TECHNICAL REPORT

ISO/TR 23786

First edition
2019-11

Road vehicles — Solutions for remote access to vehicle — Criteria for risk assessment

Véhicules routiers — Solutions relatives à l'accès à distance du véhicule — Critères d'évaluation des risques

Reference number
ISO/TR 23786:2019(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

For an explanation of 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 www.iso.org/iso/foreword.html.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The development of one of the remote communication solutions that ISO/TC22/SC31/WG6 was in charge of revealed several concerns about possible risks related to safety, security, competition, responsibility, and data protection that may originate from that solution.

To address these concerns, a list of criteria was first developed to be taken into account, independently of the considered solution. ISO/TC22/SC31/WG6 then decided to perform a risk assessment of any interface solution under its responsibility. This task was achieved based on the expertise of its expert members.

The aim of this document is to capitalize the achieved work in order to:

— Allow any ISO working group to use that list if they so want without having to redo the complete work.

— Allow stakeholders to conduct a risk analysis on remote communication solutions utilizing the basis of a comprehensive and consolidated document produced by international experts and referring, as necessary, to complementary specific documents.

The proposed list of possible risks does not pretend to be exhaustive and its users are kindly invited to refer as much as possible to the more detailed work performed in other ISO working groups (for example, regarding the risks related to cyber-security, they are invited to refer to the work performed in ISO TC22/SC32/WG11).

Road vehicles — Solutions for remote access to vehicle — Criteria for risk assessment

1 Scope

This document identifies criteria that can be considered for assessing the risks related to solutions for remote access to road vehicles, including extended vehicles (ExVe) and their implementation.

Internal communication within the vehicle or the ExVe is out of the scope of this document.

Cybersecurity risks related to the VM infrastructure (except the elements that are part of the extended vehicle) and the road-side equipment are out of the scope of this document.

The criteria identified in this document are also applicable in the case of a risk assessment related to the specification of remote communication solutions, for example a technical standard.

The list of criteria that is provided can be considered as sufficiently comprehensive but not exhaustive, from a global point of view, to allow coherent risk mitigation, if such mitigation is necessary.

This document does not suggest nor specify any methodology for performing a risk assessment.

It does not aim at replacing any methodology, technical specification or standard relative to one or other specific type of risks (for example cyber security risks).

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

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

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

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

3.1
extended vehicle
ExVe
entity, still in accordance with the specifications of the vehicle manufacturer, that extends beyond the physical boundaries of the road vehicle and consists of the road vehicle, off-board systems, external interfaces, and the data communication between the road-vehicle and the off-board systems

[SOURCE: ISO 20077-1:2017, 3.5, modified — The term ExVe has been added.]

3.2
remote communication solution specification
RCS-specification
set of technical specifications for a remote communication solution

EXAMPLE ISO 20078-1:2019 *Road vehicles — Extended vehicle (ExVe) 'web services' — Part 1: ExVe content*[3].

Note 1 to entry: A technical standard can be considered as RCS-specification.

3.3
web service
software system, with an interface described in a machine-processable format, and designed to support interoperable machine-to-machine interaction over a network

[SOURCE: ISO 20077-1:2017, 3.21]

3.4
accessing party
party that accesses *resources* (3.7) via *web services* (3.3)

[SOURCE: ISO 20078-1:2019, 3.1.6, modified — The notes to entry have been deleted and the word entity has been substituted by party.]

3.5
authorisation provider
entity at the offering party that manages the access rights to *resources* (3.7) and *resource owner* (3.9) information

[SOURCE: ISO 20078-1:2019, 3.1.9, modified — Note 1 to entry has been deleted.]

3.6
identity provider
entity responsible for authentication (identification) of users, through the use of credentials

Note 1 to entry: Offering party confirms the identity of the authenticated *resource owner* (3.9).

[SOURCE: ISO 20078-1:2019, 3.1.7, modified — Note 2 to entry has been deleted.]

