TECHNICAL REPORT

ISO/TR 23791

First edition
2019-09

Road vehicles — Extended vehicle (ExVe) web services — Result of the risk assessment on ISO 20078 series

Véhicules routiers — Web services du véhicule étendu (ExVe) — Résultats de l'évaluation des risques de la série de normes ISO 20078

Reference number
ISO/TR 23791:2019(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 ISO 20078 series specifies a possible web service to implement a certain web interface of the Extended Vehicle, depending on the concerned use case.

The development of this series has revealed several fears about possible risks related to safety, security, competition, liability, and data protection that may originate from that interface.

To address these fears, a list of criteria was first developed to be considered independently of the considered interface. This list is the object of ISO/TR 23786.

This list was then used for assessing the risks originating from the ISO 20078 series and concept to issue this document.

Finally, the risk assessment demonstrated that there are no risks resulting from the ISO 20078 series itself, however, there may be risks resulting from an implementation of that series.

Road vehicles — Extended vehicle (ExVe) web services — Result of the risk assessment on ISO 20078 series

1 Scope

This document presents the assessment of the safety, security, competition, responsibilities, and data protection risks that can originate from the ISO 20078 series.

In particular, the following risks are outside the scope of this assessment, because they relate to elements that are excluded from the scope of the ISO 20078 series:

— the risks associated with the implementation of the ISO 20078 series;

— the risks associated with the process that the accessing parties or any other parties would later on use to communicate the information they obtained;

— the risks associated with the process used by the resource owner to provide, modify, or revoke their authorization to pass information;

— the risks associated with the mitigation of the risks, should such a mitigation be necessary.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 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 http://www.iso.org/obp

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

3.1.1
accessing party
entity which accesses *resources* (3.1.8) via *web services* (3.1.11)

[SOURCE: ISO 20078-1:2019, 3.1.6, modified — Notes to entry have been deleted.]

3.1.2
authorization provider
entity at the *offering party* (3.1.7) that manages the access rights to resources and *resource owner* (3.1.9) information

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

3.1.3
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 — Note 1 to entry has been deleted.]

3.1.4
ExVe manufacturer
vehicle manufacturer responsible for the *extended vehicle* (3.1.3)

[SOURCE: ISO 20077-1:2017, 3.6]

3.1.5
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.

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

3.1.6
intermediate body
party that manages the authorizations given by the *resource owner* (3.1.9) to communicate resources to the *accessing party* (3.1.1) via *web service* (3.1.11)

3.1.7
offering party
entity who provides *web services* (3.1.11) access to *resources* (3.1.8)

[SOURCE: ISO 20078-1:2019, 3.1.3.]

3.1.8
resource
data, aggregated information or functionalities of the connected vehicle

[SOURCE: ISO 20078-1:201, 3.2.1, modified —Note 1 to entry has been deleted.]

3.1.9
resource owner
responsible party for the *resource(s)* (3.1.8)

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.]

3.1.10
resource provider
entity at the *offering party* (3.1.7) that protects and provides *resources* (3.1.8)

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

3.1.11
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.]

3.2 Abbreviated terms

ExVe Extended Vehicle

VM Vehicle Manufacturer

4 General result of the risk assessment

This document presents a risk assessment of the ISO 20078 series. This means it intends to answer to the following question: “Does the ISO 20078 series generate any safety, security, competition, responsibility, liability, or data protection risks?”

The answer is NO: The ISO 20078 series does not generate any safety, security, competition, responsibility, liability, or data protection risks.

Nevertheless, the risk assessment did not consider the manner the ISO 20078 series is implemented. Therefore, there may be safety, security, competition, responsibility, liability, or data protection risks resulting from implementation.

It is therefore recommended to conduct a risk assessment by the vehicle manufacturer on safety, security, competition, responsibility, liability, or data protection for the individual implemented solution.

5 Categories of the assessed risks

In this document, the risks that have been assessed are the one listed in ISO/TR 23786. They are regrouped 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.

More precisely, the assessment results from the answer to the following question: “Can the ExVe web service interface, when designed according to the ISO 20078 series for a certain use case, present safety, security, competition, responsibility, liability, or data protection risks originating from that series?”

