.1.2.1 Actors

C-ITS can be implemented in various *scenario*s with the participation of different *actor*s (3.2). A structure was developed to clearly arrange the different *actor*s. On the first level, the structuring elements are the C-ITS components to which the behaviour of the *actor*s can be assigned to, more precisely

— the hardware platform (sensors, actuators, others) that is required to execute the *ITS service*, both mobile and static, and

— the software running on this hardware platform to provide the *ITS service.*

The *actor*s in these fields are further subdivided into those *responsible* for

— operation,

— system management functionalities like maintenance and installation/disassembly, and

— policy framework functionalities like agreement on frameworks.

EXAMPLE There will be an *actor* who has a *behaviour* (3.4) and *responsibilities* (3.21) tied to the operation of the hardware platform. Another one will maintain the software part.

The focus of this document is the operation of *C-ITS* (3.8). Other fields are only considered if they include functionalities directly supporting system operation. This applies for the system management and policy framework part which supports the system operation.

Based on this coarse-grained structure the following *actors* (3.2) are identified. The listing does not claim to be complete it only should give an idea of potential *actors*.

a) Hardware

   1) Operation

      — road operator
      — radio station
      — communication provider
      — driver
      — traveller
      — vehicle manufacturer
      — vehicle supplier
      — mobile device manufacturer

   2) System management

      — road maintenance staff
      — communication maintenance staff
      — OEM dealer network
      — *infrastructure* (3.12) manufacturer
      — vehicle manufacturer
      — *service* (3.25) provider
      — traffic manager
      — freight and fleet manager
      — police

   3) Policy framework

      — standardization organisations
      — certification organization
      — national / European judiciaries
      — consortium of *stakeholders* (3.29) /*actors* (3.2)

b) Software

   1) Operation

      — software provider
      — driver

- road operator

2) System management
   - software maintenance provider
   - software provider
   - vehicle manufacturer
   - *infrastructure* (3.12) manufacturer
   - problem manager
3) Policy framework
   - *public key infrastructure* (3.20)/trusted third party
   - standardization organisations
   - consortium of *stakeholders*/*actors*

A.1.3 Basic service independent process descriptions

A.1.3.1 Applied approach

In preparation for the identification of the basic organisational model the methodology provides a two-stage approach. The starting point is the *ITS service* (3.14) for which the corresponding organizational structure shall be determined.

In principle any *ITS service* is a set of different *applications* (3.3) working together to provide the *service* (3.25) result to the user. Together, these *applications* form a course of *action* (3.1) that is characteristic for the specific *ITS service*, called a *process* (3.18). The approach that is described in this subclause differs between two different description perspectives: a *sequential process* (3.24) with its variations for *services in push mode* (3.27) and *pull mode* (3.26). And a *data lifecycle process* (3.16), which is the transformation result of the *sequential process* and finally finds its way into the basic organisational model.

A.1.3.2 Sequential process description

A.1.3.2.1 Push and pull mode

The description of the *sequential process* (3.24) follows in its timeline the single *actions* (3.1) moulded by the respective *applications* (3.3). Hence the description does not necessarily start from the detection of the event but might start with the request to run the *ITS service* (3.14).

In general, there is discrimination between *ITS services in push mode* (3.27) and *pull mode* (3.26). An *ITS service in push mode* consists of two independent *processes* (3.18) each describing the course of events of one or more *applications*:

- one collecting the data (e.g. triggered periodically within a defined time interval) and storing them temporarily in a database for future usage;
- the other containing the main *process* of the *ITS service* that turns some input data (usually the one collected in the other *process*) into the *service* (3.25) result by executing the service specific algorithm.

The intermediate storage/database links both independent *processes* with each other (see Figure A.1).

The classification of an *ITS service* as *service in push mode* (3.27) is based on the characteristics of the content provision: the content, that is required for the execution of the *service* is not requested explicitly when the corresponding *application* (3.3) needs this content but is constantly collected and buffered in

a temporary database. The content collection includes internal processes (own sensors) as well as third parties delivering information with the support of a communication provider.