3.7
resource
data, aggregated information or functionalities of the connected vehicle

[SOURCE: ISO 20078-1:2019 3.2.1, modified — Note 1 to entry has been deleted.]

3.8
resource provider
entity at the offering party that protects and provides *resources* (3.7)

[SOURCE: ISO 20078-1:2019, 3.1.8]

3.9
resource owner
responsible party for the *resource(s)* (3.7)

Note 1 to entry: The resource owner is responsible for granting, denying, and revoking access to resource(s).

Note 2 to entry: The responsible resource owner is determined by the concrete resource.

[SOURCE: ISO 20078-1:2019, 3.1.4]

4 Abbreviated terms

VM Vehicle Manufacturer

RCS Remote Communication Solution

5 Handling the risks

5.1 Risk categories

In the present document, the risks that have been considered are grouped as follows:

— Safety risks: risks related to the safety of persons and goods during the vehicle life cycle,

— Security risks: risks associated to the security of the vehicle communication system,

— Competition risks: risks associated to the fair competition among the concerned actors,

— Responsibility and liability risks: risks related to the responsibility and liability of the concerned actors,

— Data protection risks: risks related to the protection of the resources owned by the resource owner.

5.2 Performing the risk assessment

Prior to the risk assessment, it is important to determine and to define the scope of the assessment. For example, when the risk assessment addresses a certain remote communication solution, does it also include its implementation?

This having been done, the risk assessment itself can proceed. The risk assessment answers the following question for each of the risks listed in this document: "Does the remote communication solution present, for a certain use case, any of the considered risks?". The value of the assessment can be increased by considering the state-of-the-art of the solution for the risk or other categories such as environmental or regulatory.

This analysis is clearly independent of the possible methods or technical improvements that can be selected to reduce one or several risks. These solutions can indeed have an impact on other risks rather than the ones they intend to reduce. These solutions are therefore considered as new and subjected to a completely new risk assessment. For example, an exceptional method to solve a competition risk can have a high impact on some safety risks or vice-versa.

This having been said, the use of the ISO design methodology that is appropriate to remote communication solutions is recommended to reduce the considered risk: ISO 20077-2[2]. The resulting analysis using this recommendation can increase the value of the solution to the risk.

A template that can be used for addressing each of the considered risks is given in Annex A.

5.3 Risk assessment in the case of an RCS-specification

When the risk assessment is related to RCS-specification, the assessment results from the answer to the following question:

Does the RCS, when designed according to the specification for a certain use case, present safety, cybersecurity, competition, responsibility, or data protection risks?

NOTE For example, an RCS-specification that does not present any risk itself, can or cannot present risks due to the manner of implementation.

More precisely, the following additional questions are worth considering because of their impact on the level of the possible risks, as shown in Figure 1:

— Do the specifications contain measures that solve the considered risk?

— Do the specifications facilitate implementation that can reduce or solve that risk?

— Do the specifications contain measures that generate a risk?

— Do the specifications prohibit or inhibit implementation that reduce or resolve that risk and do not increase the complete set of risks?

Does the remote communication interface, when designed according to RCS-specs present a risk originating from that document?