The risks resulting from the implementation of the ISO 20078 series are excluded from the assessment. In particular, when implementing the ISO 20078 series, the ExVe manufacturer will design all the arbitration mechanisms, including the mechanisms aiming at mitigating the risks. To address these risks the ExVe manufacturer is invited to apply the design methodology specified in ISO 20077-2.

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

6.1 Safety risks considered

“Can the ExVe web service interface, when designed according to the ISO 20078 series for a certain use case, present safety risks originating from that series?”

The safety risks considered for this assessment are the following:

— overload safety risks that are not resulting from cybersecurity issues or problems:
  — SAFE 1. Possible overload of the electronic system of the moving vehicle (numerous simultaneous requests);
  — SAFE 2. Possible overload of the electronic system of the moving vehicle (frequent requests);
  — SAFE 3. Possible overload of the electronic system of the moving vehicle (unexpected requests);
  — SAFE 4. Possible illicit or malicious remote control of vehicles;
  — SAFE 5. Lack of compatibility 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. Lack of consideration of the complete vehicle life cycle;
  — SAFE 8. Risks related to the design validation process;
  — SAFE 9. Lack of misuse prevention;
— safety risks that are resulting from cybersecurity issues or problems:
  — SAFE 10. Lack 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 Analysis of the situation presented by the ISO 20078 series

6.2.1 SAFE 1: Possible overload of the electronic system of the moving vehicle (numerous requests)

To the question:

“Does the ISO 20078 series generate safety risks related to a possible overload of the electronic system of the moving vehicle in the case of several requests at the same time?”

The answer is NO.

The safety risks related to a possible overload of the electronic system of the moving vehicle in the case of several requests at the same time are only related to the implementation of the ISO 20078 series.

The series reduces these risks because it introduces the interface at the backend server of the manufacturer. However, the ISO 20078 series does not provide any recommendation regarding that implementation. It is suggested that the ISO 20078 series could recommend designing this implementation according to the methodology specified in ISO 20077-2.

The detailed analysis addressing this question can be found in Annex A.

6.2.2 SAFE 2: Possible overload of the electronic system of the moving vehicle (frequent requests)

To the question:

“Does the ISO 20078 series generate risks related to highly frequently repeated requests?”

The answer is NO.

The safety risks related to a possible overload of the electronic system of the moving vehicle in the case of frequently repeated requests are only related to the implementation of the ISO 20078 series.

The series reduces these risks because it introduces the interface at the backend server of the manufacturer. However, the ISO 20078 series does not provide any recommendation regarding that implementation. It is suggested that the ISO 20078 series could recommend designing this implementation according to the methodology specified in ISO 20077-2.

The detailed analysis addressing this question can be found in Annex A.

6.2.3 SAFE 3: Possible overload of the electronic system of the moving vehicle (unexpected requests)

To the question:

"Does the ISO 20078 series generate risks related to unexpected requests?"

The answer is NO.

The safety risks related to a possible overload of the electronic system of the moving vehicle in the case of unexpected requests are only related to the implementation of the ISO 20078 series.

The ISO 20078 concept, by introducing the web-service communication via the back-end server of the vehicle manufacturer, enables a possible substantial reduction of these risks, should the vehicle manufacturer appropriately design this backend server.

It is recommended unexpected requests be denied. However, the ISO 20078 series does not provide any such recommendation. It is suggested that the ISO 20078 series could recommend designing this implementation according to the methodology specified in ISO 20077-2.

The detailed analysis addressing this question may be found in Annex A.

6.2.4 SAFE 4: Possible illicit or malicious remote control of vehicles

To the question:

"Does the ISO 20078 series prohibit illicit or malicious remote control of vehicles, or an illicit or malicious remote activation of systems and components? Actively?"

The answer is NO.

The safety risks related to a possible illicit or malicious remote control of vehicles, or an illicit or malicious remote activation of systems and components are only related to the implementation of the ISO 20078 series.

The ISO 20078 concept, by introducing the web-service communication via the back-end server of the vehicle manufacturer, enables a possible substantial reduction of these risks, should the vehicle manufacturer appropriately design this backend server.

