



**HOLON SUPPLIER QUALITY REQUIREMENTS** | **HSQR REVISION 1.0**

*BETWEEN*

**HOLON GMBH  
HOLON INC.**

*AND*

**SUPPLIER**

HOLON GMBH  
ELSENER STR. 95  
33102 PADERBORN  
GERMANY

E-MAIL [INFO@DRIVEHOLON.COM](mailto:INFO@DRIVEHOLON.COM)  
INTERNET [WWW.DRIVEHOLON.COM](http://WWW.DRIVEHOLON.COM)

<b>Table of Content</b>		<b>Page</b>
1	Preamble.....	1
2	Scope of Application .....	1
3	Quality Management System Requirements .....	1
	3.1 Certification Requirements .....	1
	3.2 Scope and Maintenance of the QMS .....	2
	3.3 Legal and Regulatory Requirements .....	2
	3.4 Quality Targets .....	2
	3.5 Special Process Management.....	2
	3.6 Units and Formats .....	2
4	Product Development Obligations.....	3
	4.1 Development Process Requirements .....	3
	4.2 Feasibility Analysis.....	3
	4.3 Product and Process FMEA .....	3
	4.4 Control Plans .....	4
5	Functional Safety, Cybersecurity, and Software Obligations .....	4
	5.1 Functional Safety (ISO 26262) .....	4
	5.2 Cybersecurity (ISO/SAE 21434) .....	4
	5.3 SOTIF (ISO 21448).....	5
	5.4 System, Software and Hardware Development .....	5
6	Series Production Obligations.....	6
	6.1 Initial Sample Inspection and Approval (PPAP) .....	6
	6.2 PPAP Rejection and Resubmission .....	6
	6.3 Deviation approval .....	7
	6.4 Process Monitoring and Statistical Control .....	7
	6.5 Total Productive Maintenance .....	8
	6.6 Non-Conformance and Problem Solving .....	8
	6.7 Recall .....	9
7	Change Management.....	9
	7.1 Notification and Approval Obligation.....	9
	7.2 Requalification .....	10
8	Risk Management and Escalation Process .....	10
	8.1 General Obligations.....	10
	8.2 Risk Identification and Evaluation .....	10
	8.3 Mitigation and Monitoring.....	11
	8.4 Escalation to OEM .....	11

<b>Table of Content</b>		<b>Page</b>
8.5	Integration with Related Processes.....	11
9	Audits and Assessments.....	12
9.1	Right to Audit .....	12
9.2	Audit Types.....	12
9.3	Supplier Internal Audits and Cooperation Obligations.....	12
10	ESG and Sustainability Requirements .....	13
10.1	General Commitment.....	13
10.2	Environmental Management System .....	13
11	Documentation, Retention, and Traceability.....	13
12	Sub-suppliers and Outsourcing .....	13
13	Duration and Termination .....	14
13.1	Term of the Agreement.....	14
13.2	Termination for Cause.....	14
14	Final Provision .....	14

## 1 Preamble

The HOLON Supplier Quality Agreement (“Agreement”) governs the quality assurance relationship between HOLON GmbH (hereinafter referred to as *OEM*) and Supplier for all supplies, software, and services provided to OEM.

The purpose of this Agreement is to ensure that all products and services delivered by Supplier meet the highest standards of quality, safety, cybersecurity, and compliance throughout the product lifecycle.

The Agreement applies to the development and manufacturing of OEM’s battery-electric, SAE J3016 Level 4 autonomous mover platform, which is intended for use in highly automated public transport environments and privacy-sensitive operational domains. Typical customer groups include municipal or regional public transportation authorities, fleet operators, and private institutions such as airports, campuses, and service providers with high expectations regarding safety, reliability, data protection, and regulatory compliance.

## 2 Scope of Application

This Agreement applies to all purchased parts, assemblies, subsystems, software tools, and services delivered by Supplier to OEM, irrespective of whether they are intended for prototypes, pre-series, series production, service parts, or aftermarket purposes.

The requirements in this document apply in addition to the applicable law and governmental requirements and the general industry standards of the automotive industry described in the ISO 9001 (latest applicable version), IATF 16949 (latest applicable version) and latest applicable volumes from VDA and/or AIAG.

The Supplier shall also be obliged to forward this agreement's content to all sub-suppliers and sub-contractors utilized by Supplier and ensure compliance with the rules and regulations set forth by this Agreement.

