INTERNATIONAL STANDARD

ISO 20077-2

First edition
2018-01

Road Vehicles — Extended vehicle (ExVe) methodology —

Part 2:
Methodology for designing the extended vehicle

Véhicules routiers — Méthodologie du véhicule étendu (ExVe) —

Partie 2: Méthodologie pour désigner le véhicule étendu

Reference number
ISO 20077-2:2018(E)

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 voluntary nature of standards, 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.

This document was prepared by Technical Committee is ISO/TC 22 *Road vehicles*, Subcommittee SC 31, *Data communication*.

A list of all parts in the ISO 20077 series can be found on the ISO website.

Introduction

This document is dedicated to the extended vehicle (ExVe).

In the early 2010s, advances in technology have led to new ways of communicating with the vehicle where digital information could be accessed not only in a physical way, but also wirelessly.

The removal of the constraint of a physical connection has enabled

— remote access to vehicle functionality that previously was impossible or very difficult, and

— simplified access to multiple information sources which have together created opportunities for new functionalities.

These advances have generated an increased need for interconnection with data specific to each vehicle. This phenomenon was similar to the increase of new functionalities enabled by the usage of multiplexed buses in vehicles.

This evolution has led to the introduction of the "extended vehicle" (ExVe) concept as described in ISO 20077-1.

Technical constraints and societal needs should be taken into account when designing these new functionalities. It is also necessary to mitigate the risks introduced by the new communication means between the ExVe and the external world.

In this context, this document aims at guiding the ExVe manufacturer by specifying a set of general rules and basic principles from which each ExVe manufacturer derives their own detailed and specific methods or procedures to design an extended vehicle.

Road Vehicles — Extended vehicle (ExVe) methodology —

Part 2:
Methodology for designing the extended vehicle

1 Scope

This document specifies general rules and basic principles the manufacturer of the extended vehicle (ExVe) considers when elaborating its own design method. It does not specify the manner in which these design methods are drafted and implemented.

It specifies by means of a template the necessary information that is communicated to the ExVe manufacturer for requesting the design of a new ExVe functionality. It also specifies, by means of a template, the information the ExVe manufacturer provides for responding to that request. It does not specify the process leading to the elaboration of the request information nor the process associated to communication of the response information.

It concerns the design of the extended vehicles mentioned in the scope of ISO 20077-1, regardless of the type of communication interface which is used between the ExVe and external systems or parties. It does not concern the internal communication of the ExVe. It does not standardize the implementation of software or hardware nor preclude any technical solution the ExVe manufacturer might select when designing a new ExVe functionality.

It relates to the design and production phases of a vehicle, where these phases include the subsequent design upgrades by the ExVe manufacturer of vehicle models, variants, or types still in production.

NOTE   Should new interfaces for remote communication with the vehicle become mandatory, then this document is also applicable for designing the requested ExVe functionalities.

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 20077-1, *Road vehicles — Extended vehicle (ExVe) — Methodology — Part 1: General information*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 20077-1 and the following apply.

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

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

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

3.1
basic principle
design principle that is considered when designing an extended vehicle

3.2
life cycle
various situations that the vehicle will encounter during its whole life including manufacture, customer's use, maintenance and recycling

3.3
local diagnostic facilitator
person at the vehicle that is in communication with the remote technician and facilitates the diagnostics by that person's capacity to act as requested by the remote technician and to answer the remote technician's questions

Note 1 to entry: Any person not able, at the minimum, to understand or describe the indications of the on-board instruments and tell-tales shall not be considered as local diagnostic facilitator.

3.4
operator
person at the vehicle who is operating, controlling or working on an extended vehicle

EXAMPLE   The local diagnostic facilitator.

3.5
requester
company or legal entity who is submitting to an ExVe manufacturer a request for a new ExVe functionality in the ExVe

Note 1 to entry: When submitting a request, a vehicle manufacturer acting as an after-sales service provider shall be considered as a requester.

Note 2 to entry: When the vehicle manufacturer is the same as the ExVe manufacturer, they may use their own internal processes.

3.6
rule
fundamental design requirement that is complied with when designing an extended vehicle

4   Abbreviated terms

BP   Basic Principle

ECU   Electronic Control Unit

ExVe   Extended Vehicle

LDF   Local Diagnostic Facilitator

NUM   rule or BP number

R   Rule

VER   Version of rule or BP number

VM   Vehicle Manufacturer

5   Conventions for identifying rules and basic principles and for specifying their content

In this document, rules and basic principles are formalized as follows:

XX_NUM	Text of the rule or basic principle
VER	

XX_NUM_VER: reference of the rule (R) or basic principle (BP) in which

— XX is a letter to identify rule (R) or basic principle (BP),

— NUM is an integer which allows the rule or basic principle to be distinguished. NUM is an integer between 001 to and including 999, and

— VER: Version of the XX_NUM. VER is an integer between 001 and including 999. Any new version shall have an integer greater than the previous version.

In this document, there can only be a single version (VER) for each rule or basic principle considered.

EXAMPLE 1

R_025_011 and R_026_011 are 2 different rules.

EXAMPLE 2

BP_025_010 and BP_025_030 are 2 versions of the same basic principle which cannot belong to the same version of the standard.

NOTE   Rules and basic principle can be followed by an explanatory text.

