Concepts

For better understanding further material, get acquainted with basic concepts of analyzing safety and reliability.

Risk concepts

Concept	Description
Risk	Combination of the probability of occurrence of harm and the severity of that harm.
Hazard	A potential source of harm. A hazard is any source of potential damage, harm or adverse health effects on something or someone under certain conditions at work.
Hazardous situation	Circumstance in which people, property, or the environment are exposed to one or more hazard(s).
Harm	Physical injury or damage to the health of people, or damage to property or the environment.
Severity	Measure of the possible consequences of a hazard.
Probability	Quantitative evaluation of a event happening. There are two types of probabilities emphasized in ISO 14971:2012: • P1 – probability of foreseeable sequence of events leading to hazardous situation. • P2 – probability that harm will occur when exposed to hazard.
Detectability	Hazard detection index accounts for the likelihood of discovering and correcting a hazard or failure mode prior to harm occurrence.
Hazard Correctability	Factor rates the relative ease of mitigating a certain risk. It accounts for the associated feasibility and effort required in reducing a particular risk to the lowest practicable level.
Product Utility	Factor is meant to integrate clinical benefit into the risk score.

FMEA concepts

Concept	Description
Item	Enter the items, interfaces, or parts which have been identified through block diagrams, P-diagrams, schematics and other drawings, and other analysis conducted by the team.
Failure Mode	Potential failure mode is defined as the manner in which a component, subsystem, or system could potentially fail to meet or deliver the intended function described in the item column.
Effect of Failure	Effects of failure are defined as the effects of the failure mode on the function, as perceived by the customer(s).
Severity	Severity is the value associated with the most serious effect for a given failure mode.
Cause of Failure	Potential cause of failure is defined as an indication of how the design process could allow the failure to occur, described in terms of something that can be corrected or can be controlled.
Occurrence	Occurrence is the likelihood that a specific cause/mechanism will occur resulting in the failure mode within the design life.
Current Design Controls	Current Design Controls are those activities conducted as part of the design process that have been completed or committed to and that will assure the design adequacy for the design functional and reliability requirements under consideration.
Detectability	Detection is the rank associated with the best detection control listed in the Current Design Control Detection column.
Recommended Action	The intent of recommended actions is to improve the design. Identifying these actions should consider reducing rankings in the following order: severity, occurrence, and detection.
Responsibility Target Completion Date	The name of the individual and organization which is responsible for completing each recommended action including the target completion date.
Action taken	A brief description of the action taken and actual completion date.
Hazard Analysis Reference	Reference to Risk.

