

Explain the concept of Automotive Safety Integrity Level (ASIL) decomposition and its significance.

ASIL (Automotive Safety Integrity Level) decomposition is a method of ASIL tailoring applied during the concept and development phases (ISO 26262-9:2018, Clause 5.2; ISO 26262-1:2018, Clause 3.3 Note 1). It involves the apportioning of redundant safety requirements to sufficiently independent elements of an item (ISO 26262-1:2018, Clause 3.3; ISO 26262-10:2018, Clause 11.2).

The primary objective of ASIL decomposition is to comply with the safety goal by using multiple sufficiently independent elements, particularly with respect to systematic faults (ISO 26262-10:2018, Clause 11.1). This approach allows a safety requirement to be decomposed into redundant safety requirements, which are then allocated to sufficiently independent design elements according to permitted ASIL decomposition schemas (ISO 26262-9:2018, Clause 5.1).

Key aspects of ASIL decomposition include:

- **Independence:** For ASIL decomposition to be valid, the architectural elements implementing the decomposed requirements must be "sufficiently independent" (ISO 26262-9:2018, Clause 5.2). This means that a dependent failure analysis should not find a plausible cause of dependent failures that could violate the initial safety requirement, or any identified cause must be controlled by adequate safety measures (ISO 26262-9:2018, Clause 5.4.3). If independence is not sufficient, the redundant requirements and architectural elements inherit the initial ASIL (ISO 26262-9:2018, Clause 5.2).
- **Redundancy:** The initial safety requirement is decomposed into redundant safety requirements. Each decomposed safety requirement must be able to comply with the initial safety requirement by itself, thus providing redundancy (ISO 26262-9:2018, Clause 5.4.4).
- **Applicability:** ASIL decomposition can be applied to functional, technical, hardware, or software safety requirements (ISO 26262-9:2018, Clause 5.2).
- **Systematic Failures Focus:** ASIL decomposition is understood in the context of systematic failures, referring to the methods and measures applied to reduce the likelihood of these failures (ISO 26262-10:2018, Clause 11.2).
- **Hardware Random Failures:** The requirements concerning the evaluation of hardware architectural metrics and safety goal violations due to random hardware failures remain unchanged by ASIL decomposition (ISO 26262-9:2018, Clause 5.2; ISO 26262-9:2018, Clause 5.4.5; ISO 26262-10:2018, Clause 11.2). The target metric applies at the item level (ISO 26262-10:2018, Clause 11.2).
- **Decomposition Schemas:** Specific decomposition schemas are defined based on the initial ASIL (ISO 26262-9:2018, Clause 5.4.9). For example, an ASIL D requirement can be decomposed into:
 - one ASIL C(D) requirement and one ASIL A(D) requirement, or
 - one ASIL B(D) requirement and one ASIL B(D) requirement, or
 - one ASIL D(D) requirement and one QM(D) requirement (ISO 26262-9:2018, Clause 5.4.9).
- **ASIL Marking:** Each decomposed ASIL is marked by indicating the ASIL of the original safety goal in parentheses (e.g., ASIL C(D)) (ISO 26262-9:2018, Clause 5.4.8).

Significance: The significance of ASIL decomposition lies in its ability to assign potentially lower ASILs to the decomposed safety requirements (ISO 26262-9:2018, Clause 5.2; ISO 26262-1:2018, Clause 3.3). This tailoring measure can lead to reduced stringency in the development processes for individual elements (ISO 26262-4:2018, Clause 4.4; ISO 26262-5:2018, Clause 4.4; ISO 26262-3:2018, Clause 4.4), potentially optimizing development efforts, time, and costs, while still ensuring

the overall safety goal is achieved through the combined effect of the independent redundant elements. In a decomposed architecture, the safety requirement before decomposition is only violated if both elements simultaneously violate their safety requirements resulting from the decomposition (ISO 26262-10:2018, Clause 11.2).

Additional list of clauses:

- ISO 26262-1:2018, Clause 3.3
- ISO 26262-1:2018, Clause 3.3 Note 1
- ISO 26262-1:2018, Clause 3.3 Note 2
- ISO 26262-3:2018, Clause 4.4
- ISO 26262-4:2018, Clause 4.4
- ISO 26262-5:2018, Clause 4.4
- ISO 26262-9:2018, Clause 5.1
- ISO 26262-9:2018, Clause 5.2
- ISO 26262-9:2018, Clause 5.4.3
- ISO 26262-9:2018, Clause 5.4.4
- ISO 26262-9:2018, Clause 5.4.5
- ISO 26262-9:2018, Clause 5.4.8
- ISO 26262-9:2018, Clause 5.4.9
- ISO 26262-10:2018, Clause 11.1
- ISO 26262-10:2018, Clause 11.2

Correctness = 5P, all statements are correct

Completeness = 5P, all the important points of the question have been sufficiently addressed.