6   Overview of the design methodology of the extended vehicle

6.1   Role of the design methodology in the design process of an extended vehicle

The role of this methodology is to provide guidelines for the design of the extended vehicle and its interfaces (physical, documentation, support, etc.) by specifying a system of general requirements, including rules and basic principles, from which the ExVe manufacturer shall derive its own methods or procedures to design an extended vehicle that address a specific set of use-cases and scenarios.

It does not specify these methods and procedures, which remain part of the know-how of the ExVe manufacturer.

Each ExVe manufacturer has usually formalized the way of working in this design process through corporate methods and procedures as illustrated in Figure 1.
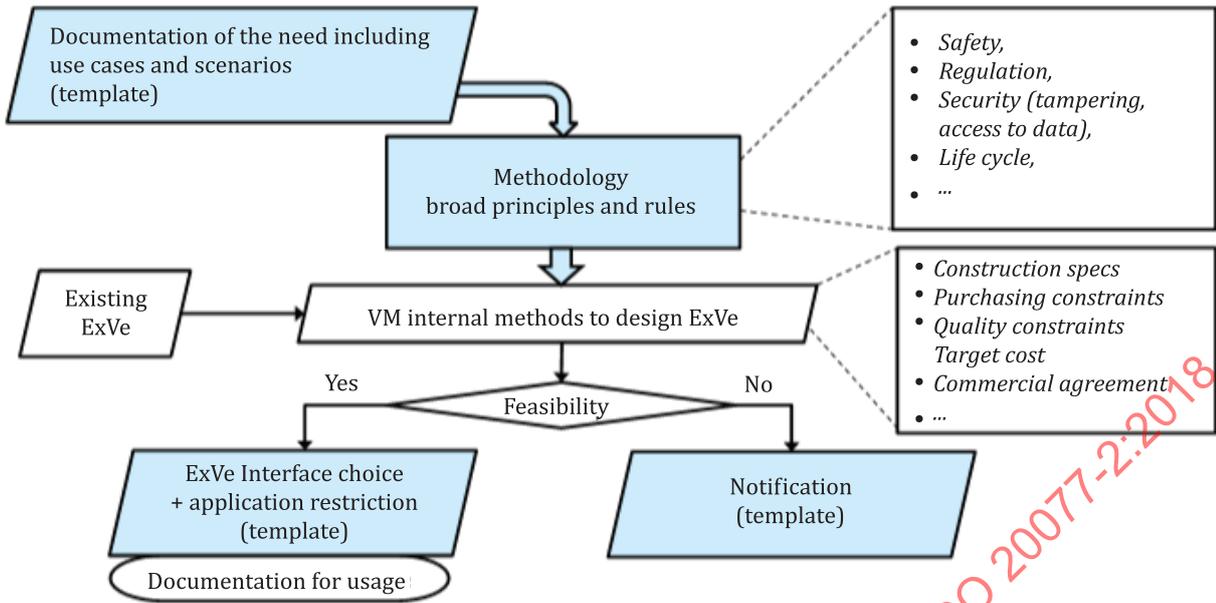
NOTE   Blue areas in this figure are within the scope of this document.

Figure 1 — Schematic of the ExVe design methodology context

6.2   The ExVe design methodology content

The ExVe design methodology contains (see Figure 2)

— a standardised template for providing the minimum information needed for a complete description of the new requested ExVe functionality (see 9.2),

— a generic system of rules and basic principles enabling the introduction of a new ExVe functionality (see Clauses 7 and 8), and

— a standardised template for providing the minimum information needed when responding to a request for an ExVe functionality (see 9.2).

Figure 2 illustrates this content in the case when the request and response information is provided by means of the templates specified in respectively Annexes A and B.
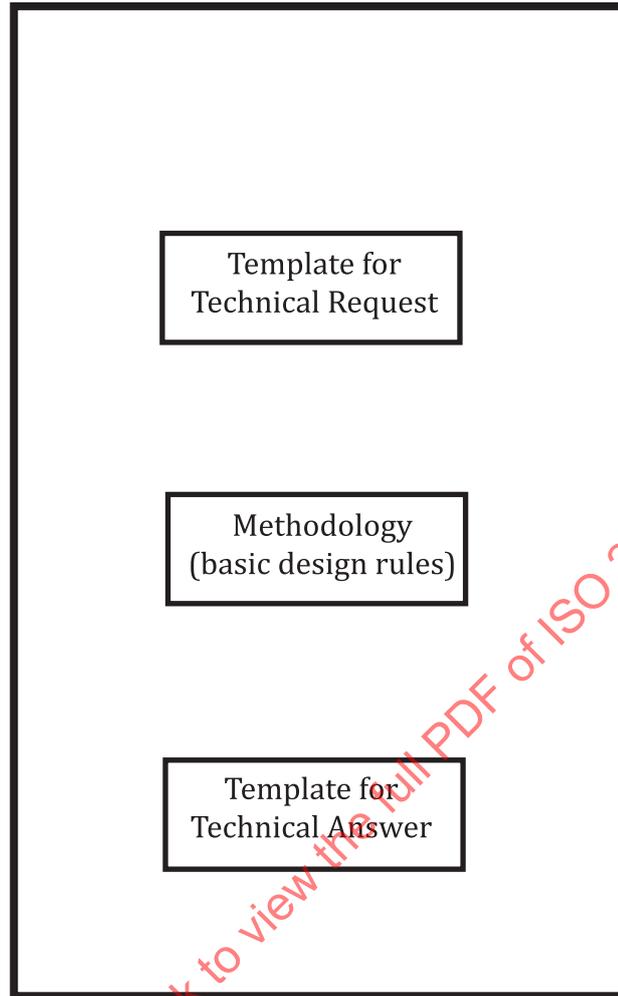
Figure 2 — Structure of this document

6.3 Consideration of new ExVe functionalities

The ExVe design methodology is applied by the ExVe manufacturer by considering the rules and basic principles of this document.

