TECHNICAL SPECIFICATION

ISO/TS 17427

First edition
2014-07-01

Intelligent transport systems — Cooperative systems — Roles and responsibilities in the context of cooperative ITS based on architecture(s) for cooperative systems

Systèmes intelligents de transport — Systèmes coopératifs — Rôles et responsabilités dans le contexte des ITS fondés sur l'architecture de systèmes coopératifs

Reference number
ISO/TS 17427:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Symbols (and abbreviated terms) **5**
5 Introduction and theoretical framework **5**
5.1 Transferring ODP to roles and responsibilities for C-ITS 5
5.2 External Enterprise Objects 6
6 Roles and responsibilities **8**
6.1 Introduction 8
6.2 General responsibilities of actors involved in C-ITS 9
6.3 Role: System operation 10
6.4 Role: Using the service 12
6.5 Role: System management 12
6.6 Role: Policy framework 14
6.7 Profiles 15
7 Compliance **15**
Annex A (informative) **Methodology and its sample application** **16**
Annex B (informative) **Profiles** **29**
Bibliography **45**

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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

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

Introduction

Cooperative-ITS (C-ITS) are a promising and remarkable advancement of Intelligent Transport Systems (ITS). Numerous cooperative applications are specified that open up new possibilities to make traffic safer, more efficient and smarter. Technologies are developed and improved to realize and support those new services and applications. But, to finally implement C-ITS and to achieve the benefits of more safety and better mobility, various actors from different industries will have to cooperate with each other in a completely new way. Actors that did not collaborate so far will have to find a way to do so. This requires a precise definition and assignment of behaviours, responsibilities and liabilities. Therefore a general, abstract organizational architecture with the description of the single roles, their behaviour and the corresponding responsibilities is the essential basis for the deployment of C-ITS.

The organizational architecture itself with the description of the roles and responsibilities is a crucial part of the whole C-ITS architecture. The organizational architectural viewpoint has extensive influences on the deployment and implementation of C-ITS.

This document describes the high level roles and responsibilities that enable C-ITS Service provision.

Intelligent transport systems — Cooperative systems — Roles and responsibilities in the context of cooperative ITS based on architecture(s) for cooperative systems

1 Scope

This Technical Specification describes the (non-actor specific) roles and responsibilities required to deploy and operate Cooperative-ITS (C-ITS). The organizational architecture described in this document is to be used for a fully operational system. The Technical Specification is couched in terms of an organizational or enterprise viewpoint, as defined in ISO/IEC 10746 Open Distributed Processing.[1]

This Technical Specification is applicable to all types of road traffic of all classes. The description of roles is completely technology agnostic and, in terms of C-ITS communication modes, embraces vehicle-vehicle communications, vehicle-infrastructure communications and infrastructure-infrastructure communications.

This Technical Specification provides a methodology for the identification of service specific roles and their corresponding responsibilities based on a process oriented approach. Additionally, the defined 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 the reference model: Open Distributed Processing (ISO/IEC 10746).[1] Open Distributed Processing offers five viewpoints of which the enterprise viewpoint corresponds with the organizational architecture and the roles and responsibilities.

This Technical Specification separates C-ITS roles into 'external' and 'internal'. Those considered to be internal are all roles set up for the sole purpose of C-ITS and those considered to be external are all roles involved in C-ITS but not set up for the sole purpose of C-ITS.

This Technical Specification describes high-level architectural viewpoint on C-ITS. It can be used as a blueprint when implementing C-ITS and the corresponding organizational structures. The characteristics of C-ITS entail a huge number of data/information exchanges. Therefore, the implementation of the organizational architecture stringently needs to respect privacy and data protection, as defined in ISO/TR 12859 and in the national laws and regulations (where instantiated). Privacy and data protection affect all roles defined in this Technical Specification and due to these characteristics, all actors occupying roles in C-ITS need to respect the corresponding standards and regulations.

2 Normative references

The following referenced documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10746:1996, *Information technology — Open Distributed Processing — Reference model*

ISO 14817:2002, *Transport information and control systems — Requirements for an ITS/TICS central Data Registry and ITS/TICS Data Dictionaries*

ISO/TS 17419, *Intelligent transport systems — Co-operative systems — Classification and management of ITS applications in a global context*"

ISO/TS 17931, *Intelligent transport systems — Extension of map database specifications for Local Dynamic Map for applications of Cooperative ITS*

ISO/IEC 19501:2005, *Information technology — Open Distributed Processing — Unified Modeling Language (UML) Version 1.4.2*

ISO 21217:2013, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

ETSI/TS 102-637:2011, *Intelligent Transport Systems (ITS); Vehicular Communications Basic Set of Applications*

3 Terms and definitions

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

3.1
action
something which happens

[SOURCE: ISO/IEC 10746-2, see Bibliography reference 2]

3.2
actor
user playing a coherent set of roles when interacting with the system within a particular use case

[SOURCE: ISO 24014-1:2007, see Bibliography reference 6]

3.3
application
mechanism of delivering some or all parts of an *ITS service* (3.23)

[SOURCE: ISO/TR 17465-1, see Bibliography reference 18]

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

[SOURCE: ISO/IEC 10746-2, see Bibliography reference 2]

3.5
community
configuration of *objects* (3.13) formed to meet an objective

[SOURCE: ISO/IEC 10746-3, see Bibliography reference 3]

3.6
cooperative-ITS
C-ITS
DEPRECATED: cooperative systems
subset of overall ITS that communicates and shares information between ITS stations to 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, see Bibliography reference 18]

3.7
enterprise object
object (3.13) in *enterprise viewpoint* (3.10)

3.8
external enterprise object
enterprise object (3.7) involved in C-ITS but not set up for the only purpose of C-ITS

[SOURCE: ISO/TS 17574:2009, see Bibliography reference 4]

3.9
internal enterprise object
complementary to *external enterprise object* (3.8)

3.10
enterprise viewpoint
a viewpoint on an ODP system and its environment that focuses on the purpose, scope and policies for that system

[SOURCE: ISO/IEC 10746-3, see Bibliography reference 3]

3.11
infrastructure
system of facilities, equipment and *ITS services* (3.23) that is needed for the operation of an organization

Note 1 to entry: Specifically in the case of C-ITS the most stationary part of C-ITS incorporating sensors, actuators, static *ITS Station(s)* (3.12).

[SOURCE: ISO 9000:2005, see Bibliography reference 7]

3.12
ITS station
entity in a communication network capable of communicating with other similar entities

Note 1 to entry: From an abstract point of view, the term "ITS station" refers to a set of functionalities. The term is often used to refer to an instantiation of these functionalities in a physical unit. Often the appropriate interpretation is obvious from the context. The proper name of physical instantiation of an ITS-S is ITS station unit (ITS-SU).

[SOURCE: ISO 21217:2010, see Bibliography reference 10]

3.13
object
model of an entity

Note 1 to entry: An object is characterized by its *behaviour* (3.4) and dually by its state. An object is distinct from any other object. An object is 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, see Bibliography reference 2]

3.14
process
process that describes a sequence of *actions* (3.1)

Note 1 to entry: A process can also be a set of interrelated or interacting activates which transform inputs into outputs.[8]

[SOURCE: ISO 9000:2005, see Bibliography reference 7]

3.15
process chain
sequence of processes (3.14) that wait in the background for an event

Note 1 to entry: Some of these *processes* (3.14) trigger a separate event that can start other *processes* (3.14) in turn

[SOURCE: SAP Help Portal, see Bibliography reference 9]

3.16
sequential process
process (3.14) based on sequence of *actions* (3.1) executed

3.17
(data) lifecycle process
process (3.14) based on data element transformation

3.18
responsibility
being accountable or answerable, as for an entity, function, system, security service or obligation

EXAMPLE A responsibility might be a legally backed assignment of *actions* (3.1) to a *role* (3.20).

[SOURCE: ISO/TS 17574:2009, see Bibliography reference 4]

3.19
roadside unit
implementation of roadside *ITS Station* (3.12) combined with other roadside equipment

EXAMPLE Sensors, actuator.

3.20
role
identifies a *behaviour* (3.4) to be associated with one of the component objects

[SOURCE: ISO/IEC 10746-2, see Bibliography reference 2]

3.21
sub-role
subordinate *role* (3.20) consisting of a defined fragment of the superior *role* (3.20)

3.22
scenario
general description of activities between (possible) participating *actors* (3.2)

3.23
ITS service
functionality provided to users of intelligent transport systems designed to increase safety, sustainability, efficiency, and/or comfort

Note 1 to entry: This definition also appears in the latest version of ISO 21217.

3.24
ITS service in push mode
ITS service (3.23) operating on data delivered without request by an actor or its system

3.25
service in pull mode
ITS service (3.23) actively requesting the data that is required for the service operation

3.26
stakeholder
individual or organization having a right, share, claim or interest in a system or in its possession of characteristics that meet their needs and expectations

[SOURCE: ISO/IEC 12207:2008, see Bibliography reference 5]

4 Symbols (and abbreviated terms)

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

5 Introduction and theoretical framework

5.1 Transferring ODP to roles and responsibilities for C-ITS

Cooperative-ITS (C-ITS) features the characteristics of a distributed system with its partition onto multiple *ITS stations* (3.12). Hence methodologies for the description of distributed systems are consulted when describing the overall architecture of C-ITS and its different viewpoints. For the description of the organisational architecture as one of the viewpoints of C-ITS, the concept of Open Distributed Processing[1],[2],[3] is applied. The organisational architecture 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". Conveyed to C-ITS, this Technical Specification is part of the organizational architecture for C-ITS and focuses on the description of C-ITS specific *roles* (3.20) and *responsibilities* (3.18).

Following the concept and terminology of ODP for the description of the *roles* (3.20) and *responsibilities* (3.18), C-ITS can be described as a *community* (3.5) composed of *external* and *internal enterprise objects* (3.8, 3.9) (see Figure 1) with the objective of providing C-ITS with its benefits regarding traffic safety, traffic efficiency, comfort and ecologic mobility to the user. *External enterprise objects* (3.8) 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* (3.8).