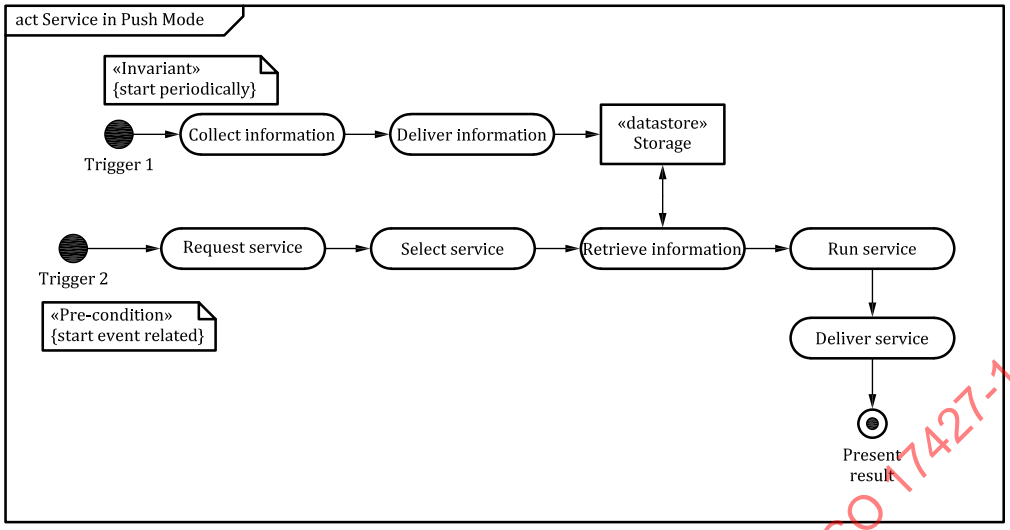


Figure A.1 — Abstract process description of a *service in push mode*

A *service in pull mode* (3.26) explicitly requests the content that is required for the transformation in the *service* (3.25) result. Compared with the *service in push mode* (3.27) this means that there is no constant, periodically triggered data collection and buffering. The required content is demand-oriented. (Figure A.2).

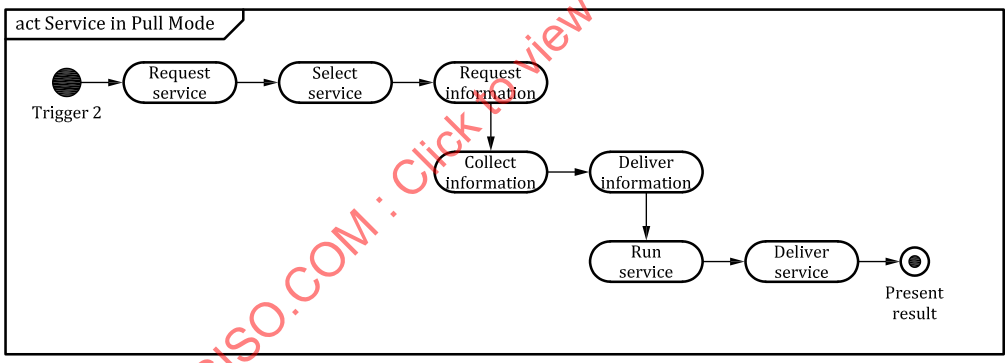


Figure A.2 — Abstract process description of a *service in pull mode*

Both the *service in push mode* (3.27) and *pull mode* (3.26) use similar elements. Certain abstract activities and functionalities may be bundled into manageable modules, in order to illustrate that they are logically belonging together, i.e. forming a common sub-process with fixed sequences of actions. For different *services* (3.25) slight differences between the activities within a module are possible. The general sequence of modules both for *services in push* or *pull mode* is stable. This is why it is named basic *sequential process* (3.24) description.

A.1.3.3 Modules

The differentiation of the various *services* (3.25) mainly relies on a detailed description of the single modules. This applies especially for the “run service” (description see below) module that contains the core *ITS service* (3.14) algorithm.

The modules for both *services in push mode* (3.27) and *pull mode* (3.26) are similar in their general description. This general description can be found in Table A.1.

Table A.1 — Basic modules

Start *service* (3.25)	trigger *service* time dependent upon request incident based others
Request *service*	— issue a request on a *service* result — arrange requirements specifying the expectations regarding the result — deliver request to recipient
Select *service*	— select a *service* based on the received request — apply description of requirements on selection — trigger *service* start
Collect data	— connect to sensor delivering data — combine sensor data with time stamp position (GNSS) detector ID — store data (short-term) in local database
Deliver data	— deliver the data collected to the intermediate storage
Request/Receive data	— *pull mode* only: data are requested, data are received
Retrieve data	— *push mode* only: collected data are retrieved from intermediate storage — forward mode only: information that shall be forwarded is retrieved
Retrieve request	— forward mode only: request that shall be forwarded is retrieved
Run service	— run algorithm over data - detailed single steps will depend on service — handle errors
Provide information	— deliver *service* results to recipient — including restriction of usage and legal restrictions
Display information	— present information to user

In the implementation of an *ITS service* (3.14), the *behaviour* (3.4) and *responsibilities* (3.21) that are part of the single modules are assigned to *ITS service* specific *actors* (3.2). The single corresponding *actions* (3.1) relate to the later identified *roles* (3.22).

A.1.3.4 Lifecycle process description

The detailed basic *lifecycle process* (3.16) description (see Figure A.3) starts with the detection of an event through a sensor. Raw data are collected and (optionally) transmitted with support of the modules "Data Delivery" (sender) and "Data Reception" (recipient) (grey shaded boxes). Several pre-processing mechanisms are executed on the data like aggregation, fusion and quality check. If necessary, the pre-processed data/alias information is transferred again (grey shaded boxes "Content Delivery", "Content Reception"). The receiver potentially executes a fusion of multiple information sources, generates the info-service and provides a preformatted *service* (3.25) result. This is (optionally) transferred (grey shaded boxes "Info-Service Delivery", "Service Reception"). The receiver renders the received *service* result and finally presents it.

