

Functional Safety and Cybersecurity Global Requirements

Published By:

Competence Center for Functional Safety and Product
Cybersecurity

Inhaltsverzeichnis

1	Purpose and Objectives	3
2	Scope	3
3	Responsibility	3
4	Terms and Abbreviations	3
5	Requirements	4
6	References	8
7	Revision History	8

1 Purpose and Objectives

The purpose of this document is to specify the general requirements related to compliance to the regulations and standards that emphasize functional safety and product cybersecurity. These include but are not limited to regulations such as the Cybersecurity Resilience Act and standards such as ISO/SAE 21434, ISO 26262, IEC 62443, ISO/IEC 15408, etc.

2 Scope

The requirements specified in this document are applicable for suppliers who are involved in the delivery or development of E/E components that have an influence on the functional safety or cybersecurity of the product

3 Responsibility

The Head of the Competence Center for Functional Safety and Product Cybersecurity of Weber Systems Group is responsible for any updates or changes in this document.

4 Terms and Abbreviations

Abbreviation	Description	Comment (Optional)
RL	Richtlinie	Präfix RL ist im Titel zu berücksichtigen
GDPR	General Data Protection Regulation	
ISO	International Standards Organisation	
SAE	Society of Automotive Engineers	
UN ECE	United Nations Economic Commission for Europe	
CSMS	Cyber Security Management System	
NIST	National Institute of Standards and Technology	
FMEA	Failure Modes and Effects Analysis	

5 Requirements

5.1 Standards and Regulations

Requirement ID	Description
RQ-CS-FUSA-01	For components that will be used within the markets where the European General Data Protection Regulation (GDPR) applies, the GDPR regulation must be checked for applicability and considered during the development process
RQ-CS-FUSA-02	For components that will be used in automotive applications, ISO/SAE 21434 shall be considered during the product lifecycle
RQ-CS-FUSA-03	For components that will be used in automotive applications, ISO 26262 shall be considered during the product lifecycle
RQ-CS-FUSA-04	The supplier shall comply with the cybersecurity resilience act
RQ-CS-FUSA-05	UN-ECE regulation no. 155 shall be taken into consideration and checked for relevance for Components that are used in Automotive applications
RQ-CS-FUSA-06	UN-ECE regulation no. 156 shall be taken into consideration and checked for relevance for Components that are used in Automotive applications
RQ-CS-FUSA-07	The Supplier is obliged to take the national and international standard into account as a draft if it is foreseeable that this is the state of the art or legislation at the time of the start of the production launch of the target model series or at the start of the sale.
RQ-CS-FUSA-08	The Supplier shall comply with Information Security Requirements for Contract partners of Weber Systems Group

5.2 Storage and Transport

Requirement ID	Description
RQ-CS-FUSA-09	The supplier shall ensure that the product/component supplied cannot be stolen during production and transport
RQ-CS-FUSA-10	The supplier shall ensure that the component cannot be manipulated by unauthorized persons during the production and transport

5.3 Product Cybersecurity

Requirement ID	Description
RQ-CS-FUSA-11	The supplier shall name a qualified person as responsible for the topic of Cybersecurity
RQ-CS-FUSA-12	The Supplier shall set up and maintain a Cybersecurity Management System (CSMS)
RQ-CS-FUSA-13	The Supplier shall set up necessary processes to perform monitoring for cybersecurity issues and respond to cybersecurity incidents
RQ-CS-FUSA-14	The Supplier ensures a cybersecurity culture is followed throughout the organization and product security is not compromised during decision making. E.g. Compromising security of the product to cut costs shall be tolerated
RQ-CS-FUSA-15	The supplier shall analyze the Threats and assess the cybersecurity risks due to the threats associated with the Component and its intended use. The outcome of such analysis shall be considered for the complete product lifecycle, with a view to minimizing cybersecurity risks, preventing incidents, and minimizing their impact, including the safety of the users.
RQ-CS-FUSA-16	The supplier shall lock irreversibly all physical manufacturing and/or debug interfaces during manufacture or secure them by cryptographic methods, which shall be reviewed and approved by Weber Systems Group
RQ-CS-FUSA-17	The components that are developed based on Weber Systems Group’s specifications shall only contain the functions and interfaces that are described in the Specifications
RQ-CS-FUSA-18	For the component, a security concept shall be created and presented to Weber System’s Group and shall be agreed upon. The concept must be adapted to every change
RQ-CS-FUSA-19	The supplier shall use tools approved by Weber Systems Group to manage certificates for diagnosis and coding during the production process.
RQ-CS-FUSA-20	The Supplier shall not use free and open-source software to perform design, development, and testing of the component
RQ-CS-FUSA-21	The supplier shall perform sufficient testing to ensure no cybersecurity weaknesses and vulnerabilities exist during design and development
RQ-CS-FUSA-22	The Supplier shall ensure that the cryptographic algorithms used shall be compliant to NIST standards
RQ-CS-FUSA-23	If Cryptographic keys are used in the component, the supplier shall