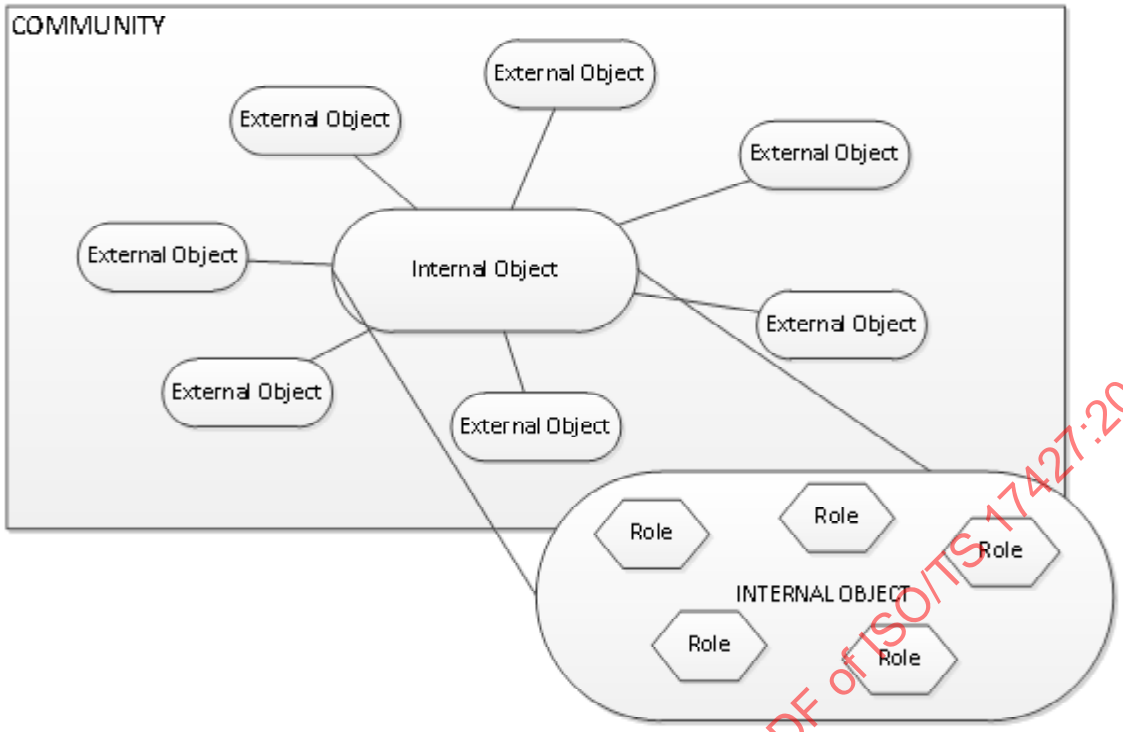

Figure 1 — Relationship between Community, Internal and External Enterprise Objects and Roles

5.2 External Enterprise Objects

C-ITS, as *internal enterprise object* (3.9), is connected with various *external enterprise objects* (3.8). The diagram (Figure 2) illustrates the *external enterprise objects* (3.8) and their interfaces to the *internal enterprise object* (3.9). Figure 2 shall illustrate the variety of parties (*external enterprise objects*) involved in C-ITS. The *external enterprise objects* (3.8) comprise examples from different levels.

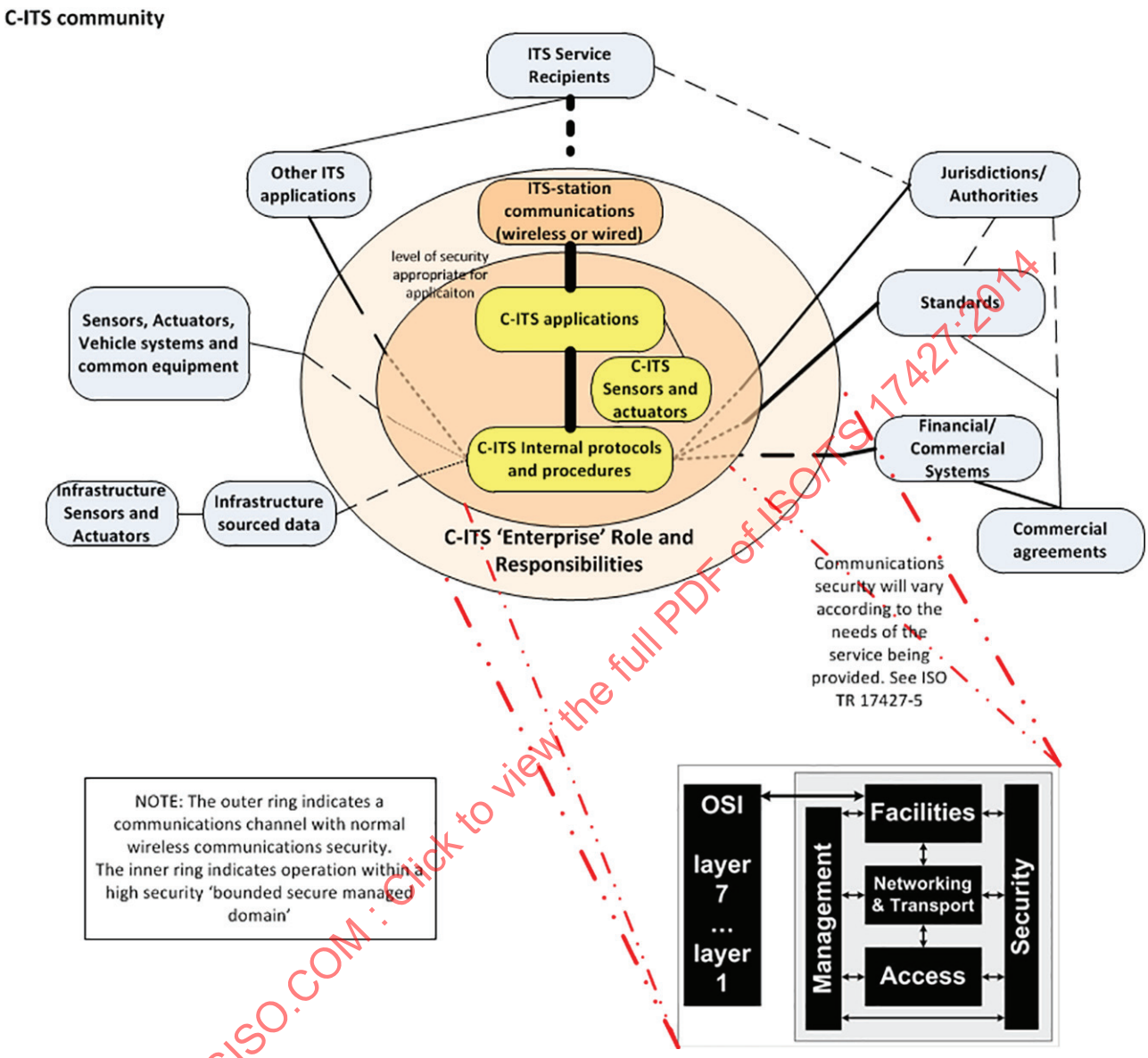

Figure 2 — External and Internal Enterprise Objects in a C-ITS Community

From the *enterprise objects* (3.5) displayed in Figure 2, the following are closely connected with C-ITS and rather have an external-internal status:

— Telecommunication systems;

— Certification;

— Standardization bodies;

— Authorities.

Criteria for the categorization of "external-internal" is that the *external enterprise objects* (3.8) are deeply involved in C-ITS and partially exhibit C-ITS specific *roles* (3.20). More details are given in Clause 6. The standard functionalities that *external enterprise objects* (3.8) provide are documented in the respective standards referenced in Clause 6.

Additionally, as shown in Figure 2, C-ITS has interfaces with other ITS systems. These are not explicitly denominated in this Technical Specification.

5.2.1 Internal Enterprise Objects

C-ITS, as *internal enterprise object* (3.9), consists of a set of specific *roles* (3.20) that are identified and described in the subsequent Clauses. The methodology that describes how these roles and responsibilities originally were identified and verified can be found in Annex A.

6 Roles and responsibilities

6.1 Introduction

All *roles* (3.20) and the corresponding *responsibilities* (3.18) identified through use of the methodology described in Annex A are described in the following subclauses.

6.1.1 Generic description of organizational architecture

In the generic view of the organizational architecture four major *roles* (3.20) were identified (Figure 3):

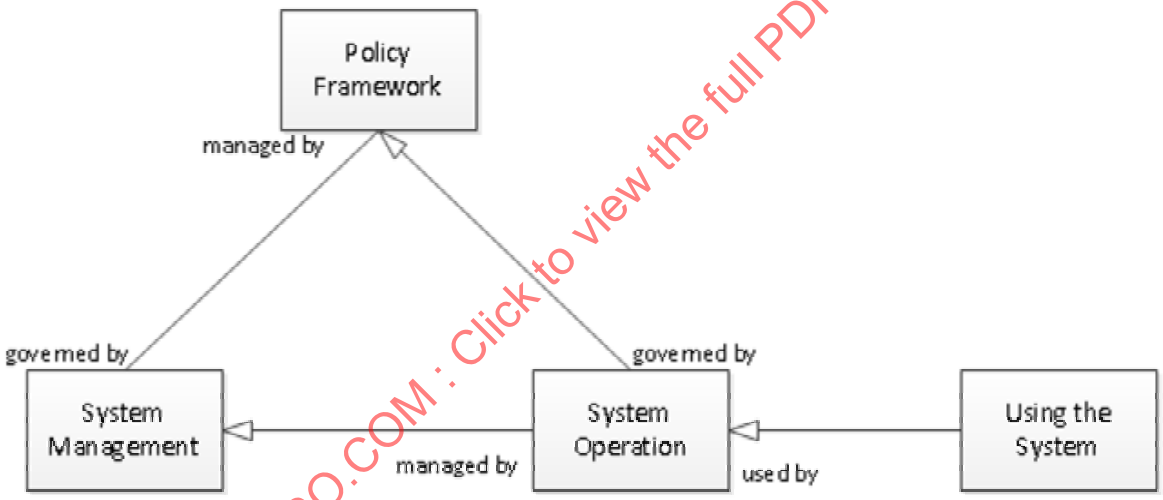

Figure 3 — Global description of Organisational Architecture

6.1.2 System operation

The *role* (3.20) "'System operation" is responsible for the proper execution of the *applications* (3.3) that provide an end-to-end *ITS service*(s) (3.23). This includes reliability for the coordination, organization and execution of the whole *process* (3.14) from initial data collection to the presentation of the final service result. One of the major interfaces of this *role* (3.20) is with the *actor*(s) (3.2) of the *role* (3.20) "Using the service" who receive(s) the service result.

Relationships with other *roles* (3.20):

The *role* (3.20) "System operation" is connected with the *role* (3.20) "System management". In this relationship, denominated with the term "managed by" in Figure 3, the *actor*(s) (3.2) with the *role* (3.20) "System management" provide supporting functionalities to the *actor*(s) (3.2) with the *role* (3.20) "System operation". This mainly includes functionalities enabling and facilitating the "System management" *behaviour* (3.4) and *responsibilities* (3.18).

The *role* (3.20) "System operation" is connected with the *role* (3.20) "Policy framework". In this relationship, denominated with the term "governed by" in Figure 3, the *actor*(s) (3.2) with the *role* "Policy framework" provide policies and regulations as well as their enforcement to the *actor*(s) (3.2) with the *role* (3.20) "System operation".

The *role* (3.20) "System operation" is connected with the *role* (3.20) "Using the system". In this relationship, denominated with the term "used by" in Figure 3, the *actor*(s) (3.2) with the *role* (3.20) "System operation" provide the achieved results to the *actor*(s) (3.20) with the *role* (3.20) "Using the system". The *role* (3.20) "Using the system" make(s) use of these results.