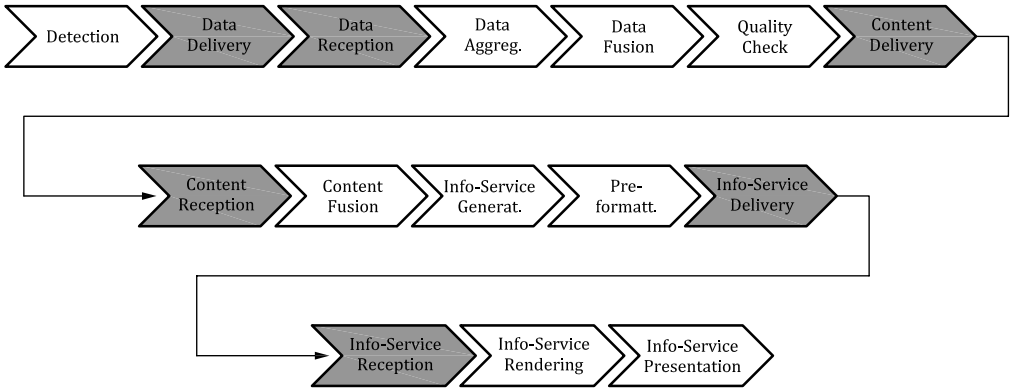


Figure A.3 — Detailed *lifecycle process* description

This abstract basic *lifecycle process* (3.16) description is adapted from the TISA value chain for traffic information[19].

A.1.3.5 Transformation of sequential to *lifecycle process* description

To facilitate the identification of the basic organisational model, the *sequential process* (3.24) description (Figure A.4) is transformed into a *lifecycle process* (3.16) description (Figure A.5). That means that the sequential time-dependent viewpoint on the *ITS service* (3.14) is changed to a data lifecycle-oriented viewpoint. This facilitates the transition to the basic organisational model.

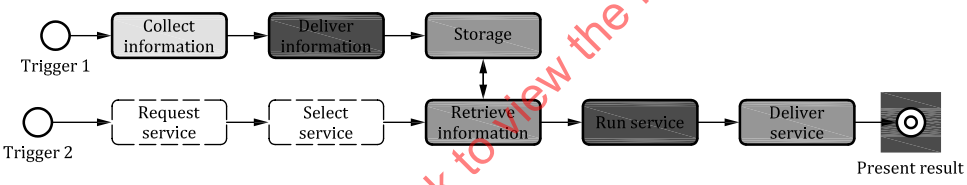


Figure A.4 — Transformation — *Sequential process* description

In the course of the transformation, information about the lifecycle of data elements that are central building blocks of the *ITS service* (3.14) is extracted from the *sequential process* (3.24) description. Different states of the raw data are tracked and the whole lifecycle is modelled. The basic underlying concept is the transition of a sensor detected event to a highly processed *service* (3.25) result that is presented to the user through an actuator.

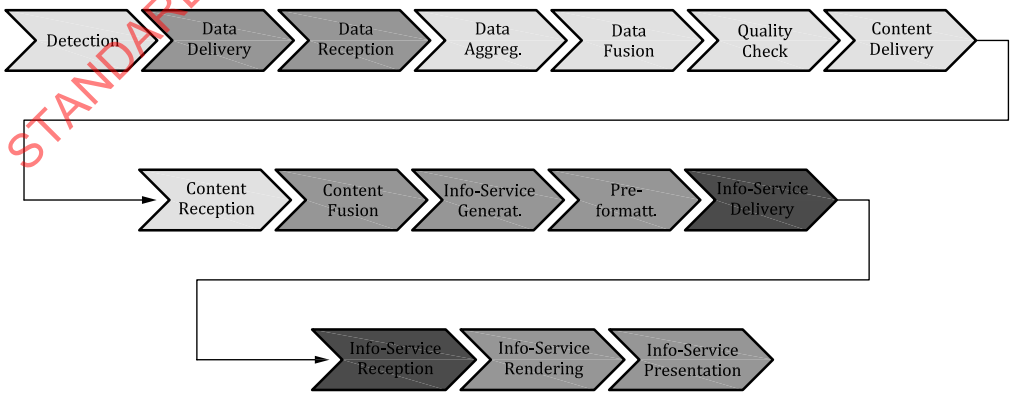


Figure A.5 — Transformation — *Lifecycle process* description

Corresponding activities in Figure A.4 and Figure A.5 are identically shaded:

— Collect information corresponds with detection;

— Deliver information corresponds with data delivery and data reception;

— Storage and retrieve information corresponds with data aggregation, data fusion, quality check, as well as with content delivery and content reception;

— "Run service" corresponds with content fusion, info-service generation, pre-formatting;

— "Deliver service" corresponds with info-service delivery, info-service reception;

— Present results corresponds with info-service rendering, service presentation.

The transformation itself is independent of the *push mode* (3.27) and *pull mode* (3.26) identified in the *sequential processes* (3.24) description, hence there will be only one *lifecycle process* (3.16) description.

A.1.3.6 From the lifecycle process description to a basic organisational model

Figure A.6 shows the *process* (3.18) of simplifying the *lifecycle process* (3.16) description from Figure A.3 (detailed basic *lifecycle process* description). In the general *lifecycle process* description:

— data/information transmission (data delivery, data reception, content delivery, content reception, *service* (3.25) delivery, *service* reception) are neglected. They are classified as supporting functionalities and will be assigned to the System Management (general) in the final organizational architecture;

— *process* steps are merged into four major steps together describing an end-to-end *ITS service* (3.14);

— detection;

— content processing;

— info-service generation;

— service presentation.