This applies during the design of or a design change to an extended vehicle involving direct or indirect communication between that vehicle and third parties, which may, for example, be the vehicle operator, the vehicle owner, service providers, or other ExVe's.

The need for new ExVe functionalities can result from legislation, standards or individual requests from requesters. In that case, the need for a new ExVe functionality shall be defined by the requester through the request template describing precisely all the required elements (e.g. performance related).

Designing specific new interfaces for remote communication with the vehicle may result from regulatory requirements. This methodology is also applicable in that case.

This methodology concerns any request from a requester for a new functionality of the ExVe. It also concerns the case when an existing functionality is requested to be extended or remotely available. It is applicable by all the involved manufacturers in the case of a multi-stage manufacturing.

Enabling new functionalities by just adding new equipment without taking the existing design into account may not give a satisfying result. On the one hand, new requested functionalities may uncontrollably interfere with functionalities which were installed in the initial or existing design. On the other hand, all the components required for these additional functionalities are not usually found in

the vehicle itself (e.g. diagnosis, voice recognition, manufacturing part-list). The basic principles of this methodology aims at highlighting the consideration of these risks.

The rules and basic principles specified in this document aim at considering, in a proper manner, the risks within the ExVe that are attributed to a new ExVe functionality, whether or not this functionality already exists. The consideration and management of these risks may lead to measures such as, but not limited to:

— modifying the electronic system (resources, etc.) of the existing ExVe in order to permit the new functionality;

— not implementing the new functionality;

— implementing the new functionality but only under specific conditions; and

— modifying other existing functionalities

Non-technical measures (e.g. contractual) may also be considered to manage the risks, for example, those related to obsolescence or disruption of existing functionalities or services.

The VM formally responds to the request according to the requirements specified in Clause 9.

7 ExVe design methodology — Rules

7.1 General

The ExVe design methodology is fundamentally based on the consideration of the following constraint:

— remote access shall preserve the basic safety and security of the vehicle during all its life-cycle phases.

Accordingly, this document includes the following 2 rules (R_01 to R_02) the ExVe manufacturer shall incorporate in its own design methods and procedures.

7.2 Safety related rule

R_001	When designing a new functionality in an extended vehicle, the ExVe manufacturer shall consider possible safety risks.
002	Functions which may impact safety shall be addressed according to the best safety practices.

The ExVe manufacturer is responsible for designing an ExVe in regard to the safety of the vehicle, its driver and passengers, its operators and other users during all phases of its life-cycle.

NOTE   For that purpose, some of the best safety practices can be found in existing standards (e.g. ISO 26262).

When designing a new functionality in an extended vehicle, the ExVe manufacturer shall therefore have design methods and procedures that integrate rule R_001.

When applying rule R_001, ExVe functionalities can be classified based on the following safety criterion:

— ExVe functionality which has no influence on the behaviour of the vehicle on the road like infotainment information/without any risk of disturbing the driver;

— ExVe functionality which has an impact on safety, either by interacting with the vehicle's behaviour (e.g. engine, brake, steering, suspension) or by distracting the driver's attention.

This classification is obtained either because the risk is internally given by the ExVe functionality, or because a risk is identified in a specific situation or in a specific operating function (the same action does not cause the same risks in each of the situations).

Examples of safety risks for moving vehicles:

EXAMPLE 1   Influence on the vehicle's braking capability.

EXAMPLE 2   Inappropriate functionality such as immobilisation of the vehicle while driving on the road.

EXAMPLE 3   Inappropriate functionality outside of specified parameters.

Examples of safety risks for stationary vehicles:

EXAMPLE 1   Inappropriate airbag deployment request when the front seat is occupied.

EXAMPLE 2   Inappropriate activation of high voltage components when high voltage battery decoupled.

EXAMPLE 3   Inappropriate activation of components during repair or maintenance activities.

7.3   Security related rule

R_002	When designing a new functionality in an extended vehicle, the ExVe manufacturer shall consider possible security risks.
002	Functions which may impact security shall be addressed according to the best security practices.

The ExVe manufacturer is responsible for designing an ExVe in order to preserve the security of the vehicle during all phases of its life-cycle.

When designing a new functionality in an extended vehicle, the ExVe manufacturer shall therefore have design methods and procedures that integrate rule R_002.

NOTE 1   Cyber-security is considered as included in this general security area.

NOTE 2   Uncontrolled communication of information can have security harmful consequences like theft of the vehicle or theft of the transported goods.

NOTE 3   When necessary, the extended vehicle can be secured (authentication of the requester, authentication integrity and confidentiality of data) in order to protect the extended vehicle from risks of tampering and unauthorized access.

NOTE 4   Some operational data could require confidential processing.

NOTE 5   Each data has an intrinsic confidentiality level. Association of data could lead to a confidentiality level far greater than the confidentiality of each data, considering possible uses.

NOTE 6   Security issues can lead to safety issues.

Examples of security risks:

EXAMPLE 1   Unauthorized coding of additional keys.

EXAMPLE 2   Unauthorized Remote ECU reprogramming.

EXAMPLE 3   Cloning of the vehicle connection interface.

EXAMPLE 4   Mismatched access.