## 3 Quality Management System Requirements

### 3.1 Certification Requirements

Supplier shall maintain a Quality Management System (QMS) certified in accordance with IATF 16949 (latest applicable version), which represents the expected standard for all suppliers involved in the design, development, and/or production of serial parts.

In justified cases and subject to OEM’s prior written approval, a QMS certified to ISO 9001 (latest applicable version) may be accepted as a temporary minimum, provided that Supplier submits a documented roadmap outlining specific milestones and timelines for achieving IATF 16949 (latest applicable version) certification.

Certification in either case shall be issued by an accredited certification body in accordance with ISO/IEC 17021 (latest applicable version). Valid certificates shall be provided to OEM upon request and without undue delay.

Any suspension, withdrawal, or change in certification status (including recertification) shall be reported to OEM immediately. To improve communication Supplier shall define a designated contact person for quality topics to OEM.

### **3.2 Scope and Maintenance of the QMS**

Supplier's QMS shall cover all locations involved in the design, development, manufacturing, testing, warehousing, and service of OEM parts.

The QMS shall be regularly reviewed, updated, and improved, ensuring effectiveness through internal audits, management reviews, and corrective actions plans.

### **3.3 Legal and Regulatory Requirements**

Supplier shall ensure compliance to applicable legal and regulatory requirements from country of origin, manufacturing and final delivery, as well as in the supply chain.

### **3.4 Quality Targets**

Supplier shall commit to a zero-defect strategy and embed this principle into all development, production and quality assurance activities. This includes ensuring process robustness, proactive defect prevention through effective risk analysis and control planning and immediate containment and root cause resolution in the event of non-conformities. OEM's expectation of zero defects applies equally to supplier hardware, software, documentation and services. Performance against this objective shall be monitored by agreed KPIs.

### **3.5 Special Process Management**

For production processes classified as "special processes" (where process results cannot be fully verified later through inspection or testing, such as welding, painting, heat treatment, soldering), Supplier shall validate such processes through initial process qualifications (e.g. CQI audits according to AIAG CQI standards or comparable procedures) and keep documentation acc. the VDA1 standard.

### **3.6 Units and Formats**

All date and time entries must follow a standardized format, preferably ISO 8601 (e.g., YYYY-MM-DDThh:mm:ssZ). This ensures consistency across systems and eliminates ambiguity caused by the latest applicable use of mixed and arbitrary formats.

All technical measurements must be documented using the International System of Units (SI). This includes, but is not limited to, units for length (meters), mass (kilograms), time (seconds), temperature (kelvin), and electric latest applicable (amperes). Non-SI units are not permitted unless explicitly justified and converted accordingly.

## 4 Product Development Obligations

### 4.1 Development Process Requirements

Supplier shall perform product development in accordance with a structured, traceable methodology that integrates Advanced Product Quality Planning (APQP) principles with a systems engineering approach. Where applicable – particularly for suppliers contributing to complex E/E systems, functional safety elements, or software components - development shall follow the V-model and support a hierarchical decomposition of stakeholder requirements into technical specifications across all relevant levels (system, sub-system, component).

For such cases, Supplier shall define and maintain system and sub-system architectures, interfaces, and verification strategies in alignment with OEM’s overarching architectural definitions and boundary conditions. Interface responsibilities shall be clearly defined and controlled throughout development. Suppliers delivering components without system-level integration responsibilities remain obligated to provide sufficient technical documentation, traceability, and evidence of conformity to applicable requirements.

At the beginning of the development engagement, Supplier shall align its development scope, interface responsibilities and system boundaries with OEM Supplier Quality. This alignment shall also include an agreement on production release (PPAP) content and timeline (see clause 6.1).

Supplier is obligated to participate in or align with OEM-led system-level risk assessments and engineering safety and cybersecurity activities. This includes ensuring compatibility and consistency between Supplier-developed risk analysis (e.g. Design and Process FMEAs, Fault Trees, DFAs, Safety and Cybersecurity Concepts) and OEM-level analysis, such as Hazard Analysis and Risk Assessment (HARA), Threat Analysis and Risk Assessment (TARA), and Hazard Identification and Risk Evaluation (HIRE). All derived requirements, safety goals, and mitigation strategies resulting from such activities shall be reflected in Supplier’s development artifacts and traceable through to design and test results.