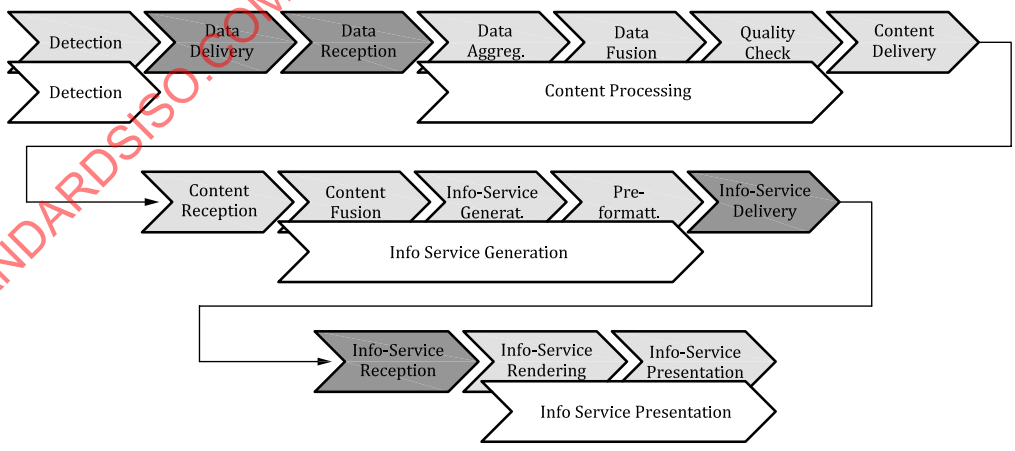


Figure A.6 — General *lifecycle process* description

The general *process* (3.18) description in Figure A.6 is used as a basis for the identification of the basic organisational model.

A.1.4 Basic organisational model

The abstract description of a *service* (3.25) with the *lifecycle process* (3.16) description and the identification of *actors* (3.2) active in the single *process* (3.18) steps allows developing a basic organisational model for the *service* operation.

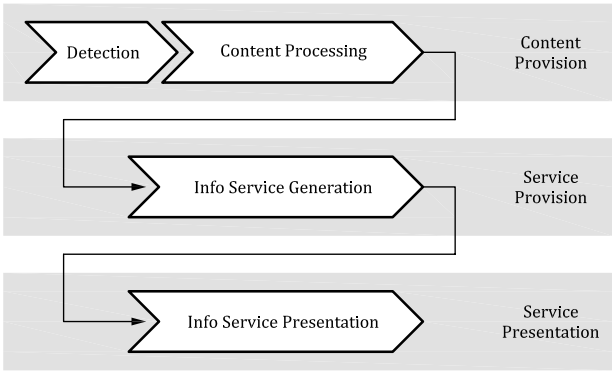


Figure A.7 — Identification of *roles* — Structuring the *ITS service process chain*

Structuring the activities described in the *lifecycle process* (3.16) description leads to the three main *actions* (3.1) and *responsibilities* (3.21) (Figure A.7):

— Content provision;

— *Service* (3.25) provision;

— *Service* presentation.

The central focus of the *role* (3.22) "Content provider" is the collection of data from a sensor, aggregation of the data and delivery of the content to the *role* "service provider". The *role* "service provider" executes the *ITS service* (3.14) where an *ITS service* can be both a more complex pre-processing of the content or a traffic safety relevant *ITS service*. The result is delivered to the *role* "Service *presentation*". The *role* "Service *presentation*" evaluates the received *service* result and fulfils required presentation preparations of the *service* result. The *service* result is presented through an appropriate actuator.

The system operation related *roles* are supported by a number of system management and policy framework *roles*. *Roles* from both fields actively support and enable the system operation with their tasks.

A.2 Sample application of methodology — Hazard location warning

A.2.1 General — Hazard location warning

For the verification of the methodology described in A.2, it is applied to hazard location warning as a sample *ITS service* (3.14).

The main purpose of the *ITS service* "hazard location warning" is to inform the driver about an upcoming hazardous location. This could be a traffic situation (accident, tail end of traffic jam), weather situation (heavy rain, ice) or dangerous items (oil, gas, etc.).

A.2.2 Identification of stakeholders and actors

A.2.2.1 Stakeholders

Stakeholders (3.29) for a "hazard location warning" service are probably:

— National/regional government with an interest in improving road safety (e.g. ministry of transport).

A.2.2.2 Actors

Actors (3.2) involved in the *ITS service* (3.14) operation of "hazard location warning" are:

— vehicle or mobile devices (including all or partially: sensors, processing unit, display/HMI);

— *infrastructure* (3.12) — both public or private (including all or partially: sensor, wireless network access point (*ITS Station* (3.15)), traffic control centre, display / variable message sign);

— in presence of *infrastructures*: network provider/operator.

Additionally, different *actors* supporting the system operation are involved with system management and policy framework functionalities, e.g. various service providers, *PKI* (3.20) /trusted third party or standardization organisations.

A.2.3 Basic service independent *process* descriptions

A.2.3.1 *Sequential* process description — Push and pull

The *service* (3.25) presumably includes a data provision in *push mode* (3.27). Therefore, the *sequential process* (3.24) description includes two separate *processes* (3.18) that are linked through the data storage (for diagram see Figure A.1).

In detail, the following *actions* (3.1) are assigned to the single *process* (3.18) steps.

