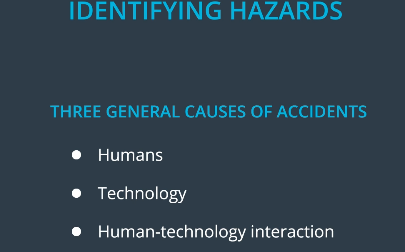
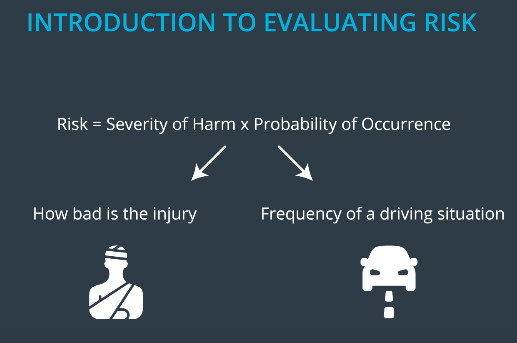
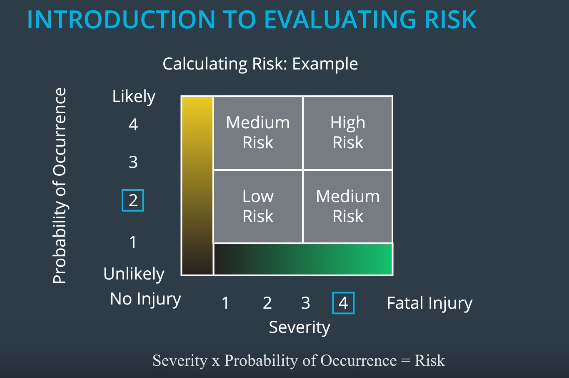
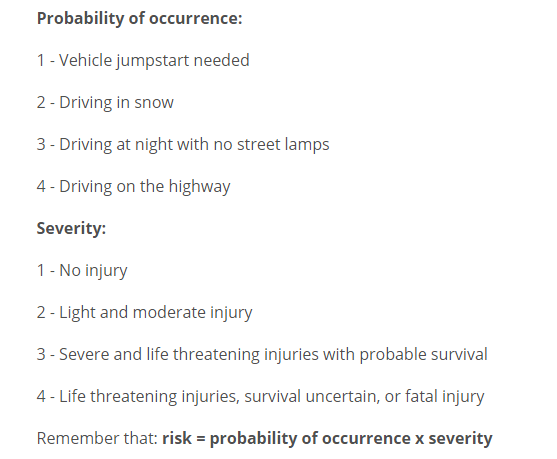
* Functional safety, which only looks at **electrical and electronic system malfunctions**, is just one part of overall vehicle safety.
* Nominal performance issues can still lead to safety problems, but nominal performance is not part of the functional safety standard.
* Functional safety focuses on keeping risks below society's current threshold.