8   ExVe Design Methodology — Basic principles

8.1   General

When addressing the basic principles in its own design methods and procedures, the ExVe manufacturer shall always fulfil the rules specified in this document.

8.2   General basic principles

BP_001	The ExVe manufacturer is responsible for the design of the extended vehicle.
002	

BP_002	The ExVe manufacturer is responsible for the design of all the interfaces of the extended vehicle that will permit communication with that extended vehicle.
002	

BP_003	The ExVe manufacturer is responsible for deciding on the implementation of any extended vehicle functionality.
002	

The ExVe manufacturer is responsible for the design of the Extended Vehicle, including its functionalities (see BP_001). Therefore, the ExVe manufacturer is responsible for both the implementation in the ExVe of each functionality and for the consistency of the whole set of functionalities.

When considering implementing a new functionality in an ExVe according to the methodology specified in this document, the ExVe manufacturer may conclude that the following restrictions apply:

— restrictions on the availability of the functionalities;

— restrictions on the performance of the functionalities;

— restrictions due to differences between vehicles, model, variants, or types; and

— restrictions due to unique market conditions.

8.3   Basic principles related to life-cycle (e.g. assembly, customer use)

BP_004	The ExVe manufacturer is responsible for assessing the impacts of a new ExVe functionality during the life-cycle phases of the ExVe.
002	

Usually, the requester expresses the availability and expected performance related to the requested ExVe functionality without any restriction with regard to the life-cycle phases of the extended vehicle when accessing data.

The ExVe manufacturer shall determine the impact of the integration of this functionality throughout the life cycle of the vehicle (see Figure 3) and therefore determine possible incompatibilities of the request considered in the situations not mentioned by the requester (e.g. manufacturing, maintenance, recycling).
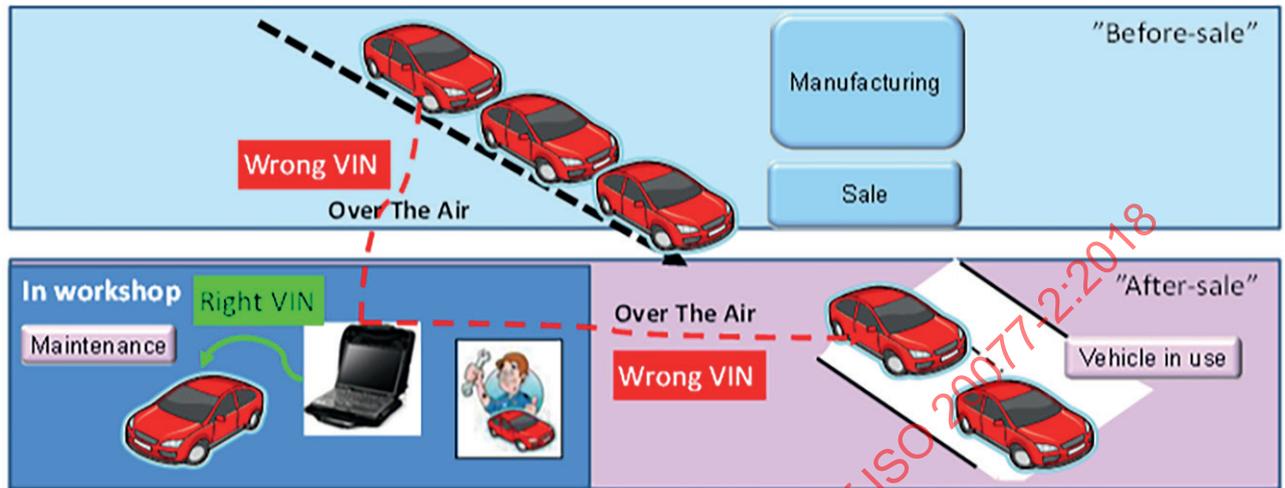
The result of this analysis can cause a reduction in performances and availability of the requested ExVe functionality.
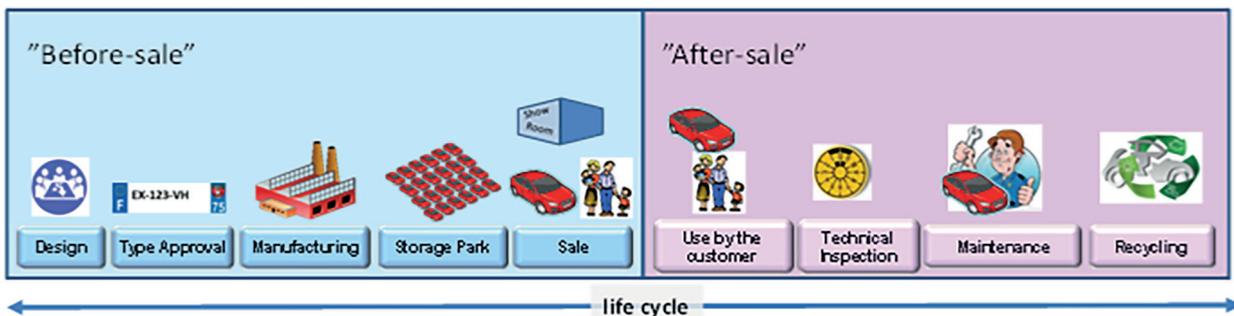
NOTE 1   Design and production phases are identified on the left part of this figure.

NOTE 2   After sales phases are identified on the right part of this figure.

Figure 3 — Illustration of the life cycle phases of an extended vehicle

EXAMPLE of BP_004 contribution to the safety rule (see Figure 4):

This example illustrates possible mistaken remote activations that need to be assessed by the ExVe manufacturer.