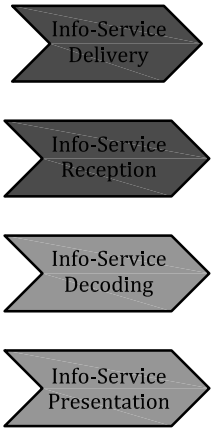
Trigger 1	The trigger event is the hazardous location, e.g. a dangerous traffic situation, weather situation or dangerous object.
Collect information	Sensor detects the event (e.g. vehicle sensor, roadside sensor, weather sensor).
Deliver information	The collected data are provided through public or proprietary interfaces.
Storage	Data storage. This could be for example the LDM implemented in an *ITS-station* (3.15). The data storage might fusion data from different sources, aggregate data, pre-process data, run a quality check.
Trigger 2	The trigger of the main *process* (3.18) is a time-dependent signal periodically starting the service.
Request service	The entity triggering the main *process* (3.18) issues a service request.
Select service	The service request is delivered to the *actor* (3.2) running the hazard location warning service, a service implementation fulfilling the service requirements is selected.
Retrieve information	It is determined which data are required for the execution of the service hazard location warning and the corresponding data are retrieved from the storage. Eventually there is another fusion of content including pre-processing computed.

Run service	Now the hazard location warning service algorithm is executed. The retrieved content is processed by the info-service and a result is computed.
Deliver service	The service result from the previous module is delivered to the presenting *actor* (3.2).
Present result	The warning message is processed by the presenting actor (3.2), including decision of presentation mode, presentation priority and presentation design. Then the warning is presented to the driver.

Figure A.8 — Single *process* (3.18) steps

A.2.3.2 Lifecycle process description

Detection	The sensor detects the hazardous location.
Data Delivery	Sensor data are provided. This part is optional and depends on the implementation.
Data Reception	Sensor data are received. This part is optional and depends on the implementation.
Data Aggreg.	Optional: Aggregation of the collected data.
Data Fusion	Optional: Fusion of data from a different source.
Quality Check	Optional: Quality check of data.
Content Delivery	Pre-processed data (content) is provided. This part is optional and depends on the implementation.
Content Reception	Pre-processed data are received. This part is optional and depends on the implementation.
Content Fusion	Optional: Fusion of content from different sources.
Info-Service Generat.	The service execution based on the content.
Pre-formatt.	Optional: Pre-formatting of service result.



The service result is provided. This part is optional and depends on the implementation.

The service result is received. This part is optional and depends on the implementation.

Preparation of the service result for the presentation that includes selection of presentation mode and presentation priority.

Presentation of the warning to the user.

Figure A.9 — Lifecycle process description

A.2.4 Transformation of sequential to lifecycle process description

The hazard location warning service can be modelled both with the *sequential processes* (3.24) and *lifecycle process* (3.16) description from B.1.2.1 and B.1.2.2. Therefore a transformation like the one described in B.1.2.3 is possible.

A.2.5 From the lifecycle process description to a basic organisational model

The hazard location warning service can be modelled with the abstract *lifecycle process* (3.16) description from B.1.2.2. Therefore a transformation like the one described in B.1.2.4 is possible.

A.2.6 Basic organisational model

The *service* (3.25) hazard location warning complies with the abstract descriptions of *sequential process* (3.24) and *lifecycle process* (3.16). The transition from the *lifecycle process* description to the basic organisational model is also possible. Therefore the *service* hazard location warning makes use of the abstract basic organisational model. That means the “hazard location warning” organizational architecture includes the following *roles* (3.22) regarding service operation:

— Content provider: *Responsible* (3.21) to provide data collection and data pre-processing,

— Service provider: *Responsible* to provide service generation,

— Presentation provider: *Responsible* to provide presentation of service results.

The system operation is supported by system management and policy framework activities with the respective *roles*.

Annex B
(informative)

Profiles

B.1 Profiles

B.1.1 General description

This clause includes different implementation *scenarios* (3.23) for the identified *roles* (3.22) and *responsibilities* (3.21).

An *ITS service* (3.14) might be implemented in multiple ways (*scenarios*). So far, there is no decision which *scenario* will be selected for the future real-world implementation of C-ITS. Furthermore, it is likely that different, interoperable *scenarios* will be implemented in different regions. Therefore this subclause describes the multiple variations.

B.1.1.1 Actors

For an abstract description of the profiles and the identification of the *scenarios* (3.23), the *actors* (3.2) are generally grouped into "vehicle (system)" and "*infrastructure* (3.12) (system)". Members of the "vehicle (system)" group include all vehicle related *actors* including entities *responsible* (3.21) for mobile devices that might or might not be connected with the vehicle itself. Members of the "*infrastructure* (system)" group include both public and private *infrastructure* providers.

This grouping simplifies the real situation. Of course both for the vehicle and the *infrastructure* (system) multiple variations of organization are possible.

B.1.1.2 Scenarios

To stay independent of future implementation choices it is necessary to present a complete set of *scenarios* (3.23) for the system operation part. As already identified in Clauses 8, A.1 and A.2, each scenario will consist of the basic processing stages dedicated to the *roles* (3.22) "content provider", "service provider" and "presentation provider". Each of the *actor* (3.2) groups described in A.1.2 (vehicle system, *infrastructure* (3.12) system) or a combination of both (vehicle system and *infrastructure* system) handles one of the mentioned processing stages. The single processing stages are independent and therefore the *actors* can be combined arbitrarily. This results in the following possible combinations of different *actors*.