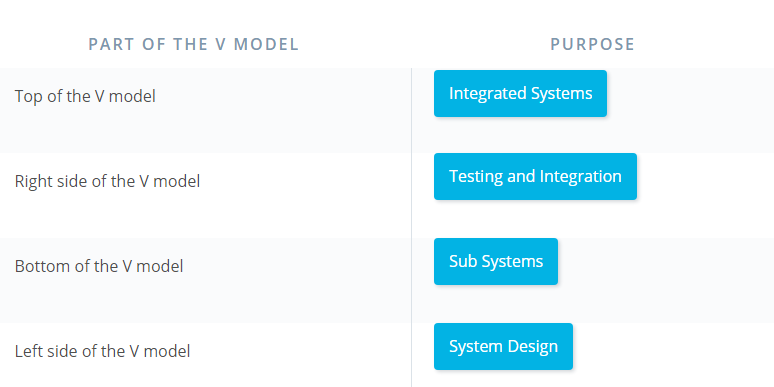


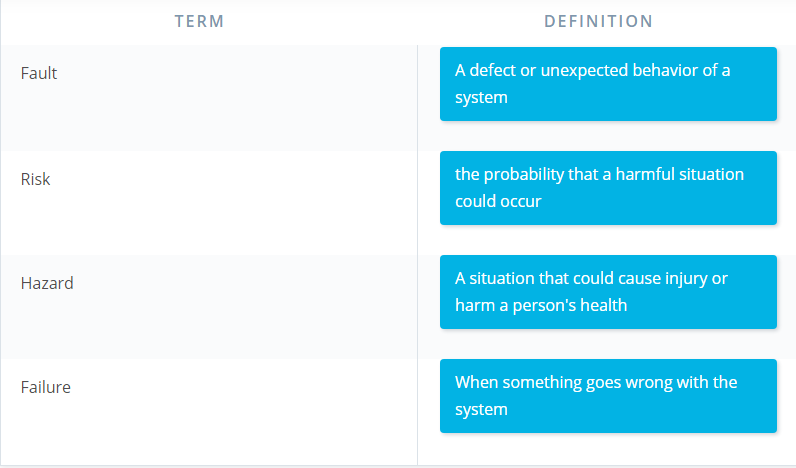




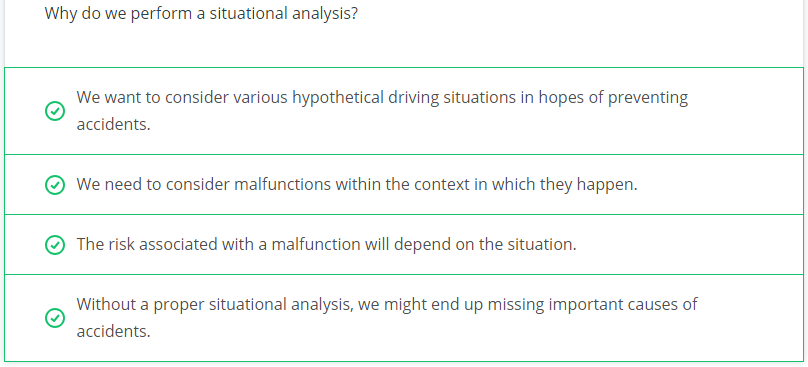


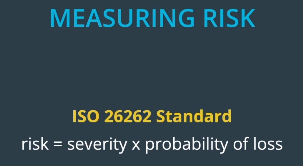




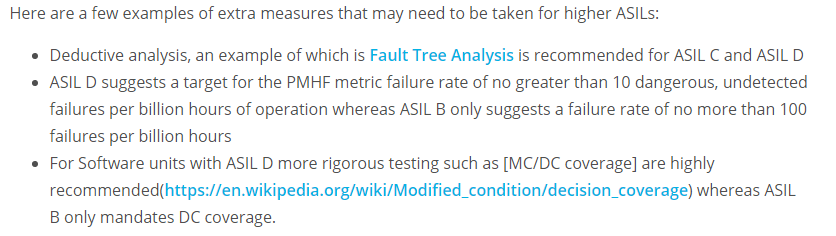


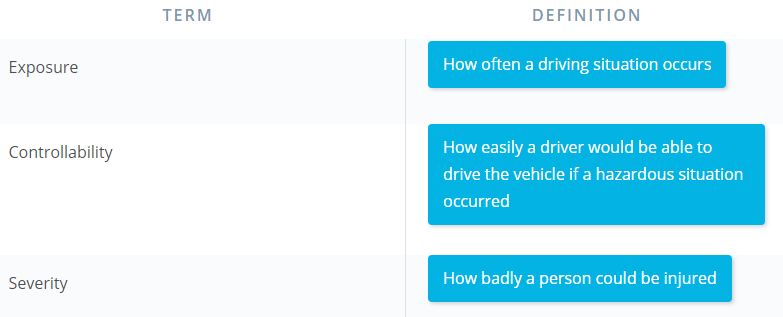


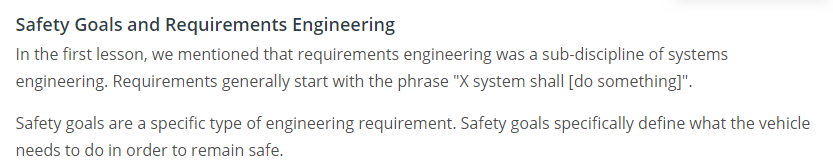




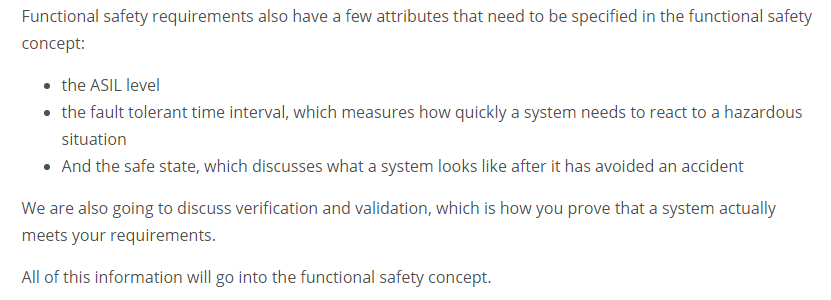




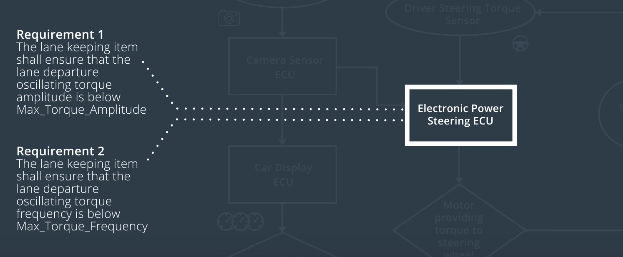


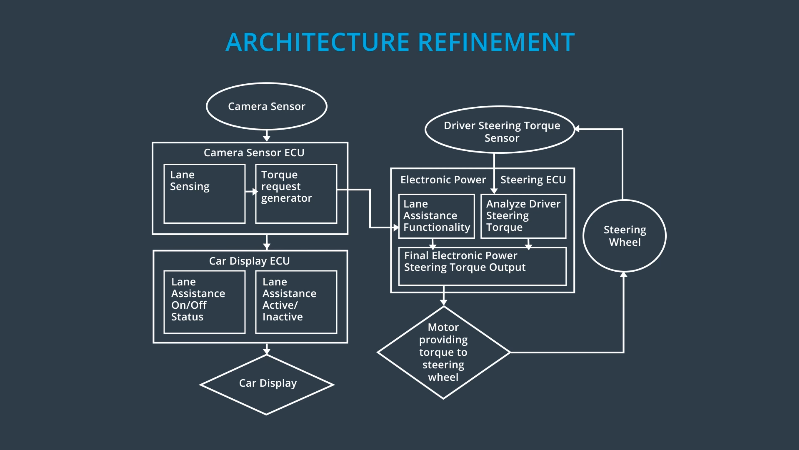


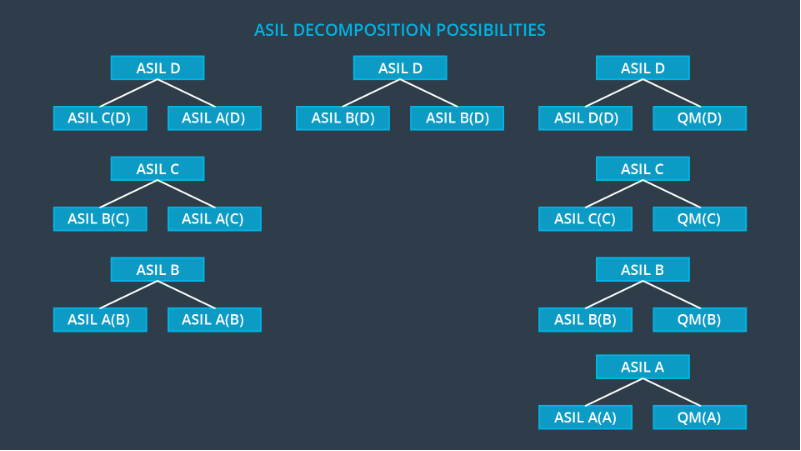
=== Safety concept ===



* The functional safety concept and technical safety concept are similar in that you will need to identify new requirements and allocate these requirements to system diagrams.
* The difference is that the functional safety concept is looking at the item from a higher level. In the technical safety concept, you will start thinking about sensors, control units and actuators. Technical safety requirements are general hardware and software requirements but still without getting into specific details. For example, in the technical safety concept you might realize that you need to add more ECUs, sensors, and extra software blocks to your system
* You will see in this lesson that the functional safety concept does not go into technical details. The functional safety concept looks at the general functionality of the item; the technical safety concept looks at the technical