However, the ISO 20078 series introduces concepts that may facilitate the introduction of mechanisms aiming at actively preventing or limiting uncontrolled or malicious remote take of control of vehicles, or an uncontrolled or malicious remote activation of systems and components.

The detailed analysis addressing this question can be found in Annex A.

6.2.5 SAFE 5: Lack of compatibility with the existing systems and mechanisms

To the question:

"Does the ISO 20078 series generate risks related the lack of compatibility with the existing design of the vehicle?"

The answer is NO.

To the question:

“Does the ISO 20078 concept address the risks related to the lack of compatibility with the existing design of the vehicle?”

The answer is YES.

The ISO 20078 concept, by introducing the web-service communication via the back-end server of the vehicle manufacturer, enables a possible substantial reduction of these risks, should the vehicle manufacturer appropriately design this backend server.

The detailed analysis addressing this question can be found in Annex A.

6.2.6 SAFE 6: Failures of the remote communication solution itself of the ExVe (including the back-end system of the manufacturer)

To the question:

“Does the ISO 20078 series generate safety risks in the case when e.g. the back-end server is down (internal failures, hacking, etc…)?”

The answer is NO.

The detailed analysis addressing this question can be found in Annex A.

6.2.7 SAFE 7: Lack of consideration of the complete ExVe life cycle

To the question:

“Does the ISO 20078 series generate safety risks related to requests that are inappropriate in the actual life cycle phase of the running vehicle?”

The answer is NO.

However, such safety issues may occur in the case of a dysfunction of the processes informing the authorization provider of a change of the life cycle stage (manufacturing, sales, operation, maintenance and repair, end of life).

The detailed analysis addressing this question can be found in Annex A.

6.2.8 SAFE 8: Risks related to the design validation process

To the question:

“Does the ISO 20078 series generate safety risks related to the validation of the design process and its traceability?”

The answer is NO.

The detailed analysis addressing this question can be found in Annex A.

6.2.9 SAFE 9: Lack of misuse prevention

To the question:

“Does the ISO 20078 concept permit a limitation of the passed information to avoid safety issues?”

The answer is YES.

To the question:

"Does the ISO 20078 series specify or recommend a limitation of the passed information to avoid safety issues?"

The answer is NO.

Addressing the issue is left by the ISO 20078 series to external actors (for example those involved at the implementation stage of the series or at the specification of the considered use-cases).

The detailed analysis addressing this question can be found in Annex A.

6.2.10 SAFE 10: Lack of, or inappropriate measures aiming at reducing the risks in case of illicit or malicious remote control of vehicles

To the question:

"Does the ISO 20078 series contain mechanisms or processes reducing the safety risks presented by a remote control"?

The answer is YES.

However, the ISO 20078 series only partially addresses these risks because, while there is no guarantee that the accessing party is free from impersonation risks (e.g. ID theft upstream its own accessing request), the ISO 20078 series does not contain any recommendation for considering and possibly limiting these risks (out of scope).

The ISO 20078 concept, by introducing the web-service communication via the back-end server of the vehicle manufacturer, enables a possible substantial reduction of these risks, should the vehicle manufacturer appropriately design this backend server.

The detailed analysis addressing these questions can be found in Annex A.

6.3 Conclusion: Assessment of the safety risks possibly originating from the ISO 20078 series

The analysis of the ISO 20078 series regarding the possible safety risks considered in this document have permitted to demonstrate:

— that the ISO 20078 concept per se, by introducing the concept of communicating via the back-end server of the manufacturer, enables the vehicle manufacturer to endorse its full responsibility for ensuring the safety of the persons and the goods during the ExVe life cycle;

— that the ISO 20078 series does not generate any risk relative to the persons and the goods during the ExVe life cycle;

— that some of the risks relative to the safety of the persons and the goods are related to the way the ISO 20078 series is implemented (see e.g. the arbitration mechanisms) and not to the ISO 20078 series per se (it has not been possible to find a safety risk originating from the ISO 20078 series itself);

— that the ISO 20078 series does not address these implementation risks; in particular, the ISO 20078 series does not recommend any measure that may help preventing these risks, such as, but not limited to the use of the design methodology specified in ISO 20077-2 for designing this implementation.