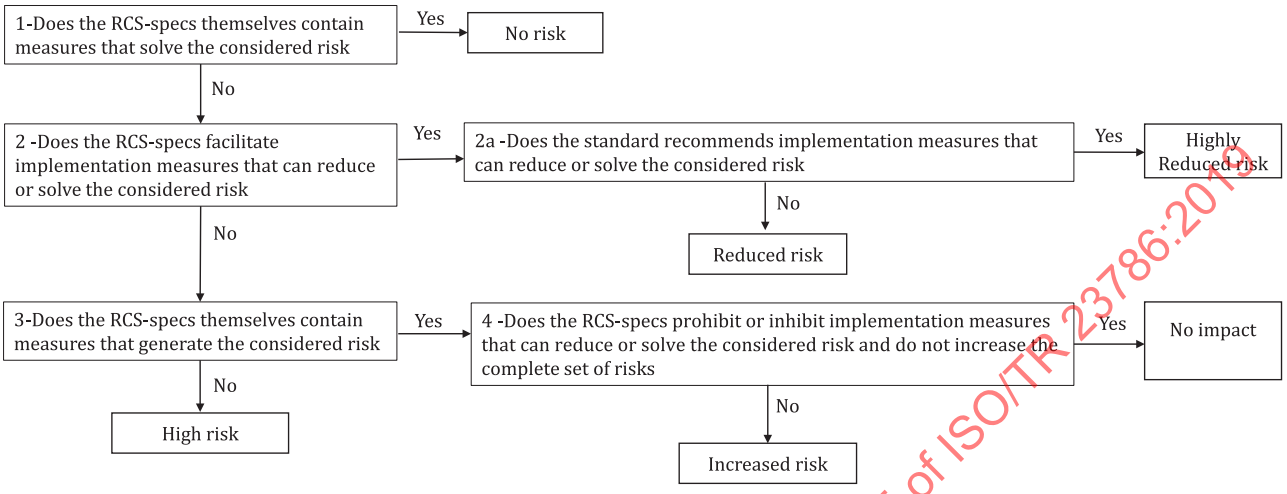

Figure 1 — RCS-specification - impact of its content on the assessed risk

6 Assessment of the risks related to the safety of persons and goods during the vehicle life cycle

6.1 List of safety risks

The safety risks considered for this assessment can contain, as a minimum, the following:

— Safety risks that are not resulting from cybersecurity issues or problems:

  — SAFE 1: Potential overload of the electronic system of the moving vehicle (numerous simultaneous requests);

  — SAFE 2: Potential overload of the electronic system of the moving vehicle (frequent requests);

  — SAFE 3: Potential overload of the electronic system of the moving vehicle (unexpected requests);

  — SAFE 4: Potential illicit or malicious remote control of vehicles;

  — SAFE 5: Incompatibility with the existing systems and mechanisms;

  — SAFE 6: Failures of the remote communication solution itself of the ExVe including the VM back-end server when applicable;

  — SAFE 7: Non-consideration of the complete vehicle life cycle;

  — SAFE 8: Risks related to the design validation process;

  — SAFE 9: Absence of misuse prevention.

— Safety risks that are resulting from cybersecurity issues or problems:

  — SAFE 10: Absence of or inappropriate measures aiming at reducing the risks in case of illicit or malicious remote control of vehicles;

  — SAFE 11: Other safety risks resulting from cybersecurity issues or problems.

NOTE In these two lists the electronic system encompasses both the hardware and the software.

6.2 Remarks related to the assessment of the safety risks

6.2.1 General

The question for analysing the safety risks is “Does the RCS present, any safety risk?”.

Remark: When the risk assessment is applied to a standardised RCS-specification (for example the ISO 20078 series that does cover implementation), the risk assessment is limited to the scope of that standard.

6.2.2 Potential overload of the electronic system of the moving vehicle

In this analysis, the safety risks related to a potential overload of the electronic system, for whatever the reason, are only concerning the electronic system of the moving vehicle.

The safety risks, if any, related to a potential overload of a communication system outside the moving vehicle can be the object of a new risk, as they are not part of the proposed list.

When assessing these risks, it is important to:

— estimate the ability of the prioritisation mechanisms in place to achieve the tasks they have been given without endangering the available computing resources of the moving vehicle.

— determine the consequences in terms of the competition risk of this ability.

6.2.3 Illicit or malicious remote control of the vehicle or vehicles

Illicit or malicious remote control of the vehicle or vehicles can result from major security / cybersecurity attacks. They can, in particular, lead to safety risks that the VM would like to reduce by appropriate design measures. For example, in ISO 20078-1[3] the implementation of web service communications via the back-end server of the vehicle manufacturer can enable a substantial reduction of these risks and can be achieved by the vehicle manufacturer appropriately designing the backend server.

