ISO 26262 Part 3 - Item Definition Review Report

Review conducted on: 2025-09-29 10:34:47

Review Summary

|  |  |
| --- | --- |
| Total Requirements Reviewed: | 31 |
| Passed: | 17 |
| Failed: | 5 |
| Partially Passed: | 6 |
| **Compliance Rate:** | **54.8%** |

Detailed Review Results

Identification and Classification

This section ensures that the item is uniquely identified within the system architecture or documentation and properly classified (e.g., as hardware, software, or a system function). This supports traceability from high-level safety goals down to detailed design elements. Clear identification also enables effective configuration management and version control throughout the development lifecycle. It is a foundational element for ensuring structured functional safety development.

Identification and Classification – Item 1

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_001 |
| **Requirement:** | Unique Identification of the Item |
| **Description:** | The item shall be uniquely identified in the system architecture or documentation. |
| **Status:** | Pass |
| **Comment:** | The Item Definition clearly states "Item ID: WIPER\_SYS\_001". |
| **Hint for Improvement:** | None.  --- |

Identification and Classification – Item 2

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_002 |
| **Requirement:** | Define Item Type |
| **Description:** | The type of the item (e.g., hardware component, software module, function) shall be clearly defined. |
| **Status:** | Pass |
| **Comment:** | The Item Definition describes the "Windscreen Wiper System" which encompasses hardware (motor, linkage, blades, stalk, pump) and potentially software. This is sufficiently defined for the concept phase. |
| **Hint for Improvement:** | None.  --- |

Identification and Classification – Item 3

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_003 |
| **Requirement:** | ASIL Decomposition Justification |
| **Description:** | If applicable, the ASIL level assigned to the item shall be justified through decomposition from the system-level ASIL. |
| **Status:** | Fail |
| **Comment:** | The Item Definition states "Applicable ASIL: ASIL A (based on HARA)". However, there is no justification or explanation of how this ASIL A was derived or if it's a result of decomposition from a higher system-level ASIL. |
| **Hint for Improvement:** | Provide a brief explanation or reference to the HARA document that details the ASIL determination and any decomposition activities.  --- |

Identification and Classification – Item 4

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_004 |
| **Requirement:** | Traceability of Safety Requirements |
| **Description:** | Safety requirements relevant to the item shall be traceable from safety goals. |
| **Status:** | Partial Pass |
| **Comment:** | The Item Definition lists "Derived Safety Goals (from HARA)" and then "Safety Mechanisms (Preliminary)". While the safety goals are stated, the direct traceability of specific safety requirements \*derived from\* these goals and \*allocated to\* the item is not explicitly detailed. The safety mechanisms are preliminary and not yet defined as requirements. |
| **Hint for Improvement:** | Explicitly state that safety requirements will be derived from the listed safety goals and will be allocated to the item. A table linking safety goals to preliminary safety requirements would be beneficial.  --- |

Identification and Classification – Item 5

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_005 |
| **Requirement:** | Version Control Application |
| **Description:** | A version control system shall be applied to manage changes to the item definition. |
| **Status:** | Pass |
| **Comment:** | The Item Definition includes "Version: 1.0" and "Date: April 5, 2025", indicating version control is being applied. |
| **Hint for Improvement:** | None.  --- |

Identification and Classification – Item 6

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_006 |
| **Requirement:** | Scope Definition |
| **Description:** | The scope of the item shall be clearly defined, including what is included and excluded. |
| **Status:** | Pass |
| **Comment:** | Section 8, "Scope and Boundaries," clearly defines what is included ("wiper motor, linkage mechanism, wiper blades, control stalk, washer pump, and associated wiring. It also includes any embedded software responsible for control logic (if applicable).") and excluded ("Rain sensor hardware/software (if part of a separate item/system). Body Control Module (BCM), though it may interact with this system. Windshield washer reservoir (considered an external component)."). |
| **Hint for Improvement:** | None.  --- |

Functional Description

This section describes the expected behavior of the item under all operating conditions, including normal, degraded, and fault modes. It includes definitions of interfaces, timing constraints, and performance requirements. A well-defined functional description is essential for identifying potential failure scenarios and serves as input to hazard analysis. It helps ensure that all relevant behaviors are considered when deriving safety requirements.