ISO 26262 Functional Safety concepts

Concept	Description
Malfunctioning Behavior	A Malfunctioning Behavior describes a failure or unintended behavior of an item with respect to its design intent. It is a subtype of a Failure Mode.
Operational Situation	An Operational Situation describes the operational scenario or driving scenario which is considered in a Hazardous Event, as part of the Hazard Analysis and Risk Assessment process.
ASIL	Automotive Safety Integrity Level is one of four levels to specify the necessary requirements for ISO-26262 and safety measures for avoiding unreasonable risks. There are four ASILs identified by ISO 26262 - A, B, C, and D. ASIL A represents the lowest degree, and ASIL D represents the highest degree of automotive hazard.
Exposure	Exposure is the likelihood of being in a particular operational situation. Exposure Classifications (E): **E0** Incredibly unlikely **E1** Very low probability (injury could happen only in rare operating conditions) **E2** Low probability **E3** Medium probability **E4** High probability (injury could happen under most operating conditions)
Severity	"Estimate of the extent of harm." Severity Classifications (S): **S0** No Injuries **S1** Light to moderate injuries **S2** Severe to life-threatening (survival probable) injuries **S3** Life-threatening (survival uncertain) to fatal injuries
Controllability	"Ability to avoid a specified harm or damage through timely reactions of individuals involved in the scenario." Controllability Classifications (C): **C0** Controllable in general **C1** Simply controllable **C2** Normally controllable (most drivers could act to prevent injury) **C3** Difficult to control or uncontrollable
Safety Goal	It represents a top-level safety requirement, defined as a result of the Hazard Analysis and Risk Assessment process. A *safety goal* is a top-level safety requirement that is assigned to a system, with the purpose of reducing the risk of one or more *hazardous events* to a tolerable level.
Functional Safety Requirement	A functional safety requirement specifies an implementation independent safety behavior, or an implementation independent safety measure, required for achievement of a safety goal from which it is derived.
Technical Safety Requirement	A technical safety requirement specifies the implementation of the functional safety requirement(s) from which it is derived. Technical safety requirements express the behaviors and details necessary to realize the safety aspects of the item at the system level. Additional details that do not act at the system level can be specified in the hardware safety requirements or software safety requirements.
Software Safety Requirement	A software safety requirement provides implementation details for software. They can express behaviors or specific software mechanisms which realize the technical safety requirements from which they are derived
Hardware Safety Requirement	A hardware safety requirement specifies hardware behaviors or hardware specific details necessary for implementing the safety concept. Hardware safety requirements are implementation specific and assigned to components or subcomponents.
ASIL Decompose relationship	An ASIL decompose relation is used to connect two safety requirements for the purposes of performing ASIL decomposition. The target requirement (supplier) should be of a higher abstraction than the source (client). ASIL decompose relations shall be applied in pairs (e.g. a requirement cannot be the supplier of a single ASIL decompose relation).
Independece Requirement relationship	A relationship between requirement elements indicating that the child requirement specifies an independence criteria that needs to be satisfied in order for an ASIL decomposition to be valid. The decomposition between the parent requirement and 2 other children requirements.
Safe State	A state of function realized by one or more architectural components. May be composed of serval subfunctions or called by other functions. Associated with safety specific behaviors, typically (but not necessarily) triggered by a failure mode.

Operating Mode	A state of function realized by one or more architectural components. May be composed of serval subfunctions or called by other functions. Associated with specific behaviors.
Recovery Requirement	A RecoveryRequirement relationship is a dependency between a safe state and requirement where the requirement indicates the criteria to recover from the safe state to another operational mode.
User Info Requirement	"A UserInfoRequirement relationship is a dependency which links a State to a requirement. The arrow direction points from a state (client) to a FSR or TSR (supplier). Linked requirements specify information that must be presented to vehicle occupants when the vehicle enters a safe state. "
FTTI fault tolerant time interval	time-span in which a fault or faults can be present in a system before a hazardous event occurs.
System Level Effect	System- or vehicle-level effect which is or could result in harm.
Vehicle Level Effect	System- or vehicle-level effect which is or could result in harm.
Traffic And People	It is used to describe the presence and behavior of any motorists or non-motorists considered in a hazardous event.
Vehicle Usage	It is used to describe the usage of a vehicle during a hazardous event.
Road Condition	It is used to describe the conditions or state of the surface a vehicle is driving on (Low-traction, Grade(Slope), etc.) during a hazardous event.
Location	It is used to describe the physical location (high speed road, intersection, parking lot, etc.) of a vehicle during a hazardous event.
Environmental Condition	It and is used to describe the environmental conditions at the time of vehicle operation in a hazardous event.
Hazardous Event	Combination of hazard and operational situation to identify automotive safety integrity level. A *hazardous event* is a relevant combination of a vehicle-level *hazard* and an operational situation of the vehicle with potential to lead to an accident if not controlled by timely driver action.
Hazard	Potential source of harm.
Accident Scenario	A combination of operational situation and malfunctioning behavior
More	This kind of malfunctioning behavior represents a failure resulting from providing more output/behavior than required.
Less	This kind of malfunctioning behavior represents a failure resulting from providing less output/behavior than required.
No	This kind of malfunctioning behavior represents a failure resulting from the behavior not being performed when required.
Intermittent	This kind of malfunctioning behavior represents a failure from the behavior being performed intermittently.
Unintended	This kind of malfunctioning behavior represents a failure resulting from the behavior being provided when not required.
Early	This kind of malfunctioning behavior represents a failure resulting from the behavior being performed earlier than required.
Late	This kind of malfunctioning behavior represents a failure resulting from the behavior being performed later than required.
Inverted	This kind of malfunctioning behavior represents a failure resulting from the behavior providing an inverted output.

Related pages

- Getting started
  - Process description
  - Project templates