In addressing a possible illicit remote control of a vehicle or vehicles the implemented measure can focus on the safety risks and not on the security and other IT related risks. The measure can also take into account fair competition as addressed in Clause 8.

There can be safety risks associated to illicit, though not malicious, remote control, as illustrated by the example below. The conditions for a safe remote control can be distinguished from the conditions addressing security risks, where an illicit remote control can lead to safety issues.

EXAMPLE A potential risk associated with remote control.

When the diagnosis of a vehicle is performed in the after-sales workshop (see Figure 2, “situation 1”), a professional can decide to control an engine injector after a prior visual inspection of the vehicle.

This same functionality can be performed using a remote communication solution when the vehicle is stopped on the roadside (see Figure 2, “situation 2”). If the injection system had a fuel leak, then the same control action can have major consequences for people and environment.

In “situation 1", there is a qualified professional who is managing the safety chain by applying specific procedures and who 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.

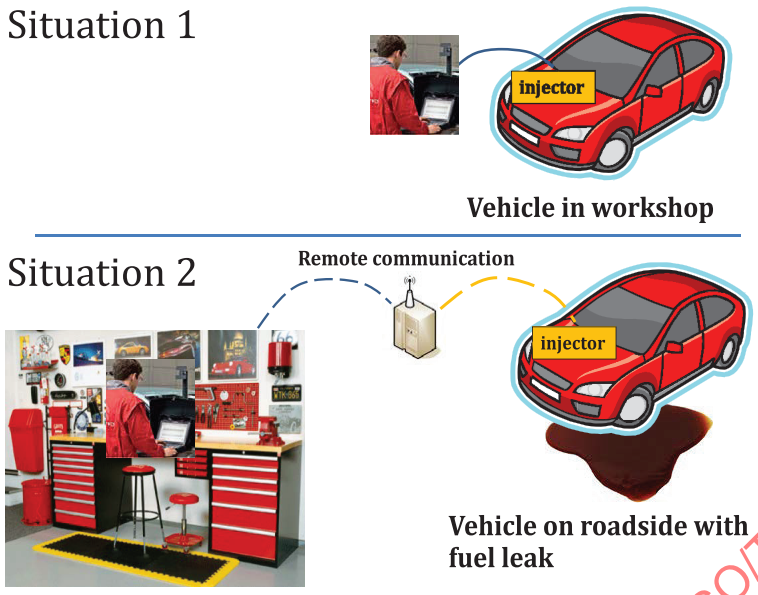

Figure 2 — Illustration of a potential risk associated with remote control

6.2.4 Other safety risks resulting from cybersecurity issues or problems

In a similar manner to the risks of malicious or illicit control, other safety risks can result from cybersecurity attacks.

Cybersecurity measures can indeed be seen as "protection" of the extended vehicle as not to compromise control, modify or delete design features (software and hardware), etc. The absence or weakness of that "protection" can lead to safety issues.

As in the case of malicious or illicit control, the assessment of these risks focuses on the safety risks and not on the cybersecurity risks.

6.2.5 Absence of consideration of the complete vehicle life cycle.

Safety issues can occur in the case of a dysfunction in the process of informing the authorisation provider of a change of the life-cycle stage (manufacturing, sales, operation, maintenance and repair, end of life).

Safety risks can also result from incompatibilities occurring in phases different than the one for which the solution has been primarily developed (see the example below). It is not enough to assess the safety risks of a solution only during the operation phase of a vehicle life cycle. The safety risks are also assessed during all other phases.

EXAMPLE Safety issue resulting from absence of consideration of the manufacturing stage.

During a maintenance check, a VIN is entered by a remote technician for accessing a vehicle in service. The VIN entered is valid, but not associated to that vehicle, but to a vehicle that is still in production.