Supplier’s development approach shall ensure compatibility with the latest applicable version of ISO 26262, ISO/SAE 21434, ISO 21448, and Automotive SPICE®, as applicable for the respective product scopes. Evidence of implementation shall be maintained in the form of documented plans, controlled baselines, requirement traceability, risk analysis, verification and test reports, and provided to OEM upon request.

### 4.2 Feasibility Analysis

Upon receipt of OEM specifications, Supplier shall conduct a detailed technical feasibility analysis and submit a formal feasibility declaration before order acceptance.

Identified Risks shall be documented, evaluated, and discussed with OEM.

### 4.3 Product and Process FMEA

Supplier shall prepare a Design Failure Mode and Effects Analysis (DFMEA) and Process Failure Mode and Effects Analysis (PFMEA) per latest applicable version of AIAG-VDA FMEA handbook. FMEAs must be living documents that are continuously updated throughout development and production. Upon request OEM shall be granted access to FMEAs for review.

## 4.4 Control Plans

Supplier shall establish Control Plans linked to the PFMEA covering all production phases (prototype, pre-series, and series). Control Plans shall ensure that critical and significant product characteristics are appropriately marked and monitored. Upon request, OEM shall be granted access to control plans for review.

# 5 Functional Safety, Cybersecurity, and Software Obligations

## 5.1 Functional Safety (ISO 26262)

Supplier shall support OEM's safety lifecycle in accordance with the latest applicable version of ISO 26262 and is responsible for all safety-related activities as structured by the Development Interface Agreement (DIA). This can include the preparation and maintenance of safety plans, confirmation measures, safety concepts and technical safety analysis (e.g. FMEA, FTA, FMEDA).

Where applicable, Supplier shall contribute to OEM's Hazard Analysis and Risk Assessment (HARA) and System Safety Analysis by providing relevant system knowledge, malfunction assessments, and scenario evaluations. Suppliers delivering safety-related systems, subsystems, or Safety Elements out of Context (SEooC) are required to clearly define and communicate the assumptions of use, safety requirements and ASIL allocation on the OEM.

Suppliers are required to deliver the component's Safety Case and Safety Manual in accordance with the Development Interface Agreement (DIA), and to provide the relevant Safety Assessment and Audit reports demonstrating compliance with the designated ASIL level.

## 5.2 Cybersecurity (ISO/SAE 21434)

Supplier shall comply with the requirements of the latest applicable version of ISO/SAE 21434 throughout the entire lifecycle of the supplied product(s), encompassing development, production, operation, and post-production phases. Prior to any development or delivery activities, Supplier agrees to enter into a Cybersecurity Interface Agreement (CIA) with the customer. This Agreement shall define the distributed cybersecurity responsibilities and activities between both parties and must be compliant with the requirements outlined in ISO/SAE 21434.

Furthermore, Supplier shall provide evidence of cybersecurity engineering capabilities in accordance with the latest applicable version of ISO/SAE 21434, including those of their supply chain. In addition, Supplier is required to supply evidence of an Information Security Management System (ISMS), such as an ISO 27001 certification or a TISAX assessment.

To ensure robust cybersecurity assurance, Supplier permits the OEM to conduct validation activities at any time. These may include penetration testing, fuzz testing, and robustness testing, either performed in-house or by accredited third parties. Supplier also ensures cybersecurity support across the product lifecycle, covering vulnerability management, software updates, and end-of-support procedures.

In the event that critical vulnerabilities are detected by any party, Supplier shall mitigate and manage the associated risks. The details of such mitigation efforts shall be governed by a Service Level Agreement. Moreover, Supplier is obligated to notify the OEM within 24 hours of any cybersecurity incident, initiate containment measures, provide a root cause analysis within a reasonable timeframe, and collaborate on resolution and post-incident review, as outlined in section 6.6.

### 5.3 SOTIF (ISO 21448)

Supplier shall support OEM's safety activities in accordance with the agreed Development Interface Agreement (DIA) and the latest applicable version of ISO 21448 (SOTIF) and ensure appropriate risk identification and mitigation. Where relevant, Supplier shall conduct internal scenario analysis and Hazard Identification and Risk Evaluation (HIRE) under defined assumptions of use, analogous to the obligations described in clause 5.1. Resulting safety requirements and assumptions shall be documented and traceable throughout design and validation.