6.1.3 Using the system

The *role* (3.20) "Using the system" is responsible to perform an appropriate reaction to the service result received from the *actors* (3.20) with *role* (3.20) "System operation". The *role* (3.20) "Using the system" might stimulate the *role* (3.20) "System operation" (trigger an *ITS service* (3.23)).

6.1.4 System management

The *role* (3.20) "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* (3.20):

The *role* (3.20) "System management" is connected with the *role* (3.20) "Policy framework", in this relationship, denominated with the term "managed by" in Figure 3, the *actor(s)* (3.2) with *role* (3.20) "System management" provide supporting functionalities to the *actor(s)* (3.2) with the *role* (3.20) "Policy framework". This mainly includes functionalities enabling and facilitating the "Policy Framework" *behaviour* (3.4) and *responsibilities* (3.18). Additionally the *actor(s)* (3.2) with the *role* (3.20) "Policy framework" provide(s) policies and regulations as well as their enforcement to the *actor(s)* (3.2) with the *role* (3.20) "System management". This is denominated with the term "governed by" in Figure 3.

6.1.5 Policy framework

The *role* (3.20) "Policy framework" is responsible for all governing and institutional activities required in the system.

Relationship with other *Roles* (3.20):

See above ("System operation", "System management"). Relationships of role (3.20) "Policy Framework" with role (3.20) "System Operation" and role (3.20) "System Management" have already been given in subclauses 6.2.1 and 6.2.3.

The three main *roles* (3.20) "System operation", "System management" and "Policy framework" are detailed with *sub-roles*. Those are described in the following subclauses. The *role* (3.20) "Using the service" is not further detailed, a more detailed description of its *responsibilities* is appended.

6.2 General responsibilities of actors involved in C-ITS

6.2.1 Registration and authorization

Prior to the use of the system each *role* (3.20) and, therefore each *actor* (3.2), 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 (compare with sign-up):

  — issue request for registration to the system,

- receive certificates for registered ITS Stations.

- Authorization – defined as authorization prior to every system usage (comparable to sign-in):
  - 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 base on the standard registration and authorization mechanisms defined in ISO 14817.

6.2.2 Privacy and Data Protection

The definition of C-ITS, as stated in ISO 17465, mentions two core characteristics of C-ITS: (a) The distributed implementation of *ITS services* (3.23), which requires a huge number of data and information exchanges between *ITS Stations* (3.12) to realize the respective end-to-end *ITS service* (3.23) and, (b) The sharing of data and information between *ITS Stations* (3.12) 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 Technical Specification. It will be one of the major tasks of the *actors* (3.2) that claim one of the *roles* (3.20) defined in this Technical Specification to respect the *responsibilities* (3.18) 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 that is moving e.g. mobile device. Therefore this content is subject to strict privacy and data protection Regulations and the *roles* (3.20) collecting or handling this content have to respect the corresponding regulations.

Each *role* (3.20) and, therefore each *actor* (3.2), is responsible to respect both ISO/TR 12859 and national regulations and laws on privacy and data protection when participating in C-ITS.

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

- Collection of data/information (content): each *actor* (3.2) collecting data/information (including the hand-over of data/information from other parties) handles this data/information with care and respect the originators privacy based on the principles outlined in ISO/TR 12859;
- Processing of data/information (content): each *actor* (3.2) processing data/information handles this data/information with care and complies with the principles outlined in ISO/TR 12859;
  - Deletion of data/information (content) after usage: each *actor* (3.2) handling data/information ensures the proper deletion of data/information after usage based on the principles outlined in ISO/TR 12859;
  - Transmission of data/information (content): each *actor* (3.2) providing an *ITS service* (3.23) that transmits data/information complies with the principles outlined in ISO/TR 12859.

Any *role* (3.20) described in the following Clauses is, in a way, in touch with data/information collected or used in C-ITS and, therefore, needs to comply with these requirements.

6.3 Role: System operation

6.3.1 General description

The *role* (3.20) “System operation” is responsible for all activities related to the operation of the system. The *responsibilities* reflect the *process chain* of the corresponding *services*.

The *role* (3.20) "System operation" is composed of the *sub-roles* (3.21) content provision, service provision and presentation provision. The mentioned *sub-roles* share the *responsibilities* (3.18) of the *role* (3.20) "System operation". The *role* (3.20) "System operation" itself bundles all *responsibilities* (3.18) of the *sub-roles* (3.21).

6.3.2 Sub-role: Content provision

The *sub-role* (3.21) "Content provision" 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* (3.21) shall be responsible for the registration of itself as a content provider and the content that is provided:

— subscribe content provision activity,

— cancel content provision activity,

— registration of content (data/information),

— cancel/deregistration of content (data/information).

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

The *responsibilities* (3.18) associated with this *sub-role* (3.21) that have a tight relation to the "Service provision" itself are:

— receive content request,

— obtain content (data/information),

— provide content (data/information).

Additionally the role 'Content Provision' is responsible for ensuring data integrity.

6.3.3 Sub-role: Service provision

The *sub-role* (3.21) "Service provision" shall connect the *sub-role* (3.21) "Content provision" with the *sub-role* (3.21) "Presentation provision".

The *sub-role* (3.21) "Service provision" identifies which algorithm is suitable to fulfil the end-to-end *ITS service* (3.23), it determines the content that is required to run the *ITS service* (3.23), afterwards runs the *ITS service* (3.23) and provides a suitable service response. The content required to run the *ITS service* (3.23) is requested and received from the *sub-role* (3.21) "Content provision". The service results shall be delivered to the *sub-role* (3.21) "Presentation provision".

Prior to the provision of the *ITS service* (3.23), the registration of the *ITS service* (3.23) with the *role* (3.20) "Service catalogue management" shall be required. The *sub-role* (3.21) "Service provision" shall be responsible for the activities:

— subscribe new *ITS service* (3.23),

— cancel/deregistration of *ITS service* (3.23).

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

The *responsibilities* (3.18) related to the *sub-role* (3.21) "Service provision" that have a tight link to the execution of the service itself are:

— receive service request,

— select *ITS service* (3.23)/ *application* (3.3)/algorithm,

— operate *ITS service* (3.23)/ *application* (3.3)/ algorithm (service generation),

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

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

— provision of service (result).

6.3.4 Sub-role: Presentation provision

The *sub-role* (3.21) "Presentation provision" shall be responsible for the suitable presentation of the service results. This includes the scheduling of presentations, the prioritization of information to be presented and the selection of the presentation mode (visual, auditory, tactile).

Responsibilities (3.18) tied to the *sub-role* (3.21) are:

— receive service results,

— scheduling of presentations,

— prioritization of service results,

— selection of presentation mode,

— conformance of presentation with regulation(s).

6.4 Role: Using the service

The *role* (3.20) "Using the service" incorporates the triggering of *ITS services* (3.23) available within the system. The entity occupying the *role* therefore issues service requests and receives service responses.

The *responsibilities* (3.18) related to the *role* (3.20) "Using the service" 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.

6.5 Role: System management

The *role* (3.20) "system management" is responsible for all management activities in the system. It supports both "System operation" and "Policy framework".

The *sub-roles* (3.21) of the *role* (3.20) "system management" are derived from the ones defined in ITIL V3 (Information Technology Infrastructure Library).[17] Not all *roles* (3.20) 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* (3.20) were merged and renamed.

Despite the revision and adaptation of the ITIL V3 *roles* (3.20) the remaining *roles* (3.20) can partially be grouped. This is announced in the text accompanying the following descriptions.

System management is a distributed role (multiple entities).

6.5.1 Sub-role: Service catalogue manager

This *sub-role* (3.21) shall be responsible for up-to-date maintaining of the service catalogue that lists all registered *ITS services* (3.23) and their status. This includes:

— add new *ITS service* (3.23) to the service catalogue,

— remove *ITS service* (3.23) that are unsubscribed from the service catalogue.

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

6.5.2 Sub-role: Communication manager

This *sub-role* (3.21) shall be responsible for enabling the communication among *ITS Stations* (3.12). This may includes:

— Station internal communication management (ISO 24102-1),

— Station remote communication management (ISO 24102-2),

— Inter-station communication management.

6.5.3 Sub-role: Service owner

This *sub-role* (3.21) shall be responsible for designing and delivering a particular C-ITS end-to-end *ITS service* (3.23) within the agreed service levels. Service ownership shall as well occur on a per process step (content provision, service provision, presentation provision) level.

6.5.4 Sub-role: C-ITS architect

This *sub-role* (3.21) shall be responsible for maintaining the implemented C-ITS Architecture, including architecture viewpoints.

6.5.5 Sub-role: Project manager

This *sub-role* (3.21) shall be responsible for planning and coordinating the resources (including software, hardware) to deploy, operate and maintain C-ITS.

6.5.6 Sub-role: Test manager

This *sub-role* (3.21) shall ensures that deployed *ITS services* (3.23) fulfil their specification.

6.5.7 Sub-roles for preparation, operation and maintenance of service environment

The following *sub-roles* (3.21) all focus on the preparation, operation and maintenance of the service environment.

6.5.8 Sub-role: Service level manager

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

6.5.9 Sub-role: Risk manager

This *sub-role* (3.21) shall be responsible for identifying, assessing and controlling risks.

6.5.10 Sub-role: Capacity manager

This *sub-role* shall be responsible for ensuring that *ITS services* (3.23) and *infrastructure* (3.11) are able to deliver the agreed capacity and performance targets.

6.5.11 Sub-role: Availability manager

This *sub-role* (3.21) shall be responsible for defining, analysing, planning, measuring and improving all aspects of the availability of the C-ITS system.

6.5.12 Sub-roles for IT-security

The following *sub-roles* (3.21) focus on IT security including access control

6.5.12.1 Sub-role: Information security manager'

This *sub-role* (3.21) shall be responsible for ensuring the confidentiality, integrity and availability of the system, data, information, C-ITS *services* and the user.

6.5.12.2 Sub-role: Access manager

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

6.5.13 Sub-roles for system maintenance and update

The following *sub-roles* (3.21) focus on system maintenance and update

6.5.13.1 Sub-role: Technical analyst

This *sub-role* (3.21) is a Technical Management *role* (3.20) which provides technical expertise and support for the management of the C-ITS infrastructure.

6.5.13.2 Sub-role: Change manager

This *sub-role* (3.21) shall be responsible for all change activities including collection of change requests, handling of change requests and application of changes.

6.5.13.3 Sub-role: Configuration manager

This *sub-role* (3.21) shall be responsible for maintaining information about *infrastructure* (3.11)/ equipment/hardware required to deliver C-ITS *services*.

6.5.13.4 Sub-role: Homologation manager

This *sub-role* (3.21) shall be responsible for product certification, test or authorization prior to deployment.

6.5.13.5 Sub-role: System monitoring

This *sub-role* (3.21) shall be responsible for monitoring the system state.

6.5.13.6 Sub-role: Financial Manager

This *sub-role* (3.21) is optional depending on the type of *ITS service* (3.23) (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* (3.23).

6.6 Role: Policy framework

6.6.1 General description

The *role* (3.20) "Policy framework" shall be responsible for all governing and institutional activities in the system and governs the management and system operational activities.

