Introduction to ISO 26262

Hazard analysis

2011-03-18

Overview ISO 26262

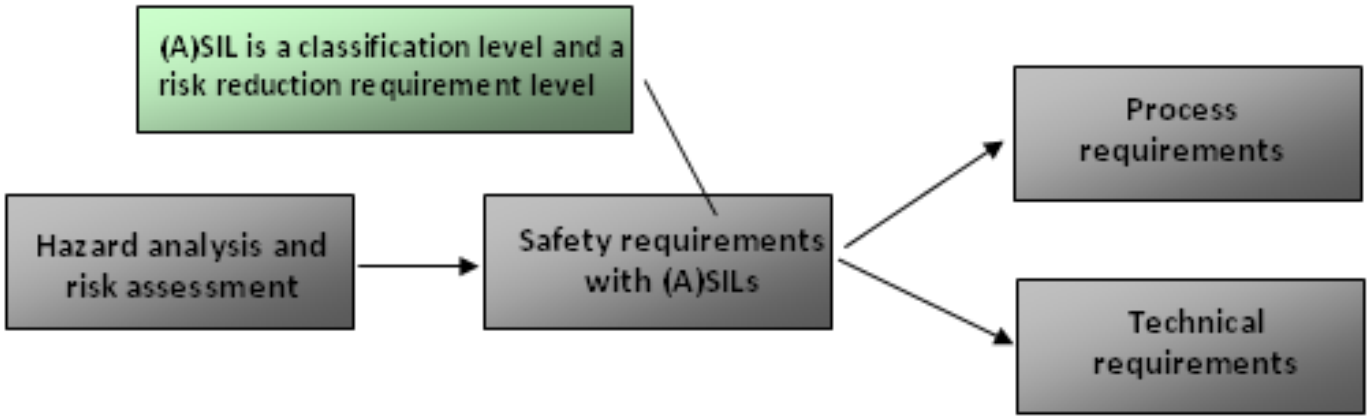
- An investigation made by WHO 1997 showed that traffic accidents caused as many as 4% of all deaths worldwide. Approximately 10% of these road accidents are caused by failure in technical systems where E/E is a part of this.

- Due to the fact that the technical complexity and integration complexity are increasing in today's vehicles, the need for a defined safety strategy for automotive business is growing.

"All information contained herein is confidential and/or proprietary to Kongsberg Automotive and any unauthorized disclosure or utilization is expressly prohibited. The information is legally safeguarded by digital fingerprints and offenders will be held liable for any damages suffered. All rights and/or title to any intellectual property are reserved."

Overview ISO 26262

- **Overview of the strategy and working process to achieve a high functional safety for the automotive business.**



Hazard analysis

- Hazards are found early in the development cycle
- HA can save development time and system cost
- HA adresses function failure modes
- HA is not applied to internal components
- Hazard classification (ISO 26262) is based on 3 parameters
  - Exposure (E)
  - Severity (S)
  - Controllability (C)

Exposure classification

- Exposure is an estimation of how much or how often the user (or third party) is exposed to a situation that is hazardous if a certain failure occurs.
- Exposure is judged on item basis and not on a specific user basis.

E1	E2	E3	E4
Very low probability	Low probability	Medium probability	High probability
Not specified	< 1% of average operating time	1% - 10% of average operating time	> 10% of average operating time

Severity classification

- Severity shall be considered for all involved parties. State explicitly for who the severity is judged.
- Severity is depending on vehicle type and situation
- The involved parties may include but is not limited to:
  - Unprotected road users
  - Driver
  - Passenger(s)
  - Oncoming vehicle occupants
  - Vehicle(s) in behind occupants
  - Service personnel
  - Production personnel

S0	S1	S2	S3
No injuries	Light and moderate injuries	Severe injuries, possibly life-threatening, survival probable	Life-threatening injuries (survival uncertain) or fatal injuries
Damage that cannot be classified safety-related	> 10% probability of AIS 1-6	> 10% probability of AIS 3-6	> 10% probability of AIS 5-6

AIS – Abbreviated Injury Scale

1. Minor
2. Moderate
3. Serious
4. Severe
5. Critical
6. Maximum

Controllability classification

- Controllability is classified from the ability of any driver/user or other road user(s) to avoid harm.
- Mitigations by other technical systems are not considered when classifying controllability.
- Driver reaction time, misuse, preventive action shall be considered when judging controllability

C0	C1	C2	C3
Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
	99% or more of all drivers or other traffic participantsare usually able to avoid a specific harm	90% or more of all drivers or other traffic participantsare usually able to avoid a specific harm	Less than 90% or more of all drivers or other traffic participantsare usually able to avoid a specific harm

Hazard analysis

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Classification example

- Simplified example for steer-by-wire functionality

Function	Failure mode	Situation	E	S	C	ASIL	Safety goal
Steer-by-wire	Commission	Driving at high speed	E4	S3	C3	D	Steer-by-wire shall not steer unintended during driving
	Stuck	Driving at high speed	E4	S3	C3	D	Steer-by-wire shall not lock during driving