### 5.4 System, Software and Hardware Development

Supplier shall perform software development in accordance with Automotive SPICE® (latest applicable version) process reference model, ensuring a structured, traceable, and quality-assured lifecycle. All relevant process areas – including:

- System (SYS), software (SW) and hardware (HW) requirements
- SYS, SW and HW Architectural Design
- SW Detailed Design and Unit Construction
- SYS, SW Integration
- SYS, SW and HW Verification
- Validation
- Supporting Process such as Quality Assurance, Configuration Management, Problem Resolution Management and Change Management
- Management Process such as Project Management and Risk Management, Product Release, Supplier Monitoring

shall be executed at a maturity level of Capability Level 2, 9 months after the project was kicked off but not later than PPAP submission, unless otherwise agreed in writing with OEM Quality Assurance. The ASPICE assessment shall be performed at least by an internal ASPICE Competent Assessor who is independent of the project. OEM may participate as Observer in the ASPICE Assessment when necessary and shall have access to the ASPICE Assessment results.

In addition to ASPICE, Supplier shall ensure compliance with applicable standards relevant to the software's safety, cybersecurity, and functionality context. This includes, but is not limited to, ISO 26262 for functional safety ISO/SAE 21434 for cybersecurity, ISO/PAS 8800 for safety and artificial intelligence, and ISO 21448 for SOTIF. Where software is safety – or security – relevant, Supplier shall ensure that associated software safety requirements, ASIL decomposition, cybersecurity goals, and mitigations are properly implemented and validated.

Furthermore, Supplier shall ensure that software is developed in accordance with state-of-the-art industry guidelines such as MISRA-C++, or AUTOSAR C++14. Deviations from such coding standards need to be justified and documented, and the deviation management shall be subject to review and approval by Supplier's quality assurance function.

OEM reserves the right to assess Supplier's system, software and hardware development activities, including architecture, traceability, verification, and coding practices, and to request supporting documentation at any time during the development lifecycle.

## 6 Series Production Obligations

### 6.1 Initial Sample Inspection and Approval (PPAP)

Before serial deliveries, Supplier shall complete Production Part Approval Process (PPAP) submissions at the defined level (default Level 3) according to AIAG standards. If Supplier products are developed in accordance with VDA MLA (see clause 4.1), a validation according to VDA Production Process and Product Approval (PPA) can be acceptable. The PPAP process shall be reinitiated after interruption of delivery for more than 12 months or after a high impacted change upon OEMs request.

Unless otherwise specified, a Level 3 PPAP submission is required. Sample parts that are used for PPAP testing need to come out of a series ready process. Process capabilities shall be confirmed by means of a documented production trial run. OEM reserves the right to participate in or initiate and conduct such trial runs. The PPAP shall be submitted in advance of the defined project milestone and must be approved in writing by OEM before any delivery of serial parts is permitted. PPAP inspection time at OEM shall be considered in the planning.

If the delivery of a component is interrupted for 12 months or longer, Supplier shall obtain a new PPAP release from OEM before resuming deliveries. The scope of the re-release shall be defined and agreed with OEM based on the nature of the product and any changes in manufacturing, testing, or regulatory conditions during the suspension period.

In addition, Supplier shall implement a program of periodic requalification for all series-supplied parts and processes, regardless of whether any change, complaint, or field failure has occurred. The requalification shall be conducted according to a schedule defined by Supplier and accepted by OEM before initial PPAP. Upon request, Supplier needs to hand over the requalification documentation to OEM.

Deviations from OEM specifications, which are not detectable during the Production Part Approval Process (PPAP), do not discharge Supplier from his obligation and authorize OEM to reject the products later.

### 6.2 PPAP Rejection and Resubmission

If the submitted PPAP is rejected by OEM, Supplier shall initiate immediate containment actions and perform a structured root cause analysis to identify the reason for non-approval. A written summary of the root cause and proposed corrective measures shall be submitted to OEM within five (5) business days of receiving the rejection notice.

Based on the nature and severity of the non-conformities, OEM may - at its sole discretion - grant a conditional release for a limited volume, timeframe, or application. A conditional release shall only be issued in writing by OEMs Supplier Quality and shall be subject to:

- Clearly defined temporary measures or risk mitigations,
- Specific validation or inspection requirements,
- Traceability of released batches or parts, and
- A documented action plan with a committed timeline for full PPAP resubmission and closure.