6.6.2 Sub-role: Compliance manager

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

6.6.3 Sub-role: Policy institution

This *sub-role* (3.21) shall be responsible for the definition of regulatory and non-regulatory policies (e.g. agreements between *stakeholder*s (3.26), regulations) regarding the design, implementation, deployment or operation of C-ITS.

6.6.4 Sub-roles: Miscellaneous

Other *sub-role*s (3.21) that are defined in the corresponding documents are listed in the following subclauses.

6.6.4.1 Sub-role: Standardization organization

Standardization is defined as an activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context.[8] Details can be found in ISO/IEC Guide 2.

6.6.4.2 Sub-role: Security certificate body

Description can be found in TR 11176,[10] TR 11769,[11], ISO 24100[12] and IEEE 1609.2 –2006.[13]

6.6.4.3 Sub-role: Legislation, jurisdiction

Description can be found in national regulations.

6.7 Profiles

A profile provides a set of one or more base assignment of *role*s (3.20) and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base *role*s (3.20) (or in the case of ITS systems, standards or otherwise defined systems), necessary to accomplish a particular function/*service* with its characteristics.

The different profiles demonstrate key characteristics of an organisational architecture:

— one *role* (3.20) can be assigned to multiple *actor*s,

— one *actor* can occupy multiple *role*s (3.20).

7 Compliance

It is recommended that any implementation of an organizational architecture for C-ITS should comply with this Technical Specification. Compliance with this Technical Specification is achieved when all *role*s (3.20) and *sub-role*s (3.21) described in Clause 6 are assigned to corresponding *actor*s in C-ITS.

Annex A
(informative)

Methodology and its sample application

A.1 Methodology to identify cooperative ITS roles, behaviour and responsibilities

A.1.1 Introduction

To identify the "Roles and responsibilities in the context of cooperative ITS based on architecture(s) for cooperative systems" an abstract methodology is defined. This methodology can be applied to any C-ITS *service*. It starts from the identification of the *ITS service* (3.23) specific *stakeholders* (3.26) and *actors* (3.2), identifies their *behaviour* (3.3) and *responsibilities* (3.18) with the support of an abstract *process* description of the service operation and finally transforms the results into a basic organisational model for this *ITS service* (3.23).

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 *scenarios* (3.22) of *ITS service* (3.23).

Stakeholders (3.26) are not necessarily active participants in C-ITS i.e. they only have an occasional interest in the deployment and/or operation of C-ITS itself. Hence the group of *stakeholders* (3.26) incorporates the following entities:

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

— interest groups (e.g. user),

— lobby groups (e.g. industry),

— industry associations.

A.1.2.1 Actors

C-ITS can be implemented in various *scenarios* (3.22) with the participation of different *actors* (3.2). A structure was developed to clearly arrange the different *actors* (3.2). On the first level, the structuring elements are the C-ITS components to which the behaviour of the *actors* (3.2) can be assigned to, more precisely:

— the hardware platform (sensors, actuators, others) that is required to execute the *ITS service* (3.23), (both mobile and static),

— the software running on this hardware platform to provide the *ITS service* (3.23).

The *actors* (3.2) in these fields are further subdivided into those responsible for:

— operation,

— system management functionalities like maintenance and installation/disassembly,

— policy framework functionalities like agreement on frameworks.

EXAMPLE There will be an *actor* (3.2) who has a *behaviour* (3.3) and *responsibilities* (3.18) tied to the operation of the hardware platform. Another one will maintain the software part.

The focus of this Technical Specification is the operation of C-ITS. Other fields are only considered if they include functionalities directly supporting system operation. This applies for the system management and policy framework part which support 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* (3.2).]

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 manufacturer
      — vehicle manufacturer
      — service provider
      — traffic manager
      — freight and fleet manager
      — police

   3) Policy framework

      — standardization organisations
      — certification organization
      — national / European judiciaries
      — consortium of *stakeholders* (3.26)/*actors* (3.2)

b) Software

   1) Operation

      — software provider
      — driver

- road operator

2) System management
   - software maintenance provider
   - software provider
   - vehicle manufacturer
   - infrastructure manufacturer
   - problem
   - manager
3) Policy framework
   - public key infrastructure / trusted third party
   - standardization organisations
   - consortium of *stakeholders* (3.26)/*actors* (3.2)

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. Starting point is the *ITS service* (3.23) for which the corresponding organizational structure shall be determined.

In principle any *ITS service* (3.23) is a set of different *applications* (3.3) working together to supply the service result to the user. Together, these *applications* (3.3) form a course of *actions* (3.1) that is characteristic for the specific *ITS service* (3.23), it is called a *process* (3.14). The approach that is described in this subclause differs between two different description perspectives: a) a *sequential process* (3.16) with its variations for services in *push* (3.24) and *pull mode* (3.25), and b) and, a *data lifecycle process* (3.17) which is the transformation result of the *sequential process* (3.16) 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* (3.16) 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* (3.23).

In general, there is discrimination between *ITS services* (3.23) *in push* (3.24) and *pull mode* (3.25). An *ITS service* (3.23) *in push mode* (3.24) consists of two independent *processes* (3.14) each describing the course of events of one or more *applications* (3.3):

- 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* (3.14) of the *ITS service* (3.23) that turns some input data (usually the one collected in the other *process* (3.14) into the service result by executing the service specific algorithm.

The intermediate storage/database links both independent *processes* (3.14) with each other. (Figure A.1)

The classification of an *ITS service* (3.23) as *service in push mode* (3.24) bases 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 both includes internal processes (own sensors), as well as, third parties delivering information with the support of a communication provider.

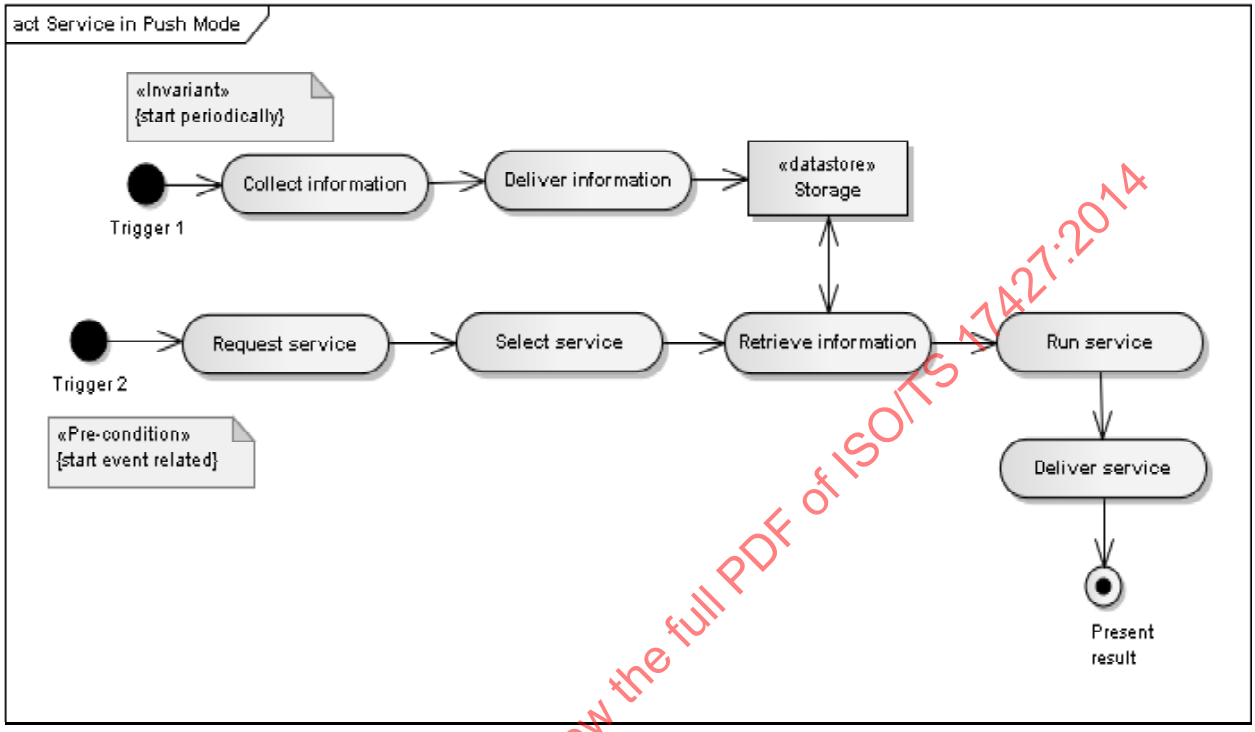

Figure A.1 — Abstract process description of a *service in push mode* (3.24)

A *service in pull mode* (3.25) explicitly requests the content that is required for the transformation in the service result. Compared with the *service in push mode* (3.24) this means that there is no constant, periodically triggered data collection and buffering. The required content is collected demand-oriented. (Figure A.2)

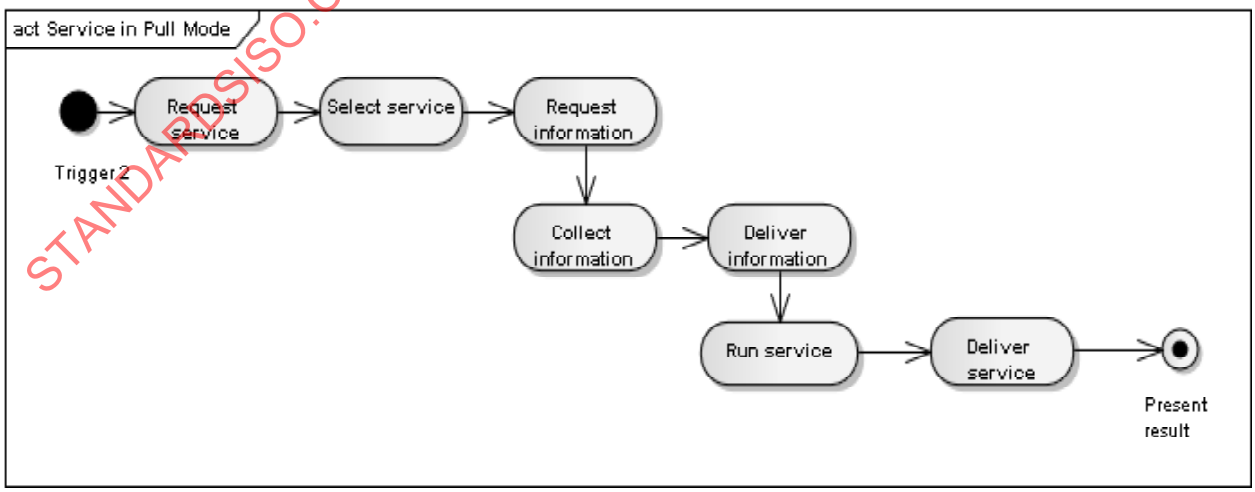

Figure A.2 — Abstract process description of a *service in pull mode* (3.25)

Both the *service in push* (3.24) and *pull mode* (3.25) use similar elements. To illustrate the parallelisms abstract activities and functionalities that may logically belong together are bundled into manageable modules. For different *services*, slight differences between the activities within a module are possible.