Functional Description – Item 1

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_007 |
| **Requirement:** | Functionality Description |
| **Description:** | The functionality of the item shall be described clearly and unambiguously. |
| **Status:** | Pass |
| **Comment:** | Section 1, "Purpose and Functionality," provides a clear description of the system's purpose and lists its operational modes and activation methods. |
| **Hint for Improvement:** | None.  --- |

Functional Description – Item 2

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_008 |
| **Requirement:** | Interface Specification |
| **Description:** | All interfaces (inputs, outputs) shall be clearly defined, including data types, ranges, and timing constraints. |
| **Status:** | Partial Pass |
| **Comment:** | Section 2, "Interfaces," lists internal and external interfaces. However, it does not specify data types, ranges, or timing constraints for these interfaces. For example, "Stalk Control Input" is mentioned, but the specific signals or data values are not defined. |
| **Hint for Improvement:** | For each interface, specify the type of signal (e.g., digital, analog), expected data values or ranges, and any relevant timing characteristics (e.g., update rate, latency).  --- |

Functional Description – Item 3

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_009 |
| **Requirement:** | Behavior Under All Conditions |
| **Description:** | The behavior of the item under all operating conditions, including fault conditions, shall be described. |
| **Status:** | Partial Pass |
| **Comment:** | Section 1 describes normal operating conditions and modes. Section 6, "Safety-Related Attributes," lists identified hazards and derived safety goals, which touch upon fault conditions. However, a comprehensive description of the item's behavior \*under\* these fault conditions is not fully detailed. For instance, what happens when the motor driver output fails? |
| **Hint for Improvement:** | Expand on the behavior of the system when specific faults occur. For example, if the motor driver fails, does the system attempt a safe state?  --- |

Functional Description – Item 4

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_010 |
| **Requirement:** | Error Handling Description |
| **Description:** | The error handling mechanisms of the item shall be described. |
| **Status:** | Partial Pass |
| **Comment:** | Section 6, "Safety-Related Attributes," lists "Safety Mechanisms (Preliminary)" which include diagnostic checks and CAN signal timeout detection. These are indicative of error handling, but a detailed description of \*how\* these mechanisms handle errors and what actions are taken is missing. |
| **Hint for Improvement:** | Elaborate on the specific error handling strategies for each identified hazard or fault. For example, what is the response to a motor current draw outside the expected range?  --- |

Functional Description – Item 5

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_011 |
| **Requirement:** | Operational Mode Specification |
| **Description:** | Operational modes (normal, degraded, fault, startup, etc.) shall be specified. |
| **Status:** | Pass |
| **Comment:** | Section 1, "Purpose and Functionality," and Section 5, "Operational Modes," clearly define the normal operational modes (Off, Intermittent, Low Speed, High Speed, Single Wipe, Wash & Wipe). Degraded or fault modes are not explicitly detailed as distinct operational modes but are alluded to in the safety attributes. |
| **Hint for Improvement:** | While not strictly required at this stage, consider briefly mentioning potential degraded modes if they are anticipated.  --- |

Functional Description – Item 6

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_012 |
| **Requirement:** | Temporal Aspects Definition |
| **Description:** | Timing constraints such as latency, jitter, and deadlines shall be clearly stated where relevant. |
| **Status:** | Fail |
| **Comment:** | Section 1 mentions "set intervals" for intermittent mode, and Section 5 specifies cycle rates for low and high speeds. However, specific timing constraints like latency, jitter, or precise deadlines for critical operations are not defined. |
| **Hint for Improvement:** | Quantify the timing requirements for critical functions. For example, specify the maximum acceptable latency for responding to a driver input or the maximum interval for the intermittent mode.  --- |

Functional Description – Item 7

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_013 |
| **Requirement:** | Performance Requirements |
| **Description:** | Performance requirements such as response time and accuracy shall be defined. |
| **Status:** | Partial Pass |
| **Comment:** | Section 5 provides cycle rates for wiper speeds, which are a form of performance. However, other performance aspects like the accuracy of the intermittent interval or the response time to a manual command are not explicitly defined. |
| **Hint for Improvement:** | Define specific performance metrics, such as the maximum response time from stalk activation to wiper movement, or the tolerance for the intermittent wipe interval.  --- |

Safety-Related Attributes

This section captures key safety-related properties such as safety goals, mitigation strategies, diagnostic coverage, and safe state definitions. These attributes are derived from the Hazard Analysis and Risk Assessment (HARA) and form the basis of the functional safety concept. They guide the implementation of safety mechanisms and define how the item contributes to overall system safety. Proper documentation ensures alignment with ISO 26262 expectations for safety integrity.