implementation of the item. In practice, developing these two documents is an iterative process where new functional requirements could lead to new technical requirements which could lead back to new functional requirements.

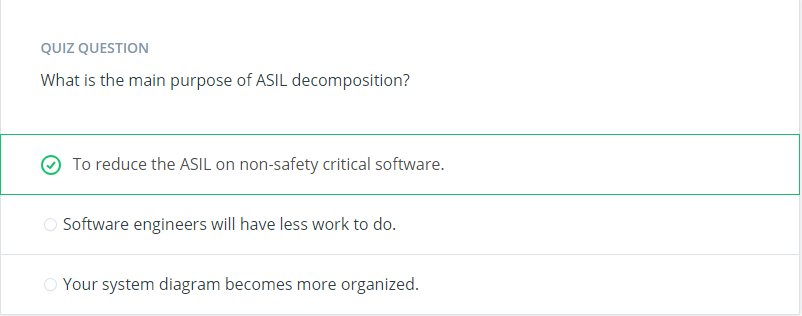


.



* We then derived the functional safety requirement: "the lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration".
* The functional safety requirement inherits the ASIL from the safety goal, so this functional safety requirement is ASIL B as well.
* What do we do now? We already decided that the lane departure warning made the lane assistance software block ASIL C. But we also have a functional safety requirement with ASIL B for the same software block. If two safety requirements are assigned to the same block, the higher ASIL prevails. So the simplest answer is that the lane assistance software block would have ASIL C.

These types of failures where one element fails and then causes another element to fail is called a cascading failure.



**Summary of Warning and Degradation Concept**

In functional safety, "concept" is synonymous with "document". So the warning and degradation concept would be a document that discusses:

* how the driver will be warned of a malfunction
* what the system will do to "degrade" the functionality i.e. take the system to a safe state and also recover from a safe state.