The general sequence of modules both for *services in push* (3.24) or *pull mode* (3.25) is stable. This is why it is named basic sequential *process* (3.16) description.

A.1.3.3 Modules

The differentiation of the various *services* 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* (3.23) algorithm.

The modules for both *services in push* (3.24) and *pull mode* (3.25) are similar in their general description. This general description can be found in Table A.1.

Table A.1 — Basic Modules

Start service	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 a *ITS service* (3.23), the *behaviour* (3.4) and *responsibilities* (3.18) that are part of the single modules are assigned to *ITS service* (3.23) specific *actors* (3.2). The single corresponding *actions* (3.1) relate to the later identified *roles* (3.20).

A.1.3.4 Lifecycle process description

The detailed basic *lifecycle process* (3.17) 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 info-service result. This is (optionally) transferred. (Grey shaded boxes: "Info-Service Delivery", "Info-Service Reception"). The receiver renders the received info-service result and finally presents it.

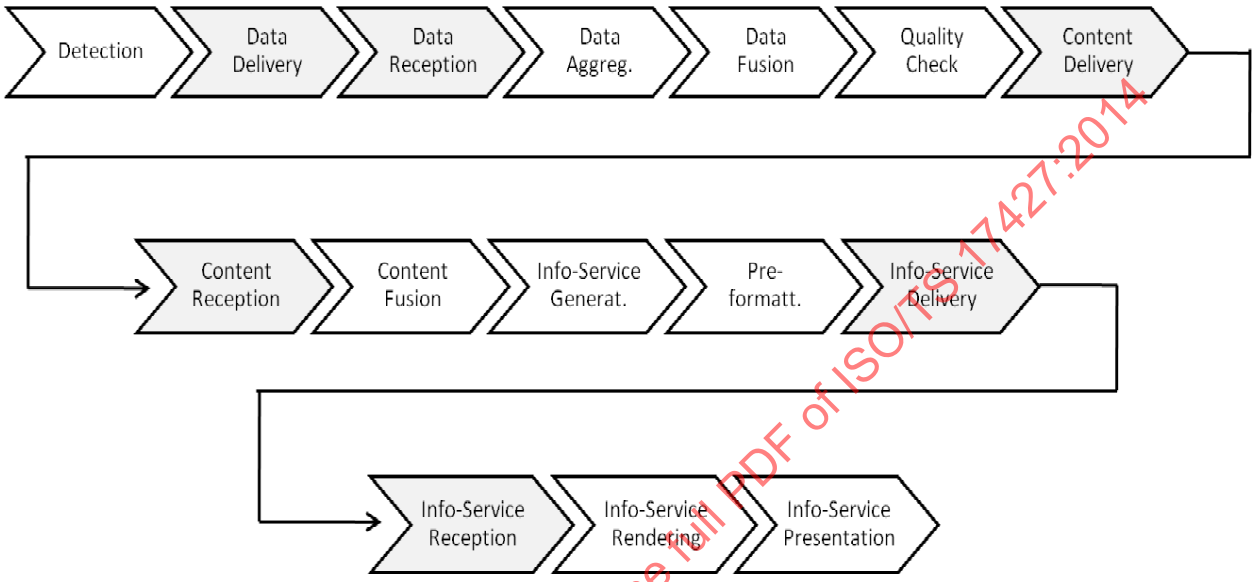

Figure A.3 — Detailed *lifecycle process* (3.17) description

This abstract basic *lifecycle process* (3.17) description is adapted from the TISA value chain for traffic information.[12]

A.1.3.5 Transformation of sequential to lifecycle process description

To facilitate the identification of the basic organisational model, the *sequential process* (3.16) description (Figure A.4) is transformed into a *lifecycle process* (3.17) description (Figure A.5). That means that the sequential time-dependent viewpoint on the *ITS service* (3.23) is changed to a data lifecycle-oriented viewpoint. This facilitates the transition to the basic organisational model.

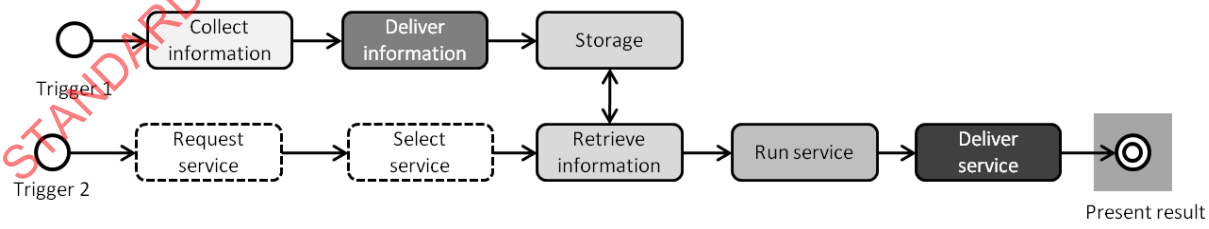

Figure A.4 — Transformation - *Sequential process* description

In the course of the transformation, information about the lifecycle of data elements that are central building blocks of the *ITS service* (3.23) is extracted from the *sequential process* (3.16) description. Different states of the raw data are tracked and the whole lifecycle is modelled. Basic underlying concept is the transition of a sensor detected event to a highly processed service result that is presented to the user through an actuator.

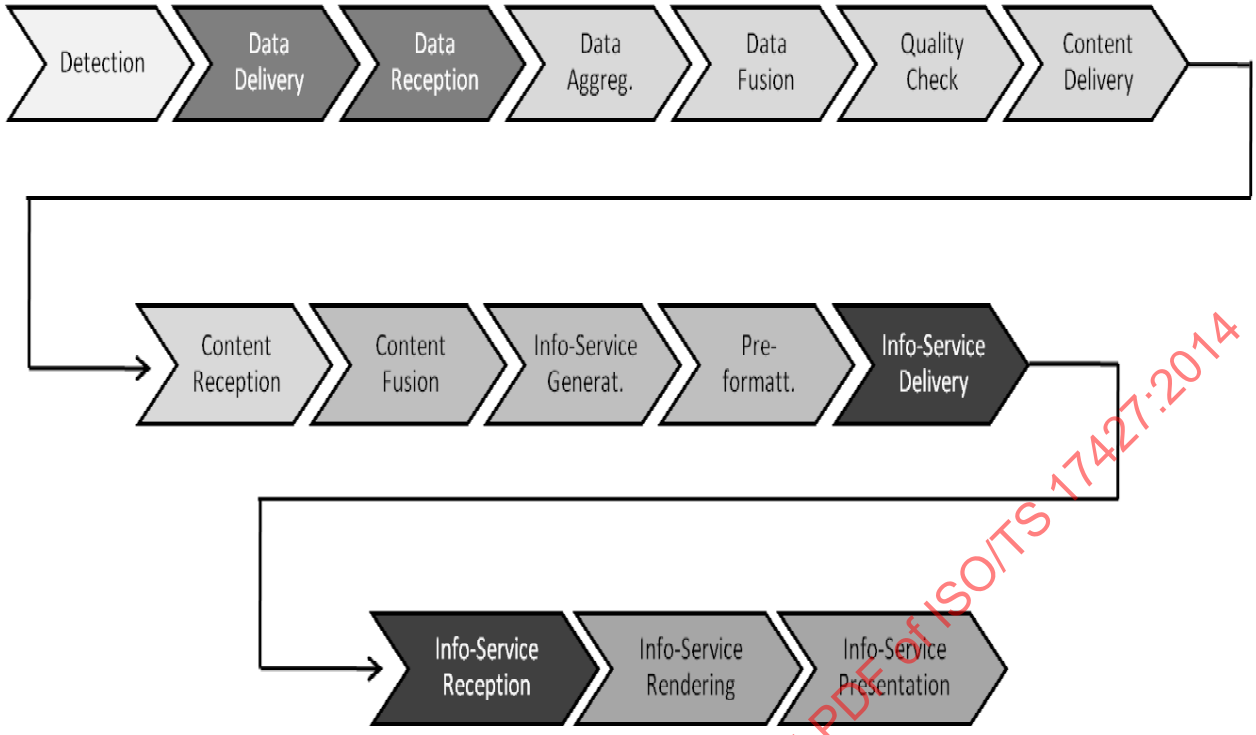

Figure A.5 — Transformation - *Lifecycle process* (3.17) description

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, info-service presentation.

The transformation itself is independent of the *push* (3.24) and *pull mode* (3.25) identified in the *sequential processes* (3.16) description, hence there will be only one *lifecycle process* (3.17) description.

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

Figure A.6 shows the process of simplifying the *lifecycle process* (3.17) description from Figure A.3 (detailed basic *lifecycle process* (3.17) description). In the general *lifecycle process* (3.17) description

— data/information transmission (data delivery, data reception, content delivery, content reception, service 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* (3.23):

  — detection,

  — content processing,

— info-service generation,

— info-service presentation.

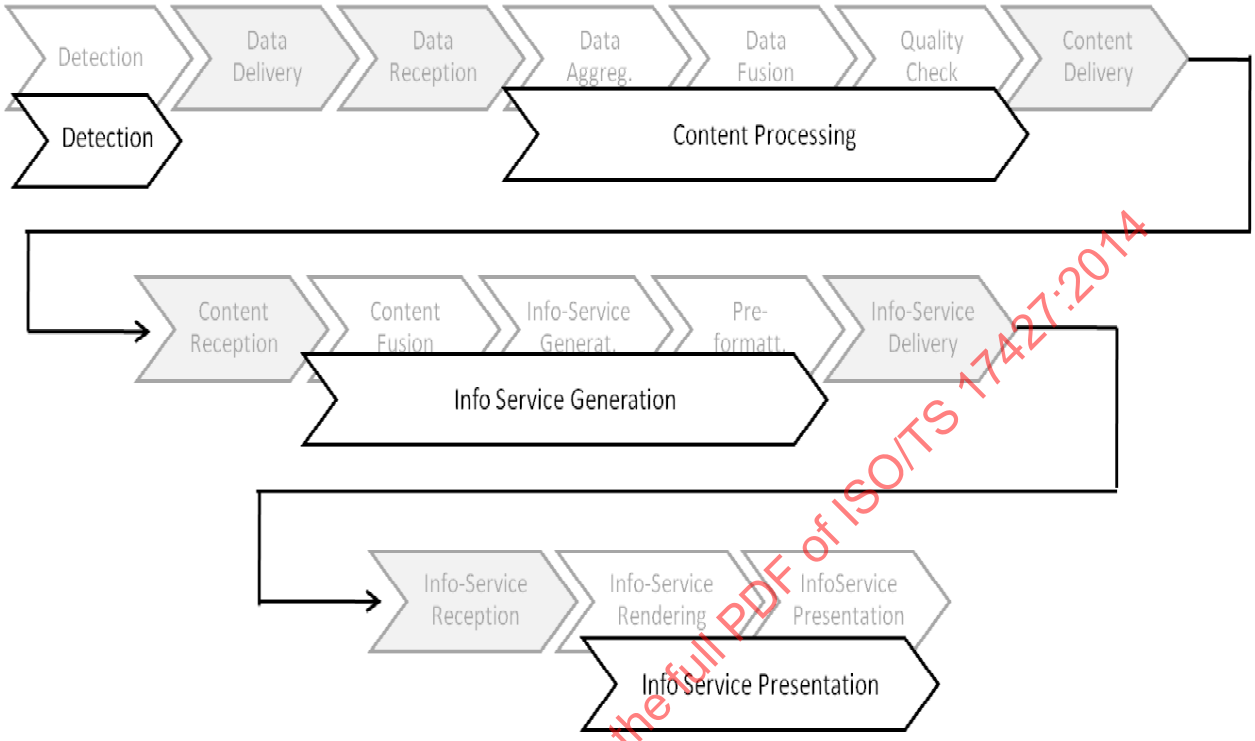

Figure A.6 — General *lifecycle process* (3.17) description

This general *process* (3.14) 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* with the *lifecycle process* (3.17) description and the identification of *actors* (3.2) active in the single *process* (3.14) steps allows developing a basic organisational model for the service operation.