Safety-Related Attributes – Item 1

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_014 |
| **Requirement:** | Linking Safety Goals |
| **Description:** | Safety goals relevant to the item shall be clearly stated. |
| **Status:** | Pass |
| **Comment:** | Section 6, "Safety-Related Attributes," clearly lists "Derived Safety Goals (from HARA)" with their respective ASILs. |
| **Hint for Improvement:** | None.  --- |

Safety-Related Attributes – Item 2

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_015 |
| **Requirement:** | Identification of Safety Mechanisms |
| **Description:** | Safety mechanisms implemented in the item shall be identified and described. |
| **Status:** | Pass |
| **Comment:** | Section 6, "Safety-Related Attributes," lists "Safety Mechanisms (Preliminary)" such as watchdog timers, diagnostic checks, end-of-travel sensors, and CAN signal timeout detection. |
| **Hint for Improvement:** | While these are preliminary, it would be beneficial to briefly describe the intended function of each mechanism in relation to the safety goals.  --- |

Safety-Related Attributes – Item 3

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_016 |
| **Requirement:** | Fault Tolerance Capability |
| **Description:** | The item's fault tolerance capability shall be described if applicable. |
| **Status:** | Fail |
| **Comment:** | The Item Definition does not explicitly describe the fault tolerance capabilities of the Windscreen Wiper System. While some safety mechanisms are listed, their contribution to fault tolerance is not detailed. |
| **Hint for Improvement:** | Describe how the system is designed to tolerate specific faults and maintain safe operation or transition to a safe state. For example, if the motor driver fails, is there a redundant path or a mechanism to prevent unintended movement?  --- |

Safety-Related Attributes – Item 4

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_017 |
| **Requirement:** | Diagnostic Coverage Definition |
| **Description:** | Diagnostic coverage for the item shall be defined and justified if applicable. |
| **Status:** | Fail |
| **Comment:** | Section 6 mentions "Diagnostic checks for wiper motor current draw," but there is no definition or justification of the diagnostic coverage achieved by these or any other diagnostics. |
| **Hint for Improvement:** | For each safety mechanism that provides diagnostics, define the target diagnostic coverage and provide a justification for how this coverage is achieved.  --- |

Safety-Related Attributes – Item 5

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_018 |
| **Requirement:** | Hazard Mitigation Strategy |
| **Description:** | Mitigation strategies for identified hazards shall be linked to this item. |
| **Status:** | Partial Pass |
| **Comment:** | Section 6 lists "Identified Hazards" and "Derived Safety Goals." The "Safety Mechanisms (Preliminary)" can be considered as initial mitigation strategies. However, the explicit linking of each hazard to its specific mitigation strategy within the item is not fully elaborated. |
| **Hint for Improvement:** | Create a clear mapping between each identified hazard and the corresponding safety goal and preliminary safety mechanism(s) that mitigate it.  --- |

Safety-Related Attributes – Item 6

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_019 |
| **Requirement:** | Safe State Behavior |
| **Description:** | The safe state or fallback behavior of the item in case of failure shall be defined. |
| **Status:** | Fail |
| **Comment:** | The Item Definition does not explicitly define the safe state or fallback behavior of the Windscreen Wiper System in case of failure. |
| **Hint for Improvement:** | Clearly define what constitutes a safe state for the wiper system. For example, is it to stop in the park position, or to deactivate completely?  --- |

Dependencies and Interactions

This section identifies internal and external dependencies, including interactions with other systems, environmental influences, and user inputs. Understanding these relationships is critical for defining correct assumptions and boundary conditions during development. It also supports the identification of potential interference or integration risks that could impact safety. Accurate documentation ensures robust interface management and system integration.

Dependencies and Interactions – Item 1

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_020 |
| **Requirement:** | Dependency Identification |
| **Description:** | All dependencies on other items shall be clearly identified. |
| **Status:** | Pass |
| **Comment:** | Section 4, "Dependencies and Assumptions," clearly lists dependencies such as "Availability of electrical power from vehicle battery," "Proper operation of wiper stalk and rain sensor (if present)," and "Sufficient washer fluid level." |
| **Hint for Improvement:** | None.  --- |

Dependencies and Interactions – Item 2

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_021 |
| **Requirement:** | Interaction Description |
| **Description:** | All interactions with other items shall be clearly described. |
| **Status:** | Pass |
| **Comment:** | Section 2, "Interfaces," describes interactions with the "Stalk Control Input," "Rain Sensor Input," "Washer Fluid Pump," "Motor Driver Output," "CAN Communication," "Driver (User)," "Vehicle Electrical System," "Windscreen Washer Reservoir," and "Body Control Module (BCM)." |
| **Hint for Improvement:** | None.  --- |

Dependencies and Interactions – Item 3

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_022 |
| **Requirement:** | External Influences Consideration |
| **Description:** | External influences such as driver inputs and environmental factors shall be considered and documented. |
| **Status:** | Pass |
| **Comment:** | Section 3, "Environmental Conditions," addresses environmental factors. Section 1 and 2 address driver inputs via the stalk control. Section 4 also mentions driver actions related to washer fluid. |
| **Hint for Improvement:** | None.  --- |