Mistaken remote activation by a provider of vehicle in « before sale » situation as in factory or show room shall be avoided. Depending of vehicle and functionality activated, there can be major safety risks for the people inside or outside of the vehicle as for goods. To avoid that, the ExVe functionality has to be activated only by the authorized person in the considered situation.

In Figure 5, a wrong VIN is entered by the technician for accessing a vehicle in service. This incorrect VIN may be the correct VIN of a vehicle still in production. This error may lead to critical issues during the production phase of that vehicle.

Figure 4 — Example of a potential risk addressed by BP_004

8.4   Basic principle related to remote access

BP_005	The ExVe manufacturer is responsible for managing the additional risks within the ExVe that are attributed to an existing functionality when this functionality becomes remotely available.
002	

A remote access can lead to operations in certain conditions in which the current status and the environment of the vehicle cannot be established.

In certain situations, this could cause damage to the vehicle, other vehicles or injuries to the passengers or people around the vehicle.

This may be the case for example of functionalities that control the engine injection system, the electronic brakes valves, or a simple function like operating an electric window.

A fundamental analysis of the additional risks associated with the ExVe functionality is therefore essential prior to the design.

EXAMPLE of BP_005 contribution to the safety rule (see Figure 5):

In the example of Figure 5, when the diagnosis of a vehicle is performed in the after-sales workshop ("situation 1"), a professional can decide to control an engine injector after a prior visual inspection of the vehicle.

This same functionality could be performed using a remote access through the extended vehicle when the vehicle is stopped on the roadside ("situation 2"). In this situation, however, if the injection system had a fuel leak, then the same control action could have major consequences for people and environment.

In "situation 1", there is a competent professional that is managing the safety chain by applying specific procedures and can react in case of an emergency. This may not be the case in "situation 2", depending on the presence or the absence of a local diagnostic facilitator.

A local diagnostic facilitator shall, at the minimum, be able to understand or describe the indications of the on-board instruments and tell-tales.
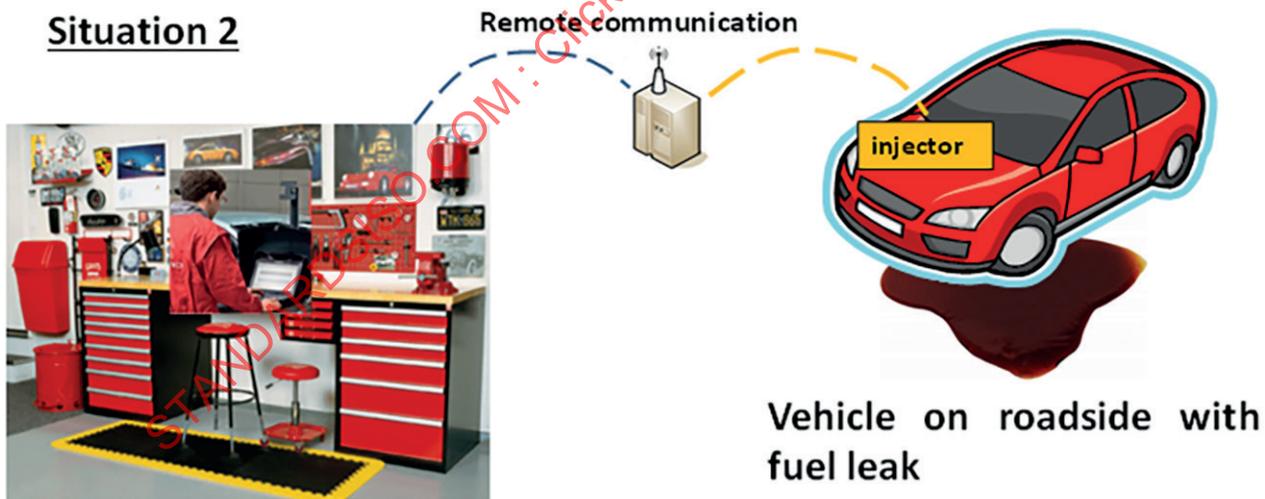

Figure 5 — Example of a potential risk related to BP_005

8.5 Basic principle related to the existing design of an extended vehicle

BP_006	The ExVe manufacturer is responsible for managing the impacts of an additional remote functionality taking into account the existing design.
002	

When a new ExVe functionality is implemented, the ExVe manufacturer may take into account the existing design (see Figure 6). The implementation may lead to having to modify some existing ExVe functionalities. The depth of modifications made depend on:

— whether the ExVe manufacturer's implementation of the functionality is on-board and/or off-board;