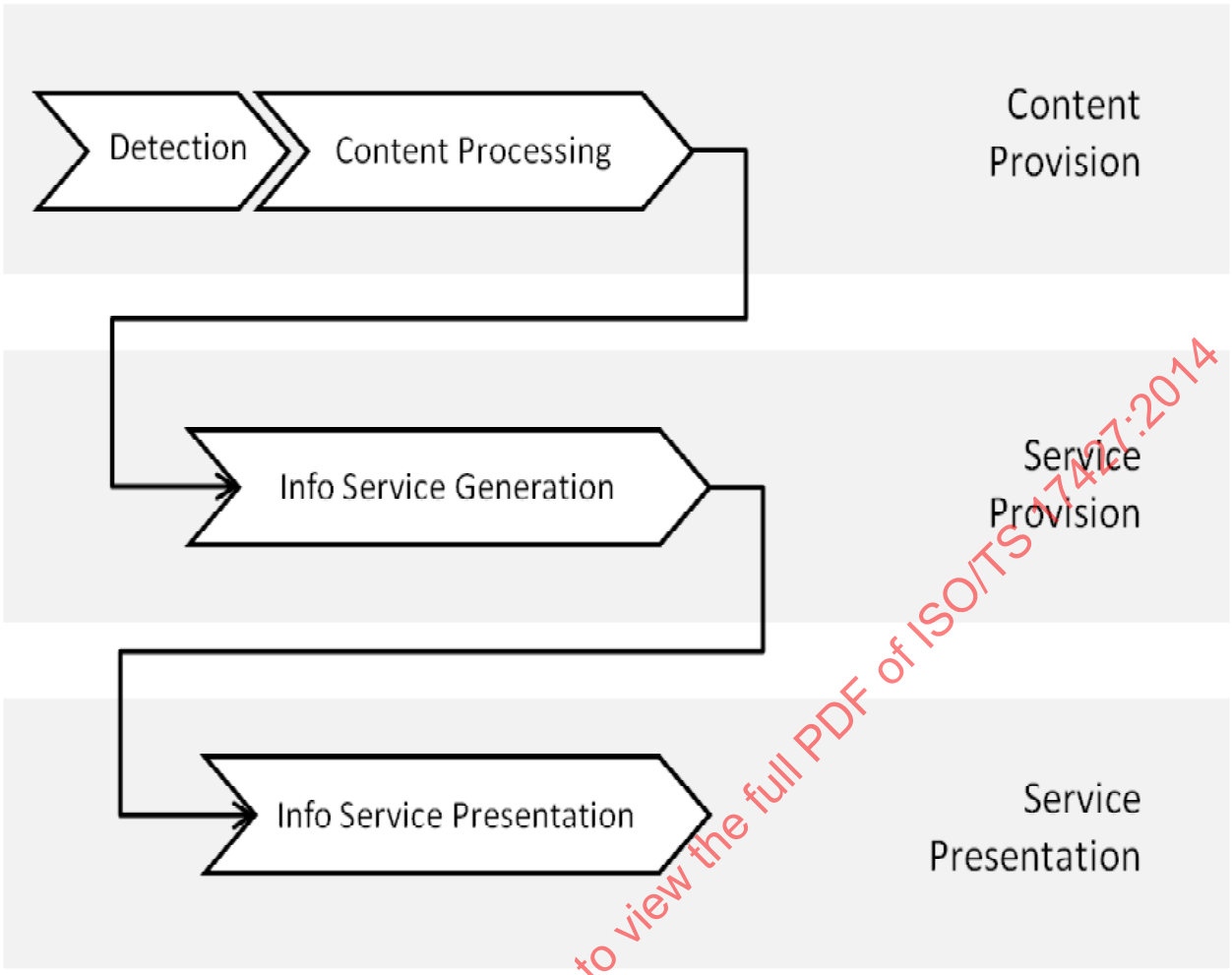

Figure A.7 — Identification of *roles* (3.20) - structuring the *ITS service* (3.23) *process chain*

Structuring the activities described in the *lifecycle process* (3.17) description leads to the three main *actions* (3.1) and *responsibilities* (3.18) (Figure A.7)

— Content provision,

— Service provision,

— Service presentation.

Central focus of the *role* (3.20) "content provision" is the collection of data from a sensor, aggregation of the data and delivery of the content to the *role service provision*. The *role* (3.20) *service provision* executes the *ITS service* (3.23) where an *ITS service* (3.23) can be both a more complex pre-processing of the content or a traffic safety relevant *ITS service* (3.23). The result is delivered to the *role* (3.20) *service presentation*. The *role* (3.20) *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* (3.20) are supported by a number of system management and policy framework *roles* (3.20). *Roles* (3.20) 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 Clause A.2 it is applied to hazard location warning as a sample *ITS service* (3.23).

The main purpose of the *ITS service* (3.23) "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 objects (oil, items).

A.2.2 Identification of stakeholders and actors

A.2.2.1 Stakeholders

Stakeholders (3.26) 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* (3.23) operation of "hazard location warning" are:

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

— *infrastructure* (3.11) – both public or private (including all or partially: sensor, wireless network access point (*ITS Station*), traffic control centre, display / variable message sign),

— in presence of *infrastructures* (3.11): A network provider/operator.

Additionally different *actors* (3.2) supporting the system operation are involved with system management and policy framework functionalities like various service providers, PKI/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* presumably includes a data provision in *push mode* (3.24). Therefore the *sequential process* (3.16) description includes two separate *processes* (3.14) 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* (3.14) steps

The triggering event is the hazardous location, e.g. a dangerous traffic situation, weather situation or dangerous object

Sensor detects the event (e.g. vehicle sensor, roadside sensor, weather sensor)

The collected data is provided through public or proprietary interfaces to the

Data storage. This could be for example the LDM implemented in an *ITS Station* (3.12). The data storage might fusion data from different sources, aggregate data, pre-process data, run a quality check.

The trigger of the main *process* (3.14) is a time-dependent signal periodically starting the service.

The entity triggering the main *process* (3.14) issues a service request.

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.

It is determined which data is required for the execution of the service hazard location warning and the corresponding data is retrieved from the Storage. Eventually there is another fusion of content including pre-processing of the content.

Now the hazard location warning service algorithm is executed. The retrieved content is processed by the info-service and a result is computed.

The service result from the previous module is delivered to the presenting *actor* (3.2).

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* (3.14) steps

A.2.3.2 Lifecycle process description

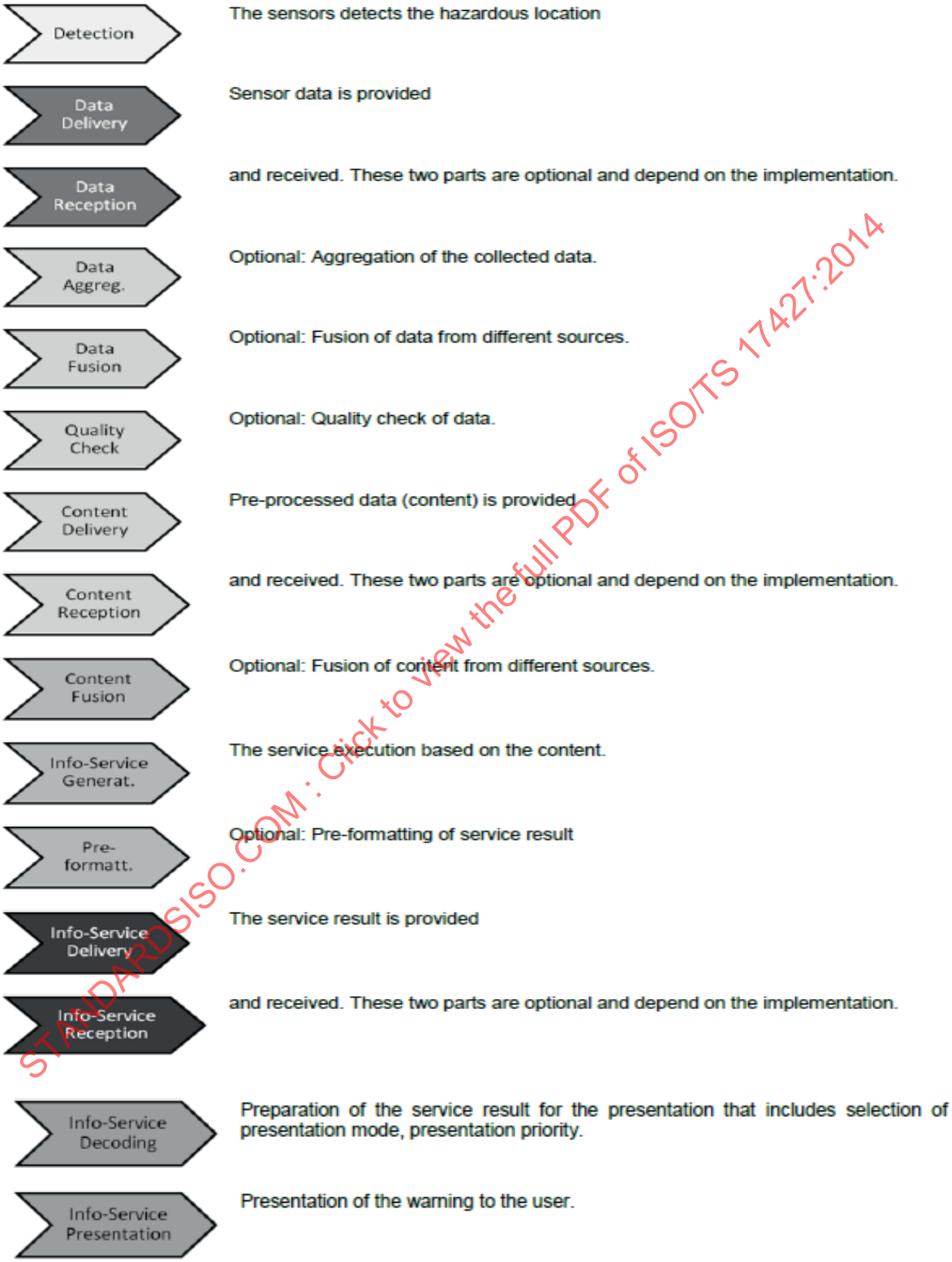

Figure A.9 — Lifecycle process description

A.2.4 Transformation of sequential to lifecycle process description

The hazard location warning service can be modelled both with the *sequential* and *lifecycle process* (3.17) description from subclauses B.1.2.1 and B.1.2.2. Therefore, a transformation like the one described in subclause 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* (3.17) description from subclause B.1.2.2. Therefore a transformation like it is described in subclause B.1.2.4 is possible.