NOTE For reasons of simplification the term "vehicle system" is abbreviated to "vehicle" and the term *infrastructure* (3.13) system is abbreviated to "*infrastructure*".

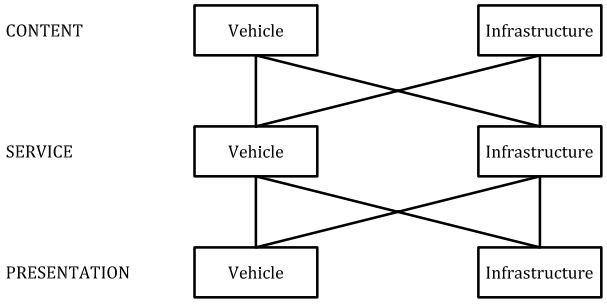


Figure B.1 — Possible *actor* combinations for the description of *scenarios*

Explicitly describing the single combinations of Figure B.1 results in the following basic *scenario* (3.23) combinations:

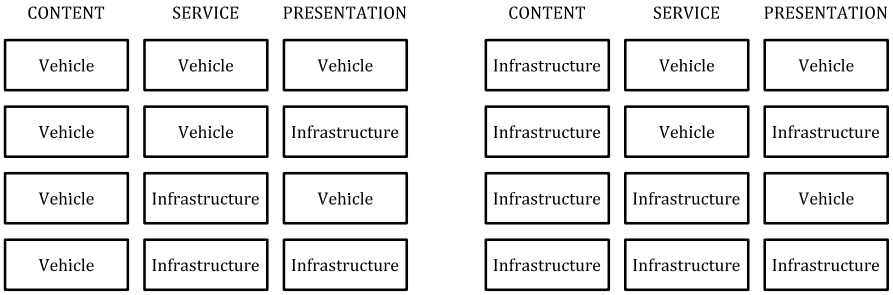


Figure B.2 — *Actor* combinations for basic *scenarios*

Scenarios (3.23) involving either vehicle and/or *infrastructure* (3.12) system *actors* (3.2) for a single processing stage but not both vehicle and infrastructure (vehicle + infrastructure) system *actors* are named basic *scenario*. The possible combinations are illustrated in Figures B.1 and B.2. The remaining *scenarios* are named complex *scenarios* and are composed of two or more corresponding basic *scenario* components.

In B.1.2 the *service* (3.25) implementation of an example *ITS service* (3.14) is modelled for all basic *scenarios*. Complex *scenarios* are not modelled due to the high number of possible implementations, but the *process* (3.18) for identifying potential complex scenarios is described in B.1.1.3.

B.1.1.3 Complex scenarios

The first variation that can be introduced by the combination of basic *scenarios* (3.23) affects the "content provider" – "service provider" transition. The data collected by the vehicle and *infrastructure* (3.12) system can both be delivered to the vehicle or *infrastructure* system for processing (Figure B.3).

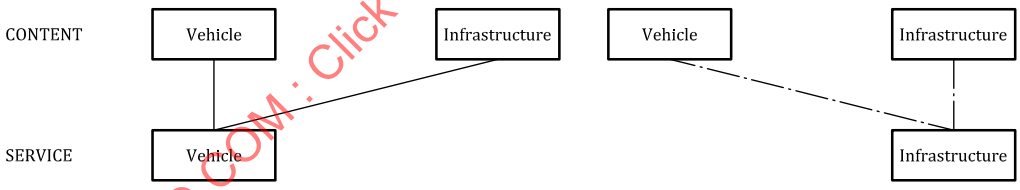


Figure B.3 — Delivery of data from multiple sources to a single recipient

It is also possible, that the vehicle or the *infrastructure* (3.12) system either deliver data both to the vehicle and the *infrastructure* system (Figure B.4).

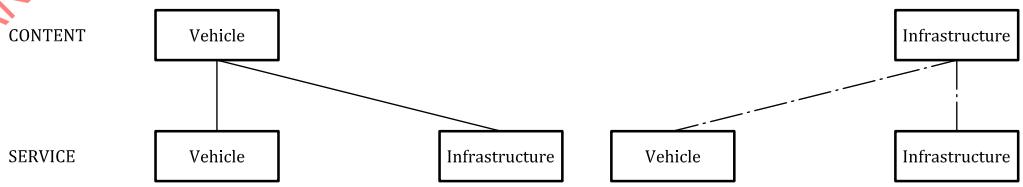


Figure B.4 — Delivery of data from a single source to multiple recipients

The second variation that can be introduced by the combination of basic *scenarios* (3.23) affects the "service provider" – "presentation provider" transition.

The "service provider" might take place either in the vehicle or *infrastructure* (3.12) system but afterwards is delivered to both the vehicle and the *infrastructure* system for the presentation of the results (Figure B.5).

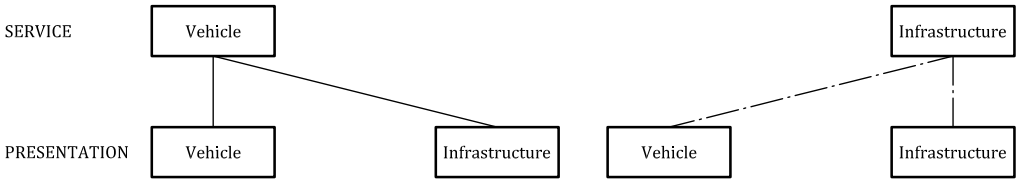


Figure B.5 — Delivery of a single *service* result to multiple recipients

Additionally, the results displayed either in the vehicle or *infrastructure* (3.12) system might come from both the vehicle and the *infrastructure* system (Figure B.6).