— consideration of existing functionalities within the extended vehicle; and

— existing functionality not meeting the requested performance or availability without affecting the original functionality.
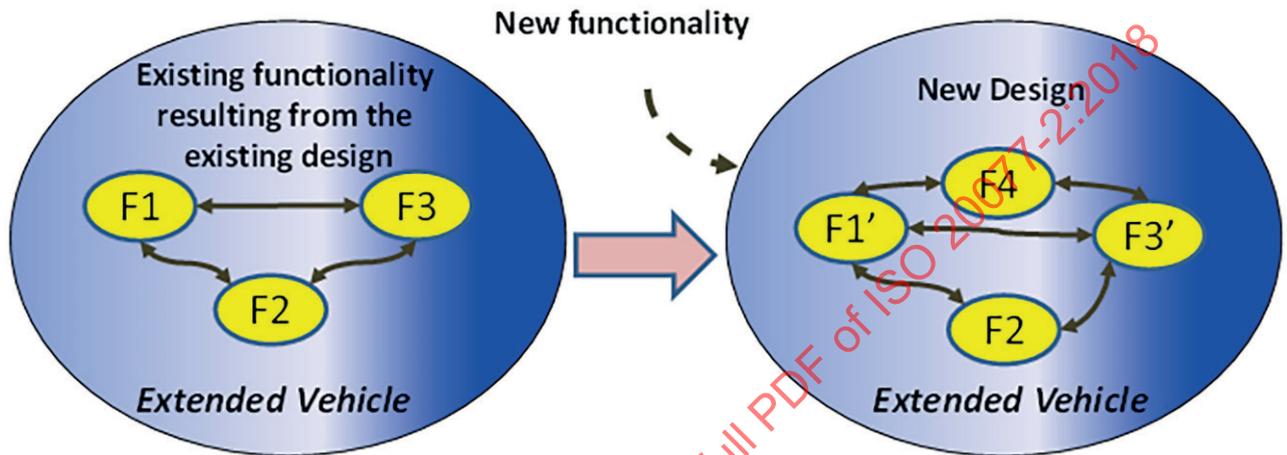

Figure 6 — Example of a new functionality integrated within an extended vehicle

Once the choice has been made by the ExVe manufacturer to keep existing functionalities, the next design steps will be:

a) to manage the priorities among these functionalities and the new one, during the ExVe operation (BP_007); and

b) to manage the resource availability (BP_008).

EXAMPLE of BP_006 contribution to the security rule (see Figure 7):

Modern vehicle electronic architecture manages the security by implementing security data within multiple ECUs. This limits the possibility of vehicle theft.

An implementation of remote functionality that does not protect the access to this security data are not acceptable.

In the example of Figure 7, the situation on the left side describes a securely locked vehicle, and the situation on the right side describes a situation where it is possible to unlock the vehicle by interfering with the locking message.

Figure 7 — Example of a risk related to BP_006

8.6 Basic principle related to interactions and management of priorities between the ExVe functionalities

BP_007	The ExVe manufacturer is responsible for defining the priorities between all functionali-
002	ties of the extended vehicle.

When an additional functionality is implemented within the extended vehicle, it shall be integrated within the existing ExVe functionalities (see BP_006) of the extended vehicle to achieve a consistent priority system.

8.7 Basic principle related to non-regression and availability of resources

BP_008	The ExVe manufacturer is responsible for securing that the additional functionality does
002	not affect already designed and implemented functionalities of the extended vehicle, in particular by taking into consideration the available resources of that extended vehicle.

From the start of a new project, subsequently and throughout the study and development cycle, it is vital to ensure adequate allocation of the digital processing capability of the system to the application functional need.

When an additional functionality is implemented within the extended vehicle, the ExVe manufacturer shall ensure that the existing functionalities (see BP_006) are not negatively impacted by implementation of the additional functionality.

> EXAMPLE of BP_008 contribution to R_001 "Safety related rule" (see Figure 8):
>
> In the first situation, the ExVe manufacturer has designed the electronic resources to be able to perform brake function in an emergency situation.
>
> In the second situation, some electronic resources have been negatively impacted and the flow of data interrupted, reducing the required resources and therefore the exchange of critical brake function data.
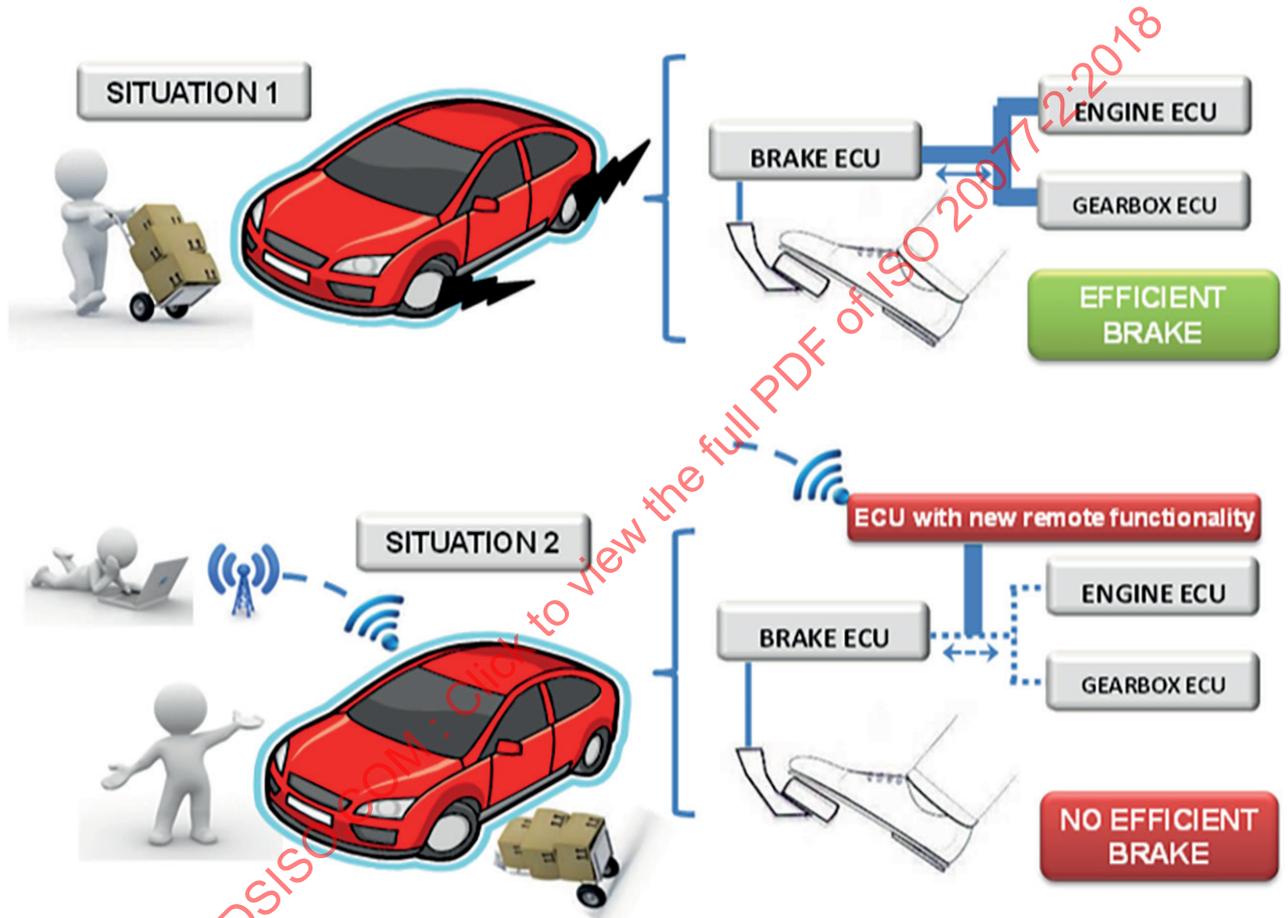