Supplier remains fully responsible for all deliveries made under conditional release and for ensuring compliance with the agreed conditions. OEM reserves the right to suspend conditional release at any time if risk levels increase or actions are not executed as agreed.

Following OEM review and agreement on the proposed corrective actions, Supplier shall update and resubmit the PPAP documentation in accordance with the revised timeline and scope communicated by OEM.

If a rejection is due to repeated or systematic deficiencies, OEM reserves the right to impose additional oversight measures, including enhanced audits, third-party support, or escalation under clause 8.

No Series delivery or vehicle integration shall proceed until the PPAP has been formally approved by OEM.

### 6.3 Deviation approval

Any deviation from the agreed specifications, drawings, materials, processes, or quality requirements must be approved in writing by OEM prior to implementation. The Supplier shall submit a formal deviation request, using OEM's required template, including:

- Clear description of the deviation, including affected parts, processes, or documentation.
- Reason for deviation and its necessity.
- Risk assessment covering potential impact on product function, safety, durability, regulatory compliance, and customer satisfaction.
- Proposed containment and corrective actions, including the planned duration of the deviation and revalidation steps after its expiry.

Deviation approval is granted at OEM's sole discretion and shall be limited to the scope, quantity, and period explicitly stated in the approval document. Any products manufactured or delivered without a valid written deviation approval shall be considered nonconforming and subject to rejection, return, or other contractual remedies.

The Supplier is responsible for ensuring that all relevant internal and external parties are informed of the approved deviation and that it is fully traceable in production, inspection, and delivery documentation.

### 6.4 Process Monitoring and Statistical Control

Supplier shall monitor and control all production processes to ensure consistent compliance with OEM's quality requirements and to prevent the occurrence of non-conformities. For product and process characteristics classified as special or critical, Supplier shall apply appropriate statistical process control (SPC) methods to demonstrate process stability and capability.

During the initial production and launch phase, when volumes are insufficient to generate statistically significant data for full SPC analysis, Supplier shall implement an interim capability verification approach. This approach shall include where applicable:

- Machine capability studies (e.g.,  $C_m$ ,  $C_{mk}$ ) or short-term capability indices,
- Verification of tooling and fixture repeatability and reproducibility (R&R),
- 100% inspection or tightened sampling to mitigate unknown variation risk,
- First-off / last-off verification routines for each production shift or batch,
- Increased audit frequency for manufacturing and inspection processes.

As production volumes increase to a level sufficient for statistical evaluation, Supplier shall transition to long-term process capability studies with a minimum requirement of  $C_{pk} \geq 1.67$  for critical characteristics and  $C_{pk} \geq 1.33$  for significant characteristics, unless otherwise agreed with OEM Supplier Quality.

Control limits shall be reviewed and adjusted based on actual process performance, and any process showing trends toward non-conformance must trigger documented corrective action. All process monitoring and capability verification results shall be retained and made available to OEM upon request.

## 6.5 Total Productive Maintenance

Supplier shall establish, maintain, and continuously improve a Total Productive Maintenance (TPM) system to ensure reliability, availability, and capability of all production equipment used in manufacturing products for OEM. The TPM system shall include, at a minimum:

- Preventive and predictive maintenance plans for all critical production and inspection equipment, based on OEM requirements, manufacturer recommendations, and historical performance data.
- Documented maintenance schedules defining frequency, responsible personnel, and specific tasks to be performed.
- Condition monitoring and early-warning systems to detect wear, drift, or impending equipment failure, preventing unplanned downtime and quality defects.
- Maintenance records and traceability retained acc. VDA Volume 1, including details of performed tasks, replaced components, calibration results, and downtime incidents.
- OEE (Overall Equipment Effectiveness) monitoring to measure and improve equipment performance over time.
- Verification of equipment readiness after maintenance or repair, including process requalification where applicable.

Any equipment failure or maintenance-related quality risk affecting parts for OEM shall be reported immediately, along with proposed containment and corrective actions.

## 6.6 Non-Conformance and Problem Solving

In the event of product or process non-conformity – either identified by Supplier or OEM - Supplier shall initiate immediate containment actions to protect OEM operations and inform OEM of the incident without due delay.