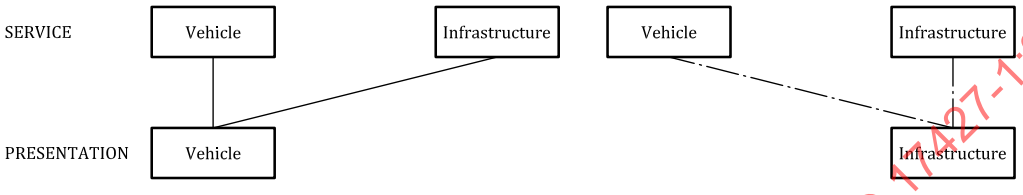


Figure B.6 — Delivery of multiple *service* results to a single recipient

The single descriptions can be combined to a large number of different *scenarios* (3.23).

B.1.1.4 Example of a complex scenario

As stated in B.1.1.2 there are a large number of possible complex *scenarios* (3.23). The following example illustrates the principles of decomposition into basic *scenarios* (Figure B.7).

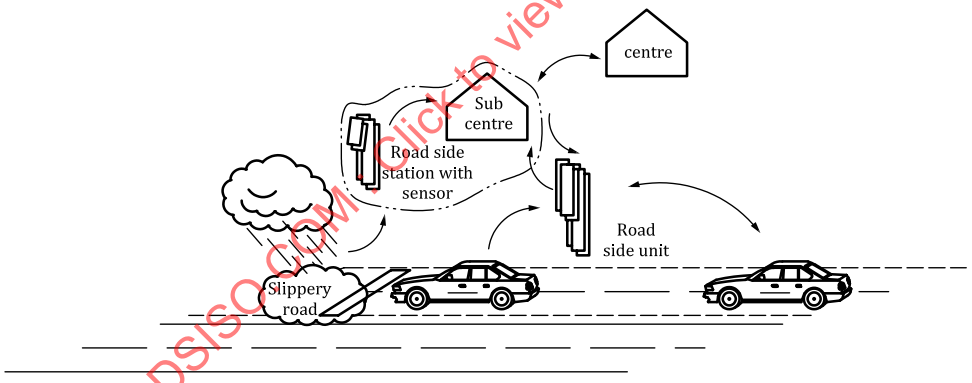


Figure B.7 — Complex *scenario* based on basic *scenarios*

Depending on the different assignment of the *roles* (3.22) to the *actor* (3.2) groups "vehicle system" and "*infrastructure* (3.12) system", different underlying basic *scenarios* (3.23) are identified.

Table B.1 — Alternative combination of basic *scenarios* for complex *scenario* illustrated in Figure B.7

	Roles in system operation			
Alternative	**Content provider**	**Service provider**	**Presentation provider**	**Basic scenarios**
1	Vehicle system *infrastructure* system	Vehicle system *Infrastructure* system	Vehicle system	1 and 7
2	Vehicle system *Infrastructure* system	*Infrastructure* system Vehicle system	Vehicle system	3 and 5
3	Vehicle system *Infrastructure* system	Vehicle system	Vehicle system	1 and 5
4	Vehicle system *Infrastructure* system	*Infrastructure* system	Vehicle system	3 and 7

In Table B.1 the multiple alternatives for the possible combinations of *actor* groups assigned to the different *role*s are listed. For a comparatively simple hybrid *scenario* as illustrated in Figure B.7, four possible combinations of basic *scenario*s exist, depending on which *actor* group is assigned to which *role*.

B.1.1.5 Supporting actions — System management and policy framework

The *scenario*s (3.23) described in B.1.2 focus on the description of the transposition of *role*s (3.22) to *actor* (3.2) groups for the system operation. Naturally every implementation *scenario* additionally deals with system management and policy framework as eminent supporting *role*s. As the profiles (B.1.2) primarily serve as an example and illustration of how the *role*s and *responsibilities* (3.21) might be assigned to the different *actor* groups the description only details this for system operation because this is more concrete.

B.1.2 Hazard location warning — Example scenarios

B.1.2.1 Definition of hazard location warning

The *service* (3.25) "hazard location warning" takes as input a specific traffic situation and delivers a hazard location warning as output.

Situations are for example dangerous traffic, weather, road conditions or any combination of the aforementioned dangerous conditions.

The term "hazardous location" refers to a location specific danger that is applicable for the end *service recipient* (3.28).

The output is a warning message that is presented in an appropriate way.

B.1.2.2 *Scenario* 1

Scenario (3.23) 1 is characterized by the following selection of *actor* (3.2) groups (Figure B.8):

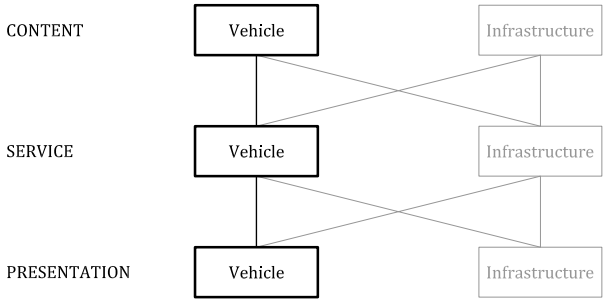


Figure B.8 — *Actor* groups involved in *Scenario* 1

B.1.2.2.1 Figurative description

The data are collected, processed and presented in the vehicle system (Figure B.9).