Figure 8 — Example of a potential safety related risk addressed by BP_008

Basic principles related to communication with the extended vehicle

BP_009	The extended vehicle design methodology is applicable regardless of the type(s) of communication (wired or wireless).
001	

BP_010	For a given use-case and use-case scenario, the ExVe manufacturer is responsible for defining the appropriate extended vehicle's interfaces for the considered functionality,
002	and for designing them so that they can support defined requests in a non-discriminatory manner.

The data for each functionality is accessed through an appropriate interface of the extended vehicle (see Figure 10).

NOTE   The use of dedicated interfaces for accessing data related to functionality does not imply the availability of the data.
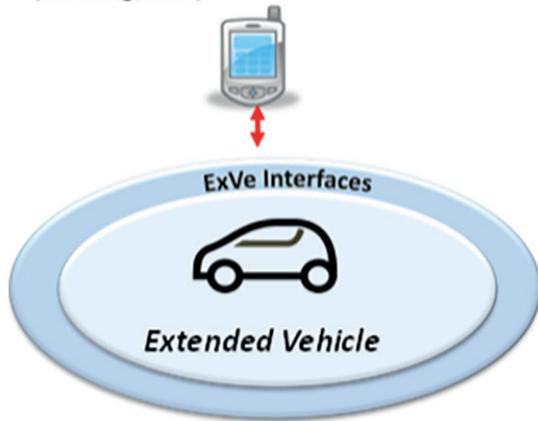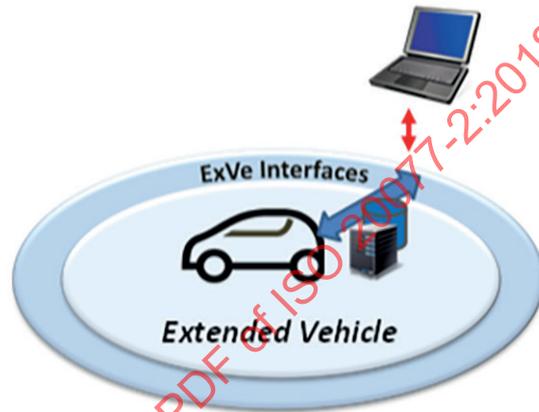

Figure 10 — Two different examples of extended vehicle interfaces, each addressing a different use-case

8.8   Basic principle related to validation of the ExVe functionality

BP_011	The ExVe manufacturer is responsible for validating the design of the complete extended
002	vehicle as a complete system.

The ExVe manufacturer is responsible for validation within the extended vehicle. The requester is responsible for the validation of the system interacting with the extended vehicle.

8.9   Basic principles related to non-monitoring

BP_012 and BP_013 have been included in order to mitigate the risks of competition distortion.

BP_012	The ExVe manufacturer is responsible for ensuring that the designed ExVe functionality
002	respects that the correlation between the vehicle owner and the performed functions is not monitored for competition purposes.

BP_013	The ExVe manufacturer is responsible for ensuring that the designed ExVe functionality
002	respects that the correlation between the after-sales service provider and the performed functions is not monitored for competition purposes.

9   ExVe design methodology — Templates

9.1   General

The target of the template for technical request ("Request template") is to support the precise description of the need.

The target of the template for technical response ("Response template") is to precise the feasibility of the request through the extended vehicle concept.

9.2 Template for technical request

For each ExVe functionality request, the requester shall use the template specified in Annex A to provide the necessary technical information.

This information shall be provided according to the procedures of the ExVe manufacturer (communication support, format, template, etc.).

It shall include the reference to a contractual agreement between the ExVe manufacturer and the requester (if applicable).

NOTE 1   This technical information complements the administrative information that is provided according to common practices and that is not the object of this document.

NOTE 2   Providing this technical information can be replaced by referencing a publicly available document (e.g. an ISO standard) that already contains this information.