The intended remote operation on the vehicle in production would present a safety issue.

The risk assessment analysis, in this case, would show that the RCS did not consider the situation of a vehicle that is still in production.

7 Assessment of the cybersecurity risks related to the vehicle remote communication system

7.1 Cybersecurity risks

The cybersecurity risks considered for this assessment contain, as a minimum, the following:

— SEC 1: Integrity and authenticity;

— SEC 2: Vehicle systems that are not located at the moving vehicle;

— SEC 3: Consequences of a complete or partial cybersecurity breach (this includes safety, security, competition, confidentiality and data protection risks);

— SEC 4. Absence of misuse prevention measures.

7.2 Remarks related to the assessment of the cybersecurity risks

7.2.1 General considerations related to cybersecurity risks

This document lists the cybersecurity risks classified as important risks to be assessed. It does not list nor consider all aspects of these risks.

The persons or bodies responsible for this assessment are invited to refer to the work performed within this domain, for example to the work achieved by ISO and in particular by ISO/TC22/SC32/WG11[4], to the work achieved by the United Nations [5], and to the work achieved by other standard organisations such as NIST[6] and ENISA[7].

Remarks:

— Regarding the criteria considered in this document, cybersecurity measures can be a method of protection of the connected vehicle and does not compromise ownership. General considerations can be related to integrity and authenticity.

— In addition, there may be confidentiality and data protection risks related to cybersecurity (e.g. SEC 3).

The final level of integrity and authenticity, that involves all actors in the process, is mainly affected by implementation of the RCS.

In the case of RCS-specifications, this implementation can be out of the scope. It is then important to highlight the point and make the appropriate recommendations for the implementation, for example by referring to ISO 20077-2:2018[2].

7.2.2 General considerations related to misuse prevention measures

In terms of security risk, it is worth questioning whether the RCS should include misuse prevention measures, for example:

— in allowing a controlled access arbitration when the vehicle is in-use,

— in allowing an efficient limitation of the passed information,

— in allowing a monitoring of the passed information,

— in only communicating with trustworthy parties.

It is highly recommended, if such measures exist to also estimate the competition risks related to such measures.

8 Assessment of the risks associated to the fair competition among the concerned actors

8.1 List of competition risks

The competition risks considered for this assessment contain, as a minimum, the following:

— FAIR 1: Potential misuse of the acquired knowledge;

— FAIR 2: Potential gaining of unique knowledge of the market through monitoring;

— FAIR 3: Potential gaining of unique knowledge of the customer's behaviour through monitoring;

— FAIR 4: Competition among the involved parties;

— FAIR 5: Excluding competitors from playing roles;

— FAIR 6: Development of new after-sales applications;

— FAIR 7: Competition among manufacturers.

8.2 Remarks related to the assessment of the competition risks

8.2.1 Involved actors

To address competition risks, there could be an initial consideration of who the involved actors are that could be affected by a potential unfair competition situation. These actors are those in the data communication chain between the vehicle and the final user of the data.

Although this list is not exhaustive, the following actors could be involved:

— The resource owner;

— The accessing party;

— The resource provider;

— One or several authorisation providers;

— One or several identity providers;

— One or several after sales service providers.

It is also important to have a complete view of the entire communication process and not only a view of the one where the RCS is directly involved.

These considerations are important as competition risks can exist at each level of the communication chain, and reducing the risks at one place can have the consequence to increase it at another place.

8.2.2 Risk related to the monitoring of the market

The issue is to determine whether there are competition risks, through monitoring, of some competing involved actors having knowledge of the market (e.g. in case of brand specific, after-sales service). In particular:

— because of their role as a resource provider,

— because of their role as an authorisation provider,

— because of their role as an identity provider.

The risk of unfair competition is existing between a party that has knowledge and other involved actors that cannot access this knowledge (see Examples 1 and 2).