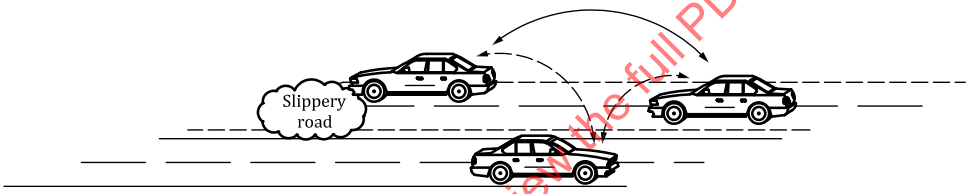


Figure B.9 — Figurative description of *scenario* 1 of *service* hazard location warning

B.1.2.2.2 Assignment of actor groups to roles

In *scenario* 1 the vehicle system is the only *actor* (3.2) hence all the *role*s (3.22) are assigned to *actor*s in the vehicle system (Figure B.10):

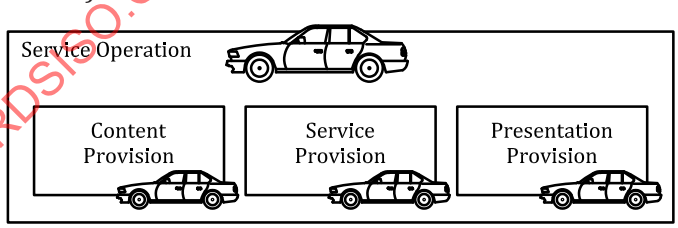


Figure B.10 — Assignment of *actor* groups in *scenario* 1

Service (3.25) operation: *Actor(s)* from vehicle system — might be an organization or consortium

Content provider: *Actor(s)* from vehicle system

Service provider: *Actor(s)* from vehicle system

Presentation provider: *Actor(s)* from vehicle system

B.1.2.3 *Scenario* 2

Scenario 2 is characterized by the following selection of *actor* (3.2) groups (Figure B.11):

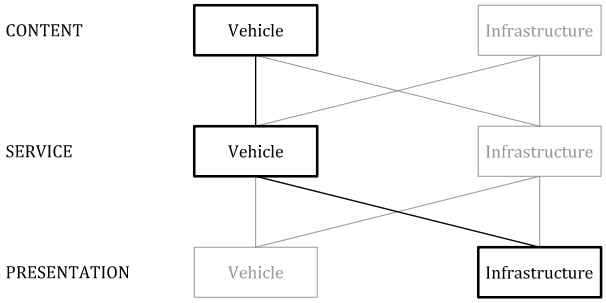


Figure B.11 — *Actor* groups involved in *scenario* 2

B.1.2.3.1 Figurative description

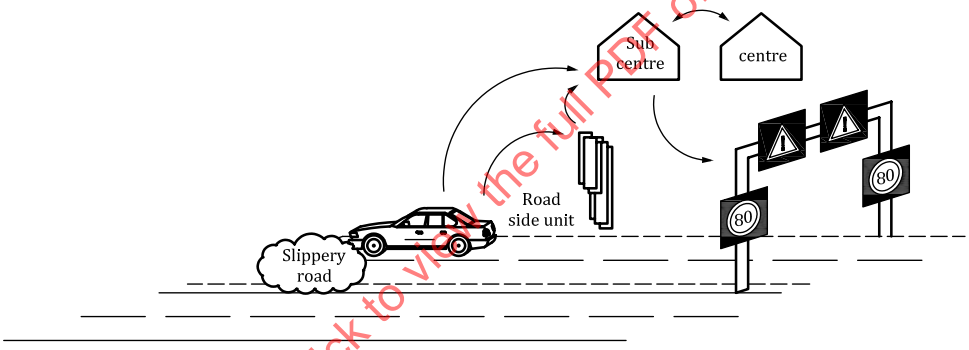


Figure B.12 — Figurative description of *scenario* 2 of *service* "hazard location warning"

The data are collected and processed by the vehicle system. The result of the *service* (3.25) is delivered to the *infrastructure* (3.12) system where it is presented (Figure B.12).

B.1.2.3.2 Assignment of "actor groups" to "roles"

In *scenario* 2 the *actor* (3.2) groups vehicle and infrastructure (3.12) system share the *roles* (3.22) and *responsibilities* (3.18) (Figure B.13).

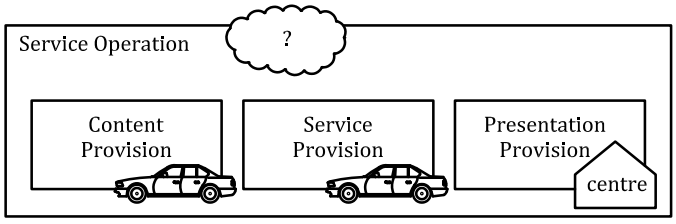


Figure B.13 — Assignment of *actor* groups in scenario 2