Safety System

02 March 2021 10:03 PM

1) Active Safety and Passive Safety System
   - Active Safety System
     - An active safety system works to prevent an accident. These systems always stay active while you drive, and continuously work to keep you from getting into an accident. Most active safety features are electronic and controlled by a computer.
     - They include traction control, electronic stability control, and braking systems. These also include advanced driver assist systems that use sensors such as forward collision warning and lane departure warning, along with adaptive cruise control.
   - Passive Safety System
     - A passive safety feature is a system that does not do any work until it is called to action. These features become active during an accident, and work to minimize damage and reduce the risk of injury during the time of impact.
     - These systems are seat belts, air bags, and the construction of the vehicle. These devices automatically deploy when the car gets into a crash.

2) Name of your project ECU ?
   - Passenger Comfort ECU.

3) ISO 26262
   - ISO 26262 is a functional safety standard used in the automotive industry, and ASIL is a key component to determine safety requirements for software development.
   - Complying with this standard is critical for automotive product development. OEMs, their suppliers, and developers of automotive components all need to comply.
   - What Is the ISO 26262 Functional Safety Standard?
     - ISO 26262 is a risk-based safety standard that's derived from IEC 61508. It applies to electric and/or electronic systems in production vehicles. This includes driver assistance, propulsion, and vehicle dynamics control systems.
     - The functional safety standard covers all of the functional safety aspects of the entire development process:
       1) Requirements specification
       2) Design
       3) Implementation
       4) Integration
       5) Verification
       6) Validation
       7) Configuration
   - what Is ASIL? And, Why Is ASIL Important?
     - Automotive Safety Integrity Level (ASIL) is a key component of ISO 26262 and it is used to measure the risk of a specific system component. The more complex the system, the greater the risk of systematic failures and random hardware failures.
     - There are four Automotive Safety Integrity Level values, named A–D. ASIL A is the minimum level of risk and ASIL D is the maximum, as you go from A to D, the compliance requirements get stricter.
     - When determining Automotive Safety Integrity Levels, there's also a fifth option — QM (quality management). This is used to note that there isn't a safety requirement for that component. (But it's typically still a good idea to comply in order to improve product quality.)
   - How to Determine ASIL?
     - ASIL is determined by three factors — severity, exposure, and controllability.
     - Severity
       - Severity measures how serious the damages are of a system failure. Damages include both people and property.

There are four classes of severity:

- S0: No injuries.
- S1: Light to moderate injuries.
- S2: Severe to life-threatening (survival probable) injuries.
- S3: Life-threatening (survival uncertain) to fatal injuries.

- Exposure
  - Exposure is the likelihood of the conditions under which a particular failure would result in a safety hazard.
  - The probability of each condition is ranked on a five-point scale:
    - 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).
- Controllability
  - Controllability is a measure of the probability that harm can be avoided when a hazardous condition occurs. This condition might be due to actions by the driver or by external measures.
  - The controllability of a hazardous situation is ranked on a four-point scale:
    - C0: Controllable in general.
    - C1: Simply controllable.
    - C2: Normally controllable (most drivers could act to prevent injury).
    - C3: Difficult to control or uncontrollable