Based on severity, complexity, and associated risk, OEM reserves the right to determine the appropriate problem-resolution method. One of the following three formats shall be required:

1. **8D Problem Solving Report (8D-Report)** – Required for complex, safety-related, regulatory, or recurring issues or issues with a high potential impact on Quality, Time, Cost (QTC). The report shall follow the structure and methodology outlined in the VDA Volume “8D-Problem Solving in 8 Disciplines”. Unless otherwise agreed the following response times apply:
  - **D3** within 24 hours
  - **D4** within 5 working days
  - **D8** within 20 working days

Until 8D report is not accepted by OEM all interim measures are to be maintained. Any delays must be proactively communicated and justified to OEM contact of the complaint in writing. Delays can only be accepted after alignment with the responsible OEM Supplier Quality and, if needed, OEMs Warranty Department.

2. **Short Problem-Solving Report (SPS-Report)** – Required for issues of limited complexity and risk. The S-Report shall be structured as follows:

- **SPS-1 – Problem Description:** due within 24 hours
- **SPS-2 – Immediate Containment Actions:** due within 24 hours
- **SPS-3 – Root Cause Analysis:** due within 5 working days
- **SPS-4 – Corrective Actions Implemented:** due within 10 working days

Any delays must be proactively communicated and justified to OEM contact of the complaint in writing. Delays can be accepted after alignment with the responsible OEM Supplier Quality.

**Sorting actions** – If a sorting action is required to maintain production, OEM will, within the scope of its cost-minimization obligation, carry out the sorting action independently or commission it. The resulting costs will be subsequently invoiced to Supplier. Supplier waives his right to a second approach with respect to sorting activities.

**Written Statement** – For clearly understood, low-risk issues with immediate and verified containment, a brief written explanation describing the issue, cause, and closure may be accepted at OEM’s discretion. No structured format is required, but the statement shall be traceable, technically justified, and approved by the responsible OEM contact.

Supplier shall use OEM’s standard **8D / SPS Problem Solving Template** for all non-conformance investigations unless otherwise instructed. OEM will communicate the required reporting format based on the circumstances of each incident.

Use of “D” step designations is reserved exclusively for formal 8D reports to avoid confusion with the simplified S-Report structure. OEM reserves the right to assess the completeness and effectiveness of submitted responses and may require escalation in accordance with clause 8 if issues are not resolved to OEM’s satisfaction.

## 6.7 Recall

Given the critical importance of safety and compliance in public transportation, Supplier acknowledges that any recall actions, field measures, or safety-related service campaigns linked to its products or services are of highest relevance. In such cases, Supplier shall provide a dedicated contact with immediate and full support in root cause analysis, corrective actions, and execution of the recall, and shall bear all direct and indirect costs arising thereof, in accordance with the contractual provisions.

## 7 Change Management

Supplier shall establish, maintain, and continuously improve a change management process that ensures full traceability and uninterrupted delivery of conforming products. This process must proactively identify, assess, and control changes to prevent disruptions in supply and maintain compliance with all relevant quality requirements.

### 7.1 Notification and Approval Obligation

Supplier shall inform OEM in writing of any intended changes affecting the product, software, material, process flow, production equipment, test methods, manufacturing location, or supply chain. Changes shall not be implemented without prior OEM written approval.

Planned changes to the product or process must be notified to OEM within a sufficient period, but in general 6 months in advance. In case of unplanned changes or special situations (see VDA Volume 2 Attachment 8) the Supplier must communicate these immediately to the persons responsible for Supplier Quality at the OEM and ask for agreement.

## 7.2 Requalification

Changes approved by OEM may necessitate partial or full requalification (e.g. repeated PPAP, new process validation) based on OEM's evaluation.

## 8 Risk Management and Escalation Process

Supplier shall establish, maintain, and continuously improve a risk-management and escalation process that ensures early identification, assessment, and mitigation of risks. The process shall include defined escalation paths to address critical issues promptly, preventing supply disruptions and ensuring compliance with all applicable requirements.

### 8.1 General Obligations

The Risk Management process must be documented and aligned with IATF 16949 and ISO 31000 principles. Where applicable, the process shall also reflect the risk-based requirements defined in Automotive SPICE®, ISO 26262 (Functional Safety), ISO/SAE 21434 (Cybersecurity), and ISO 21448 (SOTIF). The process shall cover the full product lifecycle — from concept and development through industrialization, serial production, service, and end-of-life. It shall be applied consistently to manage risks related to quality, performance, safety, cybersecurity, schedule, and regulatory compliance.