Requirement ID	Description
	maintain a key management system. The workflow of key generation, transfer and destruction shall be documented.
RQ-CS-FUSA-24	If the supplied component contains software elements, vulnerability scanning reports shall be provided to Weber Systems Group
RQ-CS-FUSA-25	The supplier shall provide cybersecurity support for the entire lifecycle of the Product for which the component is used.
RQ-CS-FUSA-26	During Support, the supplier shall perform vulnerability management for all vulnerabilities identified in the developed components (Software and Hardware) and provide fixes. The supplier shall ensure that no new vulnerabilities or weaknesses are introduced due to the fixes
RQ-CS-FUSA-27	The supplier shall inform the end of cybersecurity support to Weber Systems Group at least one year in advance before the period of support ends
RQ-CS-FUSA-28	During the end of support, the supplier shall provide all the necessary documentation (service guidelines, manuals, fixes or patches for identified issues, detailed incident reports, etc.) to Weber Systems Group
RQ-CS-FUSA-29	In case a cybersecurity incident occurs, the supplier shall support in incident response activities.
RQ-CS-FUSA-30	If any vulnerabilities or weaknesses are identified by the supplier in products supplied to Weber Systems Group, the supplier shall inform within valuable period which will be defined in the Support Agreement.
RQ-CS-FUSA-31	During the period of cybersecurity support, the supplier shall actively monitor for any cybersecurity information regarding the component supplied

5.4 Functional Safety

Requirement ID	Description
RQ-CS-FUSA-32	The supplier shall comply with functional safety requirements according to relevant functional safety norms
RQ-CS-FUSA-33	The supplier shall name a qualified person as responsible for the topic of Functional Safety
RQ-CS-FUSA-34	The supplier shall provide a released and assessed safety case and safety manual to Weber Systems Group
RQ-CS-FUSA-35	The supplier shall implement the Technical Safety requirements forwarded by Weber Systems Group to the component, which is

Requirement ID	Description
	developed based on Weber System Group's specification
RQ-CS-FUSA-36	The supplier shall test the special characteristics provided by Weber Systems Group. The special characteristics must be tested 100 %.
RQ-CS-FUSA-37	The supplier shall test the special characteristics provided internally by the different analyses. The special characteristics must be tested 100%
RQ-CS-FUSA-38	The supplier shall create and establish a Production Control Plan related to the Functional Safety special characteristics. The corresponding reports shall be provided to Weber Systems Group
RQ-CS-FUSA-39	The supplier shall create and establish a Production Process Capability Plan. The corresponding reports shall be provided to Weber Systems Group.
RQ-CS-FUSA-40	The Process FMEA and the corresponding reports shall be provided fully to Weber Systems Group.
RQ-CS-FUSA-41	The supplier shall release all the documentation related to functional safety norms and related to the development and production of the component supplied
RQ-CS-FUSA-42	The supplier shall be part of the assessment and audit and support Weber Systems Group when it comes to the activities related to the qualification of the component when needed.

6 References

1. Informationssicherheitsanforderungen für Vertragspartner

7 Revision History

Rev.	Datum	Bearbeiter	Änderungen
0.1	26.07.2022	Maher Sahli	Document creation
0.2	28.07.2022	Maher Sahli	Updates based on review comment from Mehdi Javdanitehran
0.3	28.07.2022	Maher Sahli	Updates based on review comment from Steffen Walter
1.0	02.08.2022	Maher Sahli	Documentation release
1.1	10.10.2022	Maher Sahli	Requirements ID changed
1.2	12.10.2022	Jasper Paulraj	The general cybersecurity requirements were added.
1.3	18.10.2022	Jasper Paulraj	ReqFusa_CySec_48 added.
1.4	19.10.2022	Maher Sahli	Documentation release
1.5	24.11.2022	Jasper Paulraj	Updates based on the suggestion from Johannes Felk
2.0	25.11.2022	Maher Sahli	Added release date, Requirements ID's corrected, and document release
2.1	23.09.2024	Jasper Paulraj	Title updated to not being specific. ReqFuSa_CySec_16 updated to include all employees.
3.0	30.09.2024	Maher Sahli	New Document version released
3.1	06.03.2025	Jasper Paulraj	Updated to new template. The requirements were adapted to cover the Cybersecurity Resilience Act and less focus to ISO 21434 and Iso 26262. The global requirements are reviewed together with Head of Competence Center for Functional Safety and Product Cybersecurity. New requirement IDs included
4.0	28.03.2025	Jasper Paulraj	New Document Version Released