How would you conduct a Hazard Analysis and Risk Assessment (HARA) for an automotive system?

To conduct a Hazard Analysis and Risk Assessment (HARA) for an automotive system according to ISO 26262, the following steps and considerations are involved:

The HARA is a method used to identify and categorize hazardous events of items, and to specify safety goals and Automotive Safety Integrity Levels (ASILs) related to preventing or mitigating associated hazards to avoid unreasonable risk (ISO 26262-1:2018 Clause 3.76). Its output defines the safety goals for the item, determined through a systematic evaluation of potential hazardous events, considering severity, probability of exposure, and controllability (ISO 26262-3:2018 Clause 6.2). The HARA is based on the item's functional behavior, meaning detailed design is not necessarily required (ISO 26262-3:2018 Clause 6.2).

1. Prerequisites and Initiation: Before initiating the HARA, the item definition shall be available (ISO 26262-3:2018 Clause 6.3.1, ISO 26262-12:2018 Clause 8.3.1). The hazard analysis and risk assessment shall be based on this item definition (ISO 26262-3:2018 Clause 6.4.1.1, ISO 26262-12:2018 Clause 8.4.1.1). During the HARA, the item shall be evaluated without considering internal safety mechanisms (ISO 26262-3:2018 Clause 6.4.1.2, ISO 26262-12:2018 Clause 8.4.1.2). However, available and sufficiently independent external measures can be beneficial and considered (ISO 26262-3:2018 Clause 6.4.1.2 Note 1, ISO 26262-10:2018 Clause 6.4.1 Note 1).

2. Situation Analysis and Hazard Identification: The goal of this step is to identify potential unintended behaviors of the item that could lead to a hazardous event (ISO 26262-3:2018 Clause 6.4.2, ISO 26262-12:2018 Clause 8.4.2). This activity requires a clear definition of the item, its functionality, and its boundaries (ISO 26262-3:2018 Clause 6.4.2).

Key activities include:

- **Describing operational situations:** The operational situations and operating modes in which an item's malfunctioning behavior will result in a hazardous event shall be described, covering both correct and reasonably foreseeable incorrect use of the vehicle (ISO 26262-3:2018 Clause 6.4.2.1, ISO 26262-12:2018 Clause 8.4.2.1). Factors such as vehicle usage scenarios, environmental conditions, reasonably foreseeable driver use and misuse, and interaction between operational systems can be considered (ISO 26262-3:2018 Clause 6.4.2).
- **Determining hazards:** Hazards shall be determined systematically based on the possible malfunctioning behavior of the item (ISO 26262-3:2018 Clause 6.4.2.2, ISO 26262-12:2018 Clause 8.4.2.2). These hazards, caused by malfunctioning behavior, shall be defined at the vehicle level (ISO 26262-3:2018 Clause 6.4.2.3, ISO 26262-12:2018 Clause 8.4.2.3).
- **Identifying hazardous events and consequences:** Relevant hazardous events shall be determined (ISO 26262-12:2018 Clause 8.4.2.5), and their consequences identified (ISO 26262-12:2018 Clause 8.4.2.6). A hazardous event is a combination of a hazard and an operational situation (ISO 26262-1:2018 Clause 3.77).

3. Classification of Hazardous Events: This step comprises the determination of the severity, the probability of exposure, and the controllability associated with the hazardous events of the item (ISO 26262-3:2018 Clause 6.4.3, ISO 26262-12:2018 Clause 8.4.3). All hazardous events identified in the previous step shall be classified, except those outside the scope of ISO 26262 (ISO 26262-12:2018 Clause 8.4.3.1). If classification is difficult, a conservative approach (choosing a higher classification for severity, exposure, or controllability) should be taken (ISO 26262-12:2018 Clause 8.4.3.1 Note).

- **Severity (S):** Represents an estimate of the potential harm in a particular driving situation (ISO 26262-3:2018 Clause 6.4.3). Potential injuries are evaluated for the driver, passengers, and people around the vehicle or in surrounding vehicles to determine the severity class (ISO 26262-3:2018 Clause B.2.1, ISO 26262-12:2018 Clause B.2.1). The severity shall be assigned to one of the classes S0, S1, S2, or S3 (ISO 26262-12:2018 Clause 8.4.3.2).
- **Probability of Exposure (E):** Determined by the corresponding operational situation (ISO 26262-3:2018 Clause 6.4.3).
- **Controllability (C):** Rates how easy or difficult it is for the driver or other road traffic participant to avoid the considered accident type in the considered operational situation (ISO 26262-3:2018 Clause 6.4.3, ISO 26262-10:2018 Clause 6.3).

4. ASIL Determination: Following the classification of hazardous events, the required Automotive Safety Integrity Level (ASIL) is determined (ISO 26262-3:2018 Clause 6.4.3). The ASIL is determined by considering the combination of severity, probability of exposure, and controllability (ISO 26262-3:2018 Clause 6.2). At least one safety goal is associated with each hazardous event that has been classified as ASIL A, B, C or D (ISO 26262-10:2018 Clause 4.1).