NOTE These risks can concern the vehicle manufacturer as well as other parties such as the accessing party.

EXAMPLE 1 Monitoring of the road-side assistance market.

By having both knowledge of:

— the location of vehicles on a certain highway, and

— the identity of the actor that requests remotely, e.g. diagnostic information,

it is possible by correlation to monitor part of the business of that actor.

EXAMPLE 2 Monitoring of a business chain.

By having both knowledge of:

— the location of vehicles at a certain workshop, and

— the identity of the service provider if this actor is also the accessing party,

the business relationship between the workshop and the accessing party can be visible. Correlation is then possible, making it possible for the knowledge owner to access that business chain.

8.2.3 Possible unique knowledge of the customer's behaviour through monitoring,

The issue is to determine whether there are competition risks through monitoring, of some competing involved actors having knowledge of the customer's behaviour (e.g. in case of brand specific, after-sales service). In particular:

— because of their role as a resource provider,

— because of their role as an authorisation provider,

— because of their role as an identity provider.

The risk is that, having this knowledge, one involved actor can monitor the market behaviour of a vehicle owner (for example, which after-sales service provider he selects and for which purpose), while competing involved actors that do not have the same knowledge cannot (see the example below).

Remarks:

— this risk concerns the vehicle manufacturer as well as other involved actors such as the authorisation provider(s) or the accessing party,

— this risk can also be linked to the risk related to the knowledge of the market.

EXAMPLE Unfair business monitoring.

An accessing party monitors the correlation between vehicle owners and remote after sales services. On the basis of this correlation an after-sales service provider affiliated to the accessing party contacts vehicle owners and proposes a service similar to the ones offered by the other competing after-sales service providers.

NOTE In this example, monitoring leads to unfair competition and a misuse of data privacy.

8.2.4 Risks related to the development of new after-sales applications

The issue is to determine whether the RCS presents:

— competition risks among the parties considering the development of similar but different applications;

— competition risks related to the availability, in a non-discriminatory manner, of information that is necessary for developing new services and that have not yet been made available.

The considered risks are related to the non-discriminative character of providing information.

To assess this risk, it also can be worth considering how the remote-communication solution specifies the content of the communicated resources.

8.2.5 Competition risks among manufacturers

The issue is to determine whether the remote communication solution presents risks related to the competition among vehicle manufacturers and/or vehicle component or system suppliers.

It can be determined whether the solution presents risks of communicating private data and intellectual property without the full agreement of its owner (vehicle or system manufacturers, suppliers, etc.).

9 Assessment of the risks related to the responsibility and liability of the concerned actors

Liability is a concept that is either connected to legislation or connected to business agreements; it is always based on the principle of responsibility.

This document considers the assessment of the risks that are related to the responsibility of the concerned actors and can potentially lead to liability risks, as follows:

— RESP 1: Does the remote communication solution or the RCS-specifications introduce responsibilities without allocating them to any identified party?

— RESP 2: Does the remote communication solution or the RCS-specifications confuse the share of responsibilities?

An example for responsibility and liability is a product and its environmental impact.

10 Assessment of the risks related to the protection of the resources owned by the resource owner (data protection)

The assessment considers determining whether the remote communication solution presents, for a certain use case, risks related to the protection of the resources owned by the resource owner (data protection).

The data protection risks considered for this assessment can include, as a minimum, the following risks of the possible negative impacts caused by the ability of the resource owner to:

— PROT 1: decide on the required transmitted information limiting this to prevent data misuse;

— PROT 2: grant or reject access permission for any of the involved parties (accessing party, service provider, etc.); for access to different use-cases; communicating these permissions in a timely manner;

— PROT 3: monitor the information requests made on the resource owner's behalf.

In this approach, the analysis can disregard important data protection risks, when these risks are concerning actors that are outside the scope of the remote communication solution or RCS-specifications. In this case, it is important to refer to these risks if they are identified.