A.2.6 Basic organisational model

The service hazard location warning complies with the abstract descriptions of *sequential* (3.16) and *lifecycle process* (3.17), the transition from the *lifecycle process* (3.17) description to the basic organisational model is as well 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* (3.20) regarding service operation:

— Content Provision: Responsible to provide data collection and data pre-processing,

— Service provision: Responsible to provide service generation,

— Presentation Provision: Responsible to provide presentation of service results.

Of course, the system operation is supported by system management and policy framework activities with the respective *roles* (3.20).

Annex B
(informative)

Profiles

B.1 Profiles

B.1.1 General description

This Clause includes different implementation *scenarios* (3.22) for the identified *roles* (3.20) and *responsibilities* (3.18).

An *ITS service* (3.23) might be implemented in multiple ways (*scenarios* (3.22)). So far, there is no decision which *scenario* (3.22) will be selected for the future real-world implementation of C-ITS. Furthermore, it is likely that different, interoperable *scenarios* (3.22) 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* (3.22) the *actors* (3.2) are generally grouped to "vehicle (system)" and "infrastructure (system)". Members of the "vehicle (system)" group include all vehicle related *actors* (3.2) including entities responsible for mobile device 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* (3.22) for the system operation part. As already identified in the Clauses 6, A.1 and A.2, each *scenario* (3.22) will consist of the basic processing stages dedicated to the *roles* (3.20) "Content provision", "Service provision" and "Presentation provision". Each of the *actor* (3.2) groups described in A.1.2 (vehicle system, infrastructure 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* (3.2) can be combined arbitrary. This results in the following possible combinations of different *actors* (3.2).

NOTE For reasons of simplification, the term vehicle system is abbreviated with vehicle and the term infrastructure system is abbreviated with infrastructure.

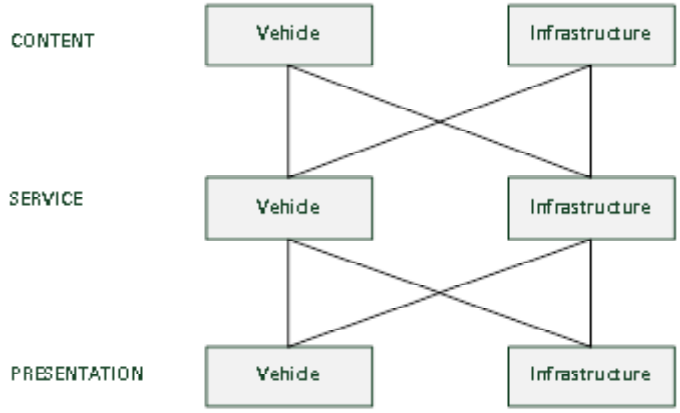

Figure B.1 — Possible *actor* (3.2) combinations for the description of *scenarios*

Those explicitly describing the single combinations of Figure B.1 result in the following basic *scenario* (3.22) combinations:

CONTENT	SERVICE	PRESENTATION	CONTENT	SERVICE	PRESENTATION
Vehicle	Vehicle	Vehicle	Infrastructure	Vehicle	Vehicle
Vehicle	Vehicle	Infrastructure	Infrastructure	Vehicle	Infrastructure
Vehicle	Infrastructure	Vehicle	Infrastructure	Infrastructure	Vehicle
Vehicle	Infrastructure	Infrastructure	Infrastructure	Infrastructure	Infrastructure

Figure B.2 — *Actor* (3.2) combinations for basic *scenarios*

Scenarios (3.22) involving either vehicle and/or infrastructure system *actors* (3.2) for a single processing stage but, not both vehicle and infrastructure (vehicle and infrastructure) system *actors* (3.2), are named basic *scenario* (3.22). The possible combinations are illustrated in Figure B.1 and Figure B.2. The remaining *scenarios* (3.22) are named complex *scenarios* (3.22) and are composed of two or more corresponding basic *scenario* (3.22) components.

In subclause B.1.2 the *service* implementation of an example *ITS service* (3.23) is modelled for all basic *scenarios* (3.22). Complex *scenarios* (3.22) are not modelled due to the high number of possible implementations. Though the *process* (3.14) for identifying potential complex *scenarios* (3.22) is described in subclause B.1.1.3.

B.1.1.3 Complex scenarios

The first variation that can be introduced by the combination of basic *scenarios* (3.22) affects the "Content provision" – "Service provision" transition. The data collected by the vehicle and infrastructure system can both be delivered to the vehicle or infrastructure system for processing (Figure B.3).

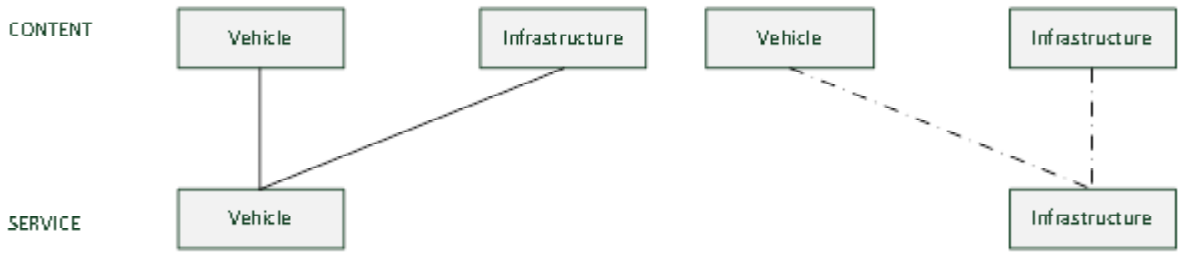

Figure B.3 — Delivery of data from multiple sources to a single recipient

As well, it is possible that the vehicle or the infrastructure system either deliver data both to the vehicle and the infrastructure system (Figure B.4).

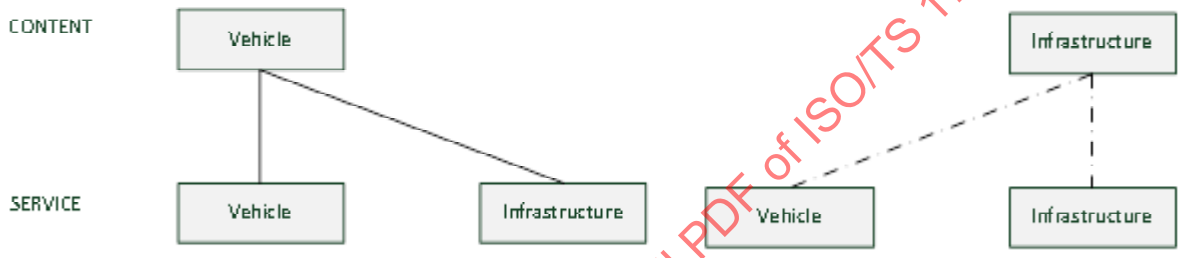

Figure B.4 — Delivery of data from a single source to multiple recipients

The second variation that can be introduced by the combination of basic *scenarios* (3.22) affects the 'Service provision' – 'Presentation Provision' transition.

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

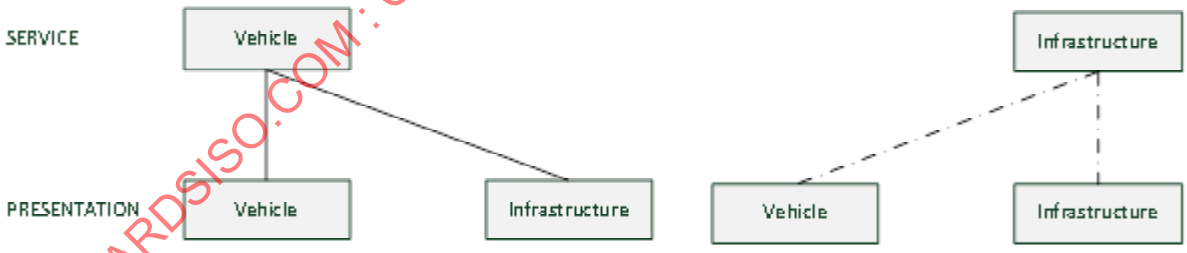

Figure B.5 — Delivery of a single service result to multiple recipients

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

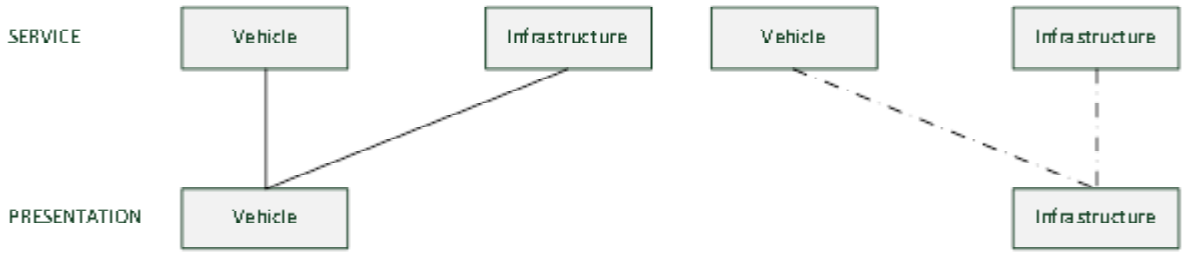

Figure B.6 — Delivery of multiple service results to a single recipient

The single descriptions can be combined to a large number of different *scenarios* (3.22).

B.1.1.4 Example of a complex scenario

As stated in subclause B.1.1.2 there is a large number of possible complex *scenarios* (3.22). The following example illustrates the principles of decomposition into basic *scenarios* (3.22) (Figure B.7).