Dependencies and Interactions – Item 4

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_023 |
| **Requirement:** | Assumptions Documentation |
| **Description:** | Assumptions made about the environment, usage, or other systems shall be clearly stated. |
| **Status:** | Pass |
| **Comment:** | Section 4, "Dependencies and Assumptions," clearly lists assumptions such as "The driver will inspect and refill washer fluid as needed," "The wiper blades are maintained and replaced according to manufacturer recommendations," etc. |
| **Hint for Improvement:** | None.  --- |

System Boundaries and Context

This section defines the physical and logical boundaries of the item, along with environmental conditions and design constraints. It clarifies where the item operates and under what limitations, such as temperature, vibration, or EMC exposure. These details ensure that the item is developed and validated under realistic assumptions. Defining this context early supports the creation of accurate test plans and operational profiles.

System Boundaries and Context – Item 1

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_024 |
| **Requirement:** | System Boundaries Definition |
| **Description:** | Physical and logical boundaries of the item shall be clearly defined. |
| **Status:** | Pass |
| **Comment:** | Section 8, "Scope and Boundaries," defines the scope which implicitly defines the boundaries of the item. The exclusions further clarify what is outside these boundaries. |
| **Hint for Improvement:** | None.  --- |

System Boundaries and Context – Item 2

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_025 |
| **Requirement:** | Interaction with Non-Safety Systems |
| **Description:** | Interactions with non-safety-related systems shall be documented. |
| **Status:** | Pass |
| **Comment:** | Section 2, "Interfaces," lists interactions with the "Vehicle Electrical System" and "Body Control Module (BCM)," which are likely to include non-safety-related aspects. |
| **Hint for Improvement:** | None.  --- |

System Boundaries and Context – Item 3

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_026 |
| **Requirement:** | Environmental Condition Consideration |
| **Description:** | Environmental conditions such as temperature, vibration, EMC, etc., shall be considered and documented. |
| **Status:** | Pass |
| **Comment:** | Section 3, "Environmental Conditions," explicitly lists operating and storage temperatures, humidity, vibration, EMC, and dust/water ingress protection. |
| **Hint for Improvement:** | None.  --- |

System Boundaries and Context – Item 4

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_027 |
| **Requirement:** | Design Constraints Statement |
| **Description:** | Design constraints (hardware, software, regulatory, etc.) shall be stated. |
| **Status:** | Pass |
| **Comment:** | Section 7, "Constraints," clearly outlines hardware, software, regulatory, and design constraints. |
| **Hint for Improvement:** | None.  --- |

Review and Approval

This section confirms that a formal review process was followed and that all necessary approvals were obtained before finalizing the item definition. It verifies that review minutes, action items, and change records are documented and closed. Configuration management practices should also be applied to maintain document integrity. This ensures process compliance and provides an auditable trail for quality assurance and functional safety governance.

Review and Approval – Item 1

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_028 |
| **Requirement:** | Formal Review Process Followed |
| **Description:** | A formal review process shall be followed during the creation or update of the item definition. |
| **Status:** | Not Applicable (for this document review) |
| **Comment:** | This checklist item pertains to the process of creating or updating the Item Definition itself. As I am reviewing a provided document, I cannot assess if a formal review process was followed during its creation. |
| **Hint for Improvement:** | Ensure that the project's quality management system includes a formal review process for Item Definitions.  --- |

Review and Approval – Item 2

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_029 |
| **Requirement:** | Approval Documentation |
| **Description:** | All necessary approvals for the item definition shall be documented. |
| **Status:** | Not Applicable (for this document review) |
| **Comment:** | Similar to REV\_ID\_028, I cannot verify the approval documentation of the provided Item Definition. |
| **Hint for Improvement:** | Ensure that the final approved version of the Item Definition is clearly marked and stored with associated approval records.  --- |

Review and Approval – Item 3

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_030 |
| **Requirement:** | Review Minutes and Action Items |
| **Description:** | Review minutes and action items shall be recorded and closed. |
| **Status:** | Not Applicable (for this document review) |
| **Comment:** | I cannot assess the review minutes and action items for the creation of this Item Definition. |
| **Hint for Improvement:** | Maintain detailed records of review meetings, including identified action items and their closure status.  --- |

Review and Approval – Item 4

|  |  |
| --- | --- |
| **ID:** | REV\_ID\_031 |
| **Requirement:** | Configuration Management Application |
| **Description:** | Configuration management shall be applied to the item definition. |
| **Status:** | Pass |
| **Comment:** | The presence of "Version: 1.0" and "Date: April 5, 2025" indicates that configuration management principles are being applied to the Item Definition. |
| **Hint for Improvement:** | None. |