The Risk Management process shall include, but not limited to, defined roles and responsibilities, criteria for risk acceptance, documentation requirements, and periodic review mechanisms.

Supplier shall establish and maintain Contingency Plans to ensure the continuity of supply in the event of production disruptions, IT outages, cyberattacks, natural disasters, pandemic events, or other critical incidents.

### 8.2 Risk Identification and Evaluation

Supplier shall proactively identify and assess risks throughout the lifecycle of the supplied product or service. Risk identification shall include, but not limited to, technical risks, interface risks, supply chain risks, functional safety and cybersecurity threats, homologation constraints, and change-related uncertainties.

Identified risks shall be evaluated using a structured method based on severity, probability, and controllability or detectability. Product-specific risks shall be supported by formal analyses such as Design FMEA, Process FMEA, Hazard Analysis and Risk Assessment (HARA), Threat Analysis and Risk Assessment (TARA), Hazard Identification and Risk Evaluation (HIRE) where applicable. These analyses shall be aligned with OEM-led system-level assessments, and Supplier results shall be made available to OEM upon request.

### 8.3 Mitigation and Monitoring

Supplier shall define appropriate mitigation actions for identified risks, assign responsible parties, and monitor the implementation and effectiveness of those actions. Mitigation strategies shall be selected in accordance with best practices (e.g., avoidance, reduction, transfer, or acceptance) and justified in the risk documentation.

Mitigation actions shall be reviewed within ten (10) business days of new risk identification or major project changes. Effectiveness metrics (e.g., risk reduction index, residual risk score) shall be tracked via a risk KPI dashboard and shared upon OEM request. Lessons learned from risk mitigations shall be captured and reused in future projects.

### 8.4 Escalation to OEM

Supplier shall, without undue delay, escalate risks to OEM when any of the following conditions apply:

- The risk could impact product safety, legal compliance, or cybersecurity integrity.
- The risk has the potential to delay project milestones or SOP-critical activities.
- A mitigation strategy cannot be defined or implemented in time.
- Residual risk remains high despite mitigation efforts.

In such cases, or in case Supplier classifies a risk as “high” or “critical”, escalation shall be initiated within 24 hours. For all other risks that Supplier is unable to control or resolve internally through its standard risk management process, escalation shall occur within five (5) days.

Escalated risks shall be communicated in writing and include a short summary, a severity level, latest applicable risk status, risk owner, applied or proposed mitigation actions and an expected timeline. OEM reserves the right to request additional information, imposing further actions, or initiate joint risk reviews as needed. Preferred communication channels are OEM’s Quality Portal or designated risk contact email.

OEM reserves the right to provide, implement or request external support by the OEM Supplier Quality or another authorized person.

During an escalation, it may also be necessary for outgoing deliveries to undergo additional inspection. This can be done as part of a so-called Controlled Shipment (CS Level) or other procedure defined by Supplier and agreed with OEM Supplier Quality.

### 8.5 Integration with Related Processes

Risk Management shall be integrated with Supplier’s broader quality and engineering processes. This includes Change Management (to assess and manage change-related risks), Configuration Management (to ensure traceability of affected versions), and Problem Management (to evaluate risk if an issue has materialized). Risk-related records and outcomes shall also inform lessons-learned reviews and continuous improvement activities.

## 9 Audits and Assessments

### 9.1 Right to Audit

OEM reserves the right to conduct audits and assessments (hereafter “audits”) or request third-party assessments at the Supplier’s facilities, as well as at sub-suppliers locations involved in fulfilling OEM contracts, to verify compliance with the requirements defined in this or other applicable contractual agreements. These audits may include, but are not limited to, quality system audits, process audits, product audits, environmental and sustainability assessments, and regulatory compliance verifications.

Supplier acknowledges that audits are an essential part of OEM’s supplier evaluation and sourcing process and that audit outcomes may influence sourcing decisions.

OEM shall generally provide a written notice period of at least four (4) weeks prior to the audit date. However, Supplier acknowledges and agrees to accept shorter notification periods when visits are required to address acute risks, ensure project continuity, or respond to official inquiries or mandates issued by authorities like Federal Transportation Authorities (e.g. Kraftfahrtbundesamt) or comparable bodies.