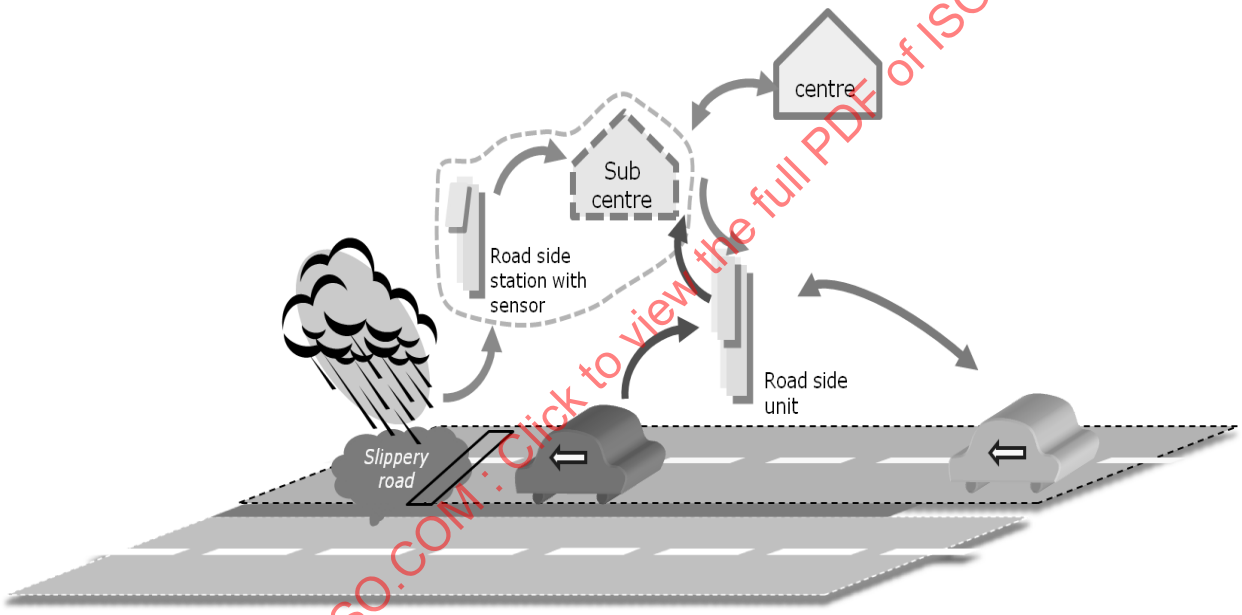

Figure B.7 — Complex *scenario* based on basic *scenarios*

Depending on the different assignment of the *roles* (3.20) to the *actor* (3.2) groups vehicle system and infrastructure system, different underlying basic *scenarios* (3.22) are identified.

Table B.1 — Alternative combination of basic *scenarios* (3.22) for complex *scenario* (3.22) illustrated in Figure B.7

Roles in System Operation				
Alternative	**Content Provision**	**Service provision**	**Presentation Provision**	**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* (3.2) groups assigned to the different *roles* (3.20) are listed. Already for a comparatively simple hybrid *scenario* (3.22), like the one illustrated in Figure B.7, four possible combinations of basic *scenarios* (3.22) exist depending on which *actor* (3.2) group is assigned to which *role* (3.20).

B.1.1.5 Supporting Actions – System management and policy framework

The *scenarios* (3.22) described in subclause B.1.2 focus on the description of the transposition of *roles* (3.20) to *actor* (3.2) groups for the system operation. Naturally every implementation *scenario* (3.22) additionally deals with system management and policy framework as eminent supporting *roles* (3.20). As the profiles (subclause B.1.2) primarily serve as an example and illustration of how the *roles* (3.20) and *responsibilities* (3.18) might be assigned to the different *actor* (3.2) 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 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 user.

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

B.1.2.2 Scenario 1

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

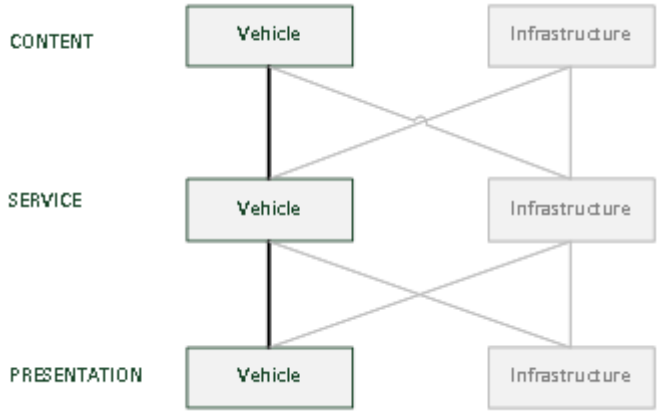

Figure B.8 — *Actor* groups (3.2) involved in Scenario 1

B.1.2.2.1 Figurative description

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

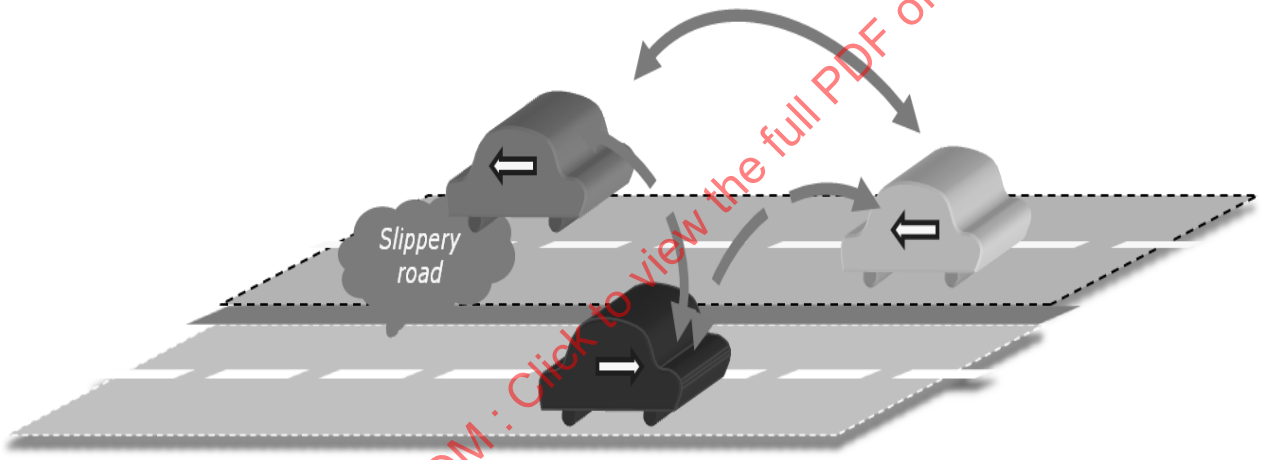

Figure B.9 — Figurative description of scenario 1 of service hazard location warning

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 *roles* (3.20) are assigned to *actors* (3.2) in the vehicle system (Figure B.10):

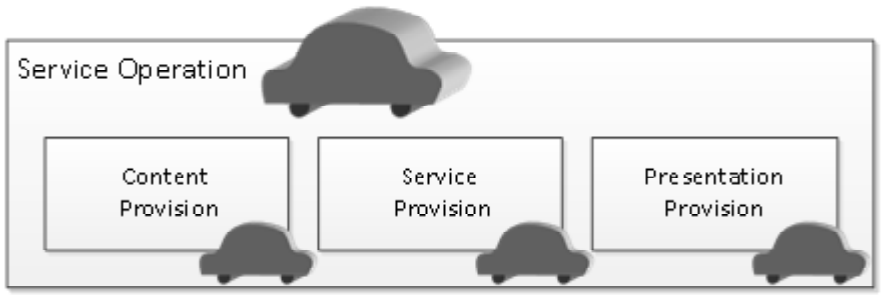

Figure B.10 — Assignment of *actor* groups in scenario 1

Service Operation: consortium — *Actor(s)* (3.2) from vehicle system – might be an organization or

Content Provision: *Actor(s)* (3.2) from vehicle system

Service provision: *Actor(s)* (3.2) from vehicle system

Presentation Provision: *Actor(s)* (3.2) 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):

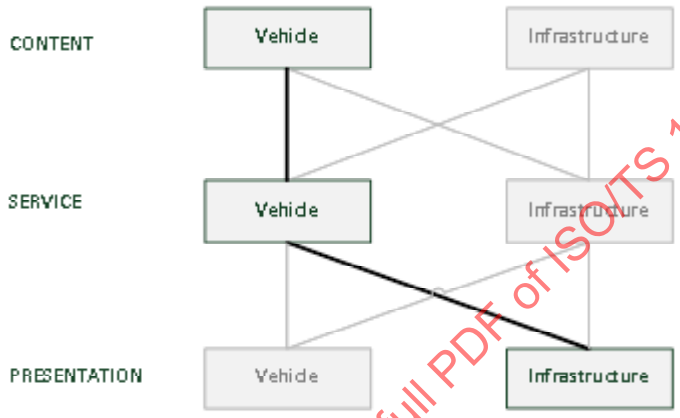

Figure B.11 — *Actor* (3.2) groups involved in scenario 2

B.1.2.3.1 Figurative description

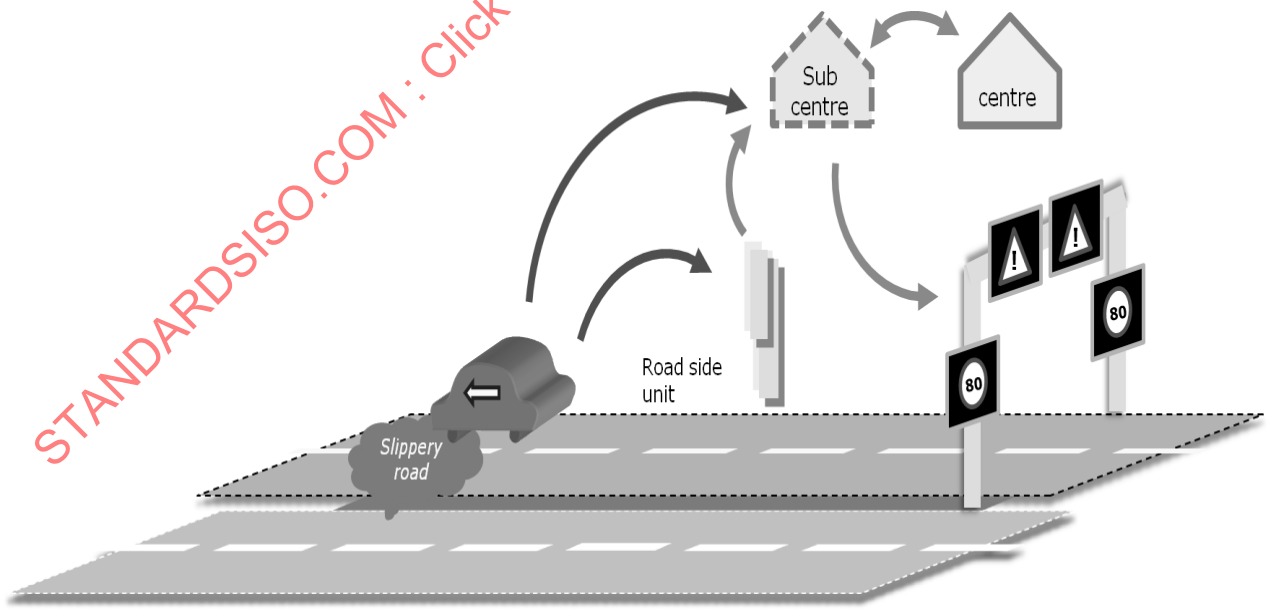

Figure B.12 — Figurative description of scenario 2 of service hazard location warning

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