Functional Safety

Introduction

The term "functional" comes from a branch of systems engineering called requirements engineering.

- *Functional requirements* - what your system is supposed to do; in other words, the system's functions.
- *Non-functional requirements* - how the system should behave: for example, how reliable is the system?

Functional safety looks at what happens when the system does something that it was not supposed to do, which is called a malfunction.

The most generic standard is **IEC 61508**, which originated from industrial markets. It currently exists as a standard in the IEC/ISO basic safety publication, which covers "general functional safety," for a number of industries. *ISO 26262* specifically applies to automotive passenger vehicle electrical and electronic systems. The ISO 26262 standard is an branch of the IEC 61508 standard.