During such audits, Supplier shall grant OEM and its designated representatives’ full access to relevant areas, processes, documentation, and personnel necessary to perform the audit. Supplier shall bear its own costs associated with participation and corrective actions, unless otherwise agreed.

### 9.2 Audit Types

OEM may initiate various types of audits depending on the nature of the product, associated risks, and applicable standards. These include:

- System Audits to verify compliance with management standards like IATF 16949 / ISO 9001, ISO 26262, ISO/SAE 21434, and other related frameworks like Automotive SPICE® as applicable.
- Process Audits to assess the effectiveness and control of development, manufacturing, testing, logistics, or support processes.
- Product Audits to evaluate the conformity of delivered goods or services against specifications, drawings, or standards.
- Regulatory and Special Audits are required to fulfill legal, environmental, sustainability, or governmental obligations such as cost analysis.

The audit scope, objectives, and potential findings shall be communicated to the Supplier during a formal opening session. Audit results shall be documented in a written report issued by OEM. OEM may classify findings by severity and require corresponding containment, corrective, and preventive actions.

### 9.3 Supplier Internal Audits and Cooperation Obligations

Supplier shall maintain an internal audit program in accordance with its QMS, ensuring regular reviews of process performance, product conformity, and regulatory compliance. Audit frequency and scope shall be risk-based and aligned with IATF 16949 / ISO 9001 (latest applicable version) and any additional applicable standards relevant to Supplier’s scope of supply.

Upon request Supplier shall cooperate fully with OEM in any follow-up actions derived from audits, including joint root cause analyses, tracking of mitigation measures, and confirmation of implementation status. Failure to cooperate with justified audit requests or to implement corrective actions in a timely manner may lead to escalation measures, including enhanced oversight, sourcing restrictions, or disqualification.

## 10 ESG and Sustainability Requirements

### 10.1 General Commitment

Supplier shall operate in accordance with recognized principles of environmental protection, social responsibility, and ethical corporate governance, and shall ensure that their own supply chain reflects the same commitment. This includes, at a minimum, compliance with all applicable laws and regulations regarding environmental impact, labor and human rights, occupational health and safety, anti-corruption, and responsible sourcing of raw materials.

### 10.2 Environmental Management System

Supplier is expected to maintain an Environmental Management System certified to ISO 14001 (latest applicable version) or an equivalent standard, or to demonstrate active implementation of environmental risk management practices. Upon request, Supplier shall provide relevant documentation on environmental targets, energy usage, emissions, waste reduction measures, and materials compliance (e.g., REACH, RoHS, WEEE).

## 11 Documentation, Retention, and Traceability

Supplier shall maintain complete documentation of all quality-relevant records, including design documents, risk analyses, safety work products, audit reports, and PPAP submissions.

Such records shall be retained in accordance with the defined retention periods of VDA Volume 1 (latest applicable version). At minimum until end of vehicle life or 15 years.

The Supplier shall implement traceability systems ensuring that all critical parts and software components can be traced to their manufacturing batch, version, supply chain, and applied processes.

## 12 Sub-suppliers and Outsourcing

Supplier may only subcontract development, production, or test activities relevant to OEM deliverables with the prior written approval of OEM.

Supplier remains fully responsible for the quality, compliance, and performance of all sub-suppliers and outsourced activities, regardless of OEM approval.

Supplier shall monitor and audit its sub-suppliers regularly to ensure that their Quality, Functional Safety and Cybersecurity Management System, and compliance obligations align with those required by this Agreement.

## **13 Duration and Termination**

### **13.1 Term of the Agreement**

This Agreement enters into force on the date of signature by both parties and shall remain valid for the duration of the commercial relationship between OEM and Supplier unless superseded or terminated in accordance with this Agreement.

### **13.2 Termination for Cause**

OEM may terminate this Agreement with immediate effect if Supplier materially breaches any obligation of this Agreement, including, but not limited to, persistent delivery of non-conforming products, failure to implement corrective actions, loss of certification, or insolvency.

In case of termination, Supplier shall immediately return or destroy all confidential OEM documents and data and certify such destruction upon request.

## **14 Final Provision**

This Agreement constitutes the entire agreement between the parties regarding the subject matter and supersedes all prior agreements, oral or written. Amendments and modifications of this Agreement shall be made in writing and signed by authorized representatives of both parties.

If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall remain in full force and effect. The invalid provision shall be replaced by a valid provision that most closely approximates the intended economic purpose.