5. Management of Variances for T&B (Truck & Bus): For Truck & Bus (T&B) vehicles, specific variances shall be considered when conducting a HARA, including the type of base vehicle, the T&B vehicle configuration, and the T&B vehicle operation (ISO 26262-3:2018 Clause 6.4.5.2). When classifying S, E, and C, an appropriate combination of these variance types shall be considered (ISO 26262-3:2018 Clause 6.4.5.7).

6. Work Products and Verification: The HARA process results in specific work products:

- A Hazard analysis and risk assessment report (ISO 26262-3:2018 Clause 6.5.1).
- A Verification report of the hazard analysis and risk assessment (ISO 26262-3:2018 Clause 6.5.2).

The hazard analysis and risk assessment, including the safety goals, shall be verified to provide evidence for their appropriate selection, compliance with the item definition, consistency, completeness, and consistency of safety goals with assigned ASILs (ISO 26262-3:2018 Clause 6.4.6.1). Assumptions made during HARA that are relevant for ASIL determination shall be identified and validated (ISO 26262-3:2018 Clause 6.4.4.4).

Additional List of Clauses:

- ISO 26262-1:2018 Clause 3.76 Hazard analysis and risk assessment
- ISO 26262-1:2018 Clause 3.77 Hazardous event
- ISO 26262-3:2018 Clause B.2.1 General (Examples of severity)
- ISO 26262-3:2018 Clause 6.2 General (Hazard analysis, risk assessment and ASIL determination)
- ISO 26262-3:2018 Clause 6.3.1 Prerequisites (Inputs to this clause)
- ISO 26262-3:2018 Clause 6.4.1.1 Initiation of the hazard analysis and risk assessment
- ISO 26262-3:2018 Clause 6.4.1.2 Initiation of the hazard analysis and risk assessment
- ISO 26262-3:2018 Clause 6.4.1.2 Note 1 (Evaluation of an item)
- ISO 26262-3:2018 Clause 6.4.2 Situation analysis and hazard identification
- ISO 26262-3:2018 Clause 6.4.2.1 Situation analysis and hazard identification
- ISO 26262-3:2018 Clause 6.4.2.2 Situation analysis and hazard identification
- ISO 26262-3:2018 Clause 6.4.2.3 Situation analysis and hazard identification
- ISO 26262-3:2018 Clause 6.4.3 Classification of hazardous events

- ISO 26262-3:2018 Clause 6.4.4.4 Assumptions used for, or resulting from the hazard analysis and risk assessment which are relevant for ASIL determination
- ISO 26262-3:2018 Clause 6.4.5.2 Management of variances of T&B in hazard analysis and risk assessment
- ISO 26262-3:2018 Clause 6.4.5.7 Management of variances of T&B in hazard analysis and risk assessment
- ISO 26262-3:2018 Clause 6.4.6.1 Verification (of HARA)
- ISO 26262-3:2018 Clause 6.5.1 Work products (Hazard analysis and risk assessment report)
- ISO 26262-3:2018 Clause 6.5.2 Work products (Verification report)
- ISO 26262-10:2018 Clause 4.1 Functional safety for automotive systems (relationship with IEC 61508)
- ISO 26262-10:2018 Clause 6.3 An observation regarding controllability classification
- ISO 26262-10:2018 Clause 6.4.1 General (External measures)
- ISO 26262-10:2018 Clause 6.4.1 Note 1 (External measures)
- ISO 26262-12:2018 Clause 8.3.1 Prerequisites (Input to this clause)
- ISO 26262-12:2018 Clause 8.4.1.1 Initiation of the hazard analysis and risk assessment
- ISO 26262-12:2018 Clause 8.4.1.2 Initiation of the hazard analysis and risk assessment
- ISO 26262-12:2018 Clause 8.4.2 Situation analysis and hazard identification
- ISO 26262-12:2018 Clause 8.4.2.1 Situation analysis and hazard identification
- ISO 26262-12:2018 Clause 8.4.2.2 Hazard Identification
- ISO 26262-12:2018 Clause 8.4.2.3 Hazard Identification
- ISO 26262-12:2018 Clause 8.4.2.5 Relevant hazardous events shall be determined.
- ISO 26262-12:2018 Clause 8.4.2.6 The consequences of hazardous events shall be identified.
- ISO 26262-12:2018 Clause 8.4.3 Classification of Hazardous Events
- ISO 26262-12:2018 Clause 8.4.3.1 Classification of Hazardous Events
- ISO 26262-12:2018 Clause 8.4.3.1 Note (Classification of a given hazard)
- ISO 26262-12:2018 Clause 8.4.3.2 The severity of potential harm shall be estimated based on a defined rationale for each hazardous event.
- ISO 26262-12:2018 Clause B.2.1 General (Examples of severity)

Correctness = 5P,
Completeness = 5P, even included specialties for T&B