* Hardware safety requirements
  + Hardware development may not be dependent on hardware requirements
  + Technical safety requirements are inputs to hardware safety requirements.
  + Each TSR has a designated allocation, indicating whether it pertains to hardware, software or both.
  + HSR must be described in terms of current, timing, voltage, hardware diagnostics and so on.
  + HSR should also encompass how faults are detected, what types of faults can be detected, and how external faults from other elements are detected.
* Software safety requirement
  + Start-up diagnostics
  + Software participation
  + Boot time
  + Execution order
  + Shutdown sequence
  + Interfaces
  + Timing and methods
* Hardware architectural design – component and its interaction
* Hardware detailed design – electrical and electronics parts and its interaction making up hardware component.
* Software unit design comment best practices, comment should:
  + Contain the functional description of a section of source code file,
  + Describe interface
  + Describe return values
  + Have traceability tags to the software requirements and even
  + Unit test cases IDs for the future traceability
* Faults and failure:
  + Random – mostly hardware failure. These are probabilistic failure. Hardware can have random/ systematic failure.
  + Systematic : failure related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or the manufacturing process, operational procedure, documentation or other relevant factors. These are deterministic failure.
* Failure mode: manner in which an element or an item fails to provide the intended behavior.
* Safety mechanism – it is a technical solution implemented by E/E functions or elements, or by other technologies, to detect and mitigate or tolerate faults or control or avoid failure in order to maintain intended functionality or achieve or maintain a safe state.
* Failure distribution – is how much of a failure rate is allocated to a particular failure mode.
* Several types of faults studied in ISO26262:
  + Single point faults: is a fault of a hardware element that does not have at least one safety mechanism and can lead directly to the violation of a safety goal.
  + Residual fault – failure not controlled by safety mechanism.
  + Latent fault – can lead to violation of safety fault in combination of independent fault.
  + Detected dule point faults
  + Perceived dual point faults
  + Safe faults
  + Triple point fault leading to latent fault needs detailed analysis.
* Permanent faults: that stays in the systems till it is removed. Ex.
  + Open
  + Shot, etc.
* Transient faults disappear after certain duration on its own. Ex.
  + Bit flips
  + EMC
  + Soft errors etc.