Table 1 gives explanations and examples for documenting the template for technical request.

Figure 11 illustrates the possible detail level of the needs to be included in the request template.
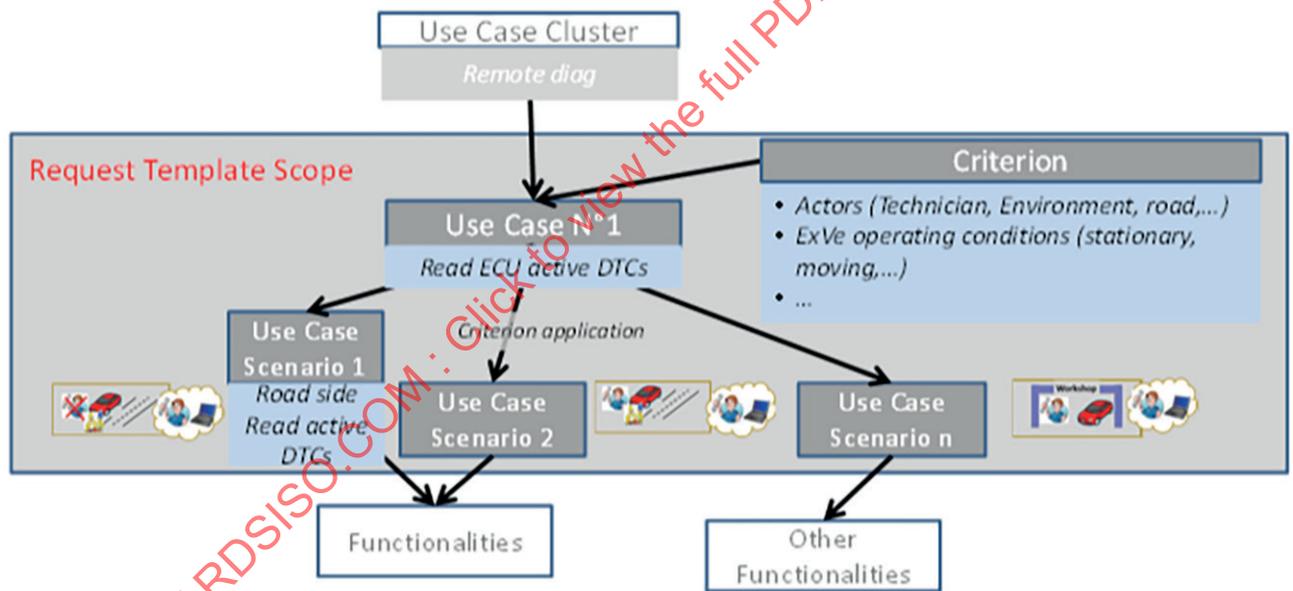

Figure 11 — Schematic related to the detail of the needs included in a request template

Table 1 — Explanations and examples for documenting the template for technical request

REQUEST FORM (technical)		
Reference to a contractual agreement between the ExVe manufacturer and the requester (if applicable)		*EXAMPLE:* *NDA Nr 13345/XX/2017*
General description of the need		
Use case		
Requested information	General explanation	Example for documenting
Proposed name for the ExVe functionality	Description of what should be fulfilled by this functionality	*Read ECUs Active DTCs*
NOTE The examples mentioned in this table are mentioned for illustration only.		

Table 1 *(continued)*

REQUEST FORM (technical)		
Reference to a contractual agreement between the ExVe manufacturer and the requester (if applicable)		*EXAMPLE:* *NDA Nr 13345/XX/2017*
Functionality goals	Expected principle users of the functionality	*When there is a failure in a vehicle, send over the air the list of active DTCs.*
Users for the functionality	Describe precisely who is mainly in charge of the functionality.	*Remote Technician, Technician in front of the vehicle, Computer*
Responsible during functionality application	Describe precisely who will be responsible to manage the safe condition during the functionality application.	*Main user*
Conditions for functionality usage	Describe as precisely as possible the different conditions for the functionality application.	*Usage during vehicle stationary and/or engine running and/or vehicle moving,*
Nominal response	Describe precisely the response expected: contain, form.	*DTC list*
Minimum response	If it's not possible to give the nominal response describe precisely what should be the minimum response expected	*No DTC present*
Performance expected	Describe overall Performance expected for this functionality, for example minimum time expected for the answer, frequency, timing constraints of the answer, format of data and size	*Receive the list of DTC in 10 s maximum*
Use case scenario 1		
Description	*EXAMPLE Read active DTCs with vehicle in the Road Side, Technician in Remote.*	
Use case scenario 2		
Description	*EXAMPLE Read active DTCs with vehicle moving, Technician in Remote.*	
...		
Use case scenario n		
Description		
NOTE The examples mentioned in this table are mentioned for illustration only.		

9.3   Template for technical response

For each ExVe functionality request, the ExVe manufacturer shall use the template specified in Annex B to provide the necessary technical response information.

This information shall be provided according to the procedures of the ExVe manufacturer (communication support, format, template, etc.).

NOTE   This technical information complements the administrative information that is provided according to common practices and that is not the object of this document.

Table 2 gives explanations and examples for documenting the template for technical response.

Remarks:

—   If the requested ExVe functionality cannot be made, the VM informs the requester about it.

—   If needed, the VM describes the possible usage limitations of the new ExVe functionality.

—   The availability of the ExVe functionality and its data is the consequence of a design trade-off, the design may then vary based on each ExVe manufacturer.