ISO/TR 23791:2019 (E)

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

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions
3.2 Abbreviated terms

4 General result of the risk assessment

5 Categories of the assessed risks

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
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)
6.2.2 SAFE 2: Possible overload of the electronic system of the moving vehicle (frequent requests)
6.2.3 SAFE 3: Possible overload of the electronic system of the moving vehicle (unexpected requests)
6.2.4 SAFE 4: Possible illicit or malicious remote control of vehicles
6.2.5 SAFE 5: Lack of compatibility with the existing systems and mechanisms
6.2.6 SAFE 6: Failures of the remote communication solution itself of the ExVe (including the back-end system of the manufacturer)
6.2.7 SAFE 7: Lack of consideration of the complete ExVe life cycle
6.2.8 SAFE 8: Risks related to the design validation process
6.2.9 SAFE 9: Lack of misuse prevention
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
6.3 Conclusion: Assessment of the safety risks possibly originating from the ISO 20078 series

7 Assessment of the risks associated to the security of the ExVe communication system

7.1 Security risks considered
7.2 Analysis of the situation presented by the ISO 20078 series
7.2.1 General considerations relative to the specification of the OAuth2 framework
7.2.2 General consideration related to cybersecurity
7.2.3 SEC 1: Risks related to integrity and authenticity
7.2.4 SEC 2: Security risks at vehicle systems that are not located at the moving vehicle
7.2.5 SEC 3: Risks related to the consequences of a complete or partial cybersecurity breach (this includes safety, security, competition, confidentiality and data protection risks)
7.2.6 SEC 4: Lack of misuse prevention measures
7.3 Conclusion: Assessment of the security risks possibly originating from the ISO 20078 series

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

8.1 Competition risks considered

8.2 Analysis of the situation presented by the ISO 20078 series
8.2.1 Involved actors
8.2.2 FAIR 1: Possible misuse of the acquired knowledge
8.2.3 FAIR 2: Possible gaining of unique knowledge of the market through monitoring
8.2.4 FAIR 3: Possible gaining of unique knowledge of the customer's behaviour through monitoring
8.2.5 FAIR 4: Competition risks among the involved parties
8.2.6 FAIR 5: Risk of excluding competitors from playing roles
8.2.7 FAIR 6: Risks related to the development of new after-sales applications
8.2.8 FAIR 7: Competition risks among manufacturers and/or vehicle components (systems) suppliers
8.3 Conclusion: Assessment of the competition risks possibly originating from the ISO 20078 series

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

9.1 Liability and responsibility
9.2 Analysis of the situation presented by the ISO 20078 series
9.3 Conclusion: Assessment of the risks related to the responsibility of the concerned actors possibly originating from the ISO 20078 series

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

10.1 Data protection risks considered
10.2 Analysis of the situation presented by the ISO 20078 series
10.3 Conclusion: Assessment of the risks related to the protection of the resources owned by the resource owner and possibly originating from the ISO 20078 series (data protection risks)

Annex A (informative) Assessment of safety risks

A.1 Possible overload of the electronic system of the moving vehicle (numerous requests)
A.2 Possible overload of the electronic system of the moving vehicle (repeated requests)
A.3 Possible overload of the electronic system of the moving vehicle (unexpected requests)
A.4 Possible illicit or malicious remote control of vehicles (prevention)
A.5 Illicit or malicious remote control of vehicles (reduction of the risks)
A.6 Lack of compatibility with the existing systems and mechanisms
A.7 Failures of the remote communication solution itself of the ExVe (including the VM back-end server)
A.8 Lack of consideration of the complete ExVe life cycle
A.9 Risks related to the design validation process
A.10 Lack of misuse prevention

Annex B (informative) Assessment of security risks

B.1 Cybersecurity risks (general)
B.2 Risks related to integrity and authenticity
B.3 Risks at vehicle systems that are not located at the moving vehicle
B.4 Consequences of a security breach
B.5 Misuse prevention measures

Annex C (informative) Assessment of competition risks

C.1 Possible misuse of the acquired knowledge
C.2 Possible gaining of unique knowledge of the market through monitoring
C.3 Possible gaining of unique knowledge of the customer's behaviour through monitoring
C.4 Competition risks among the involved parties
C.5 Risk of excluding competitors from playing roles
C.6 Risks related to the development of new after-sales applications
C.7 Competition risks among manufacturers and/or vehicle components suppliers

Annex D (informative) Assessment of the risks related to responsibility and liability of the concerned actors

Annex E (informative) Assessment of data protection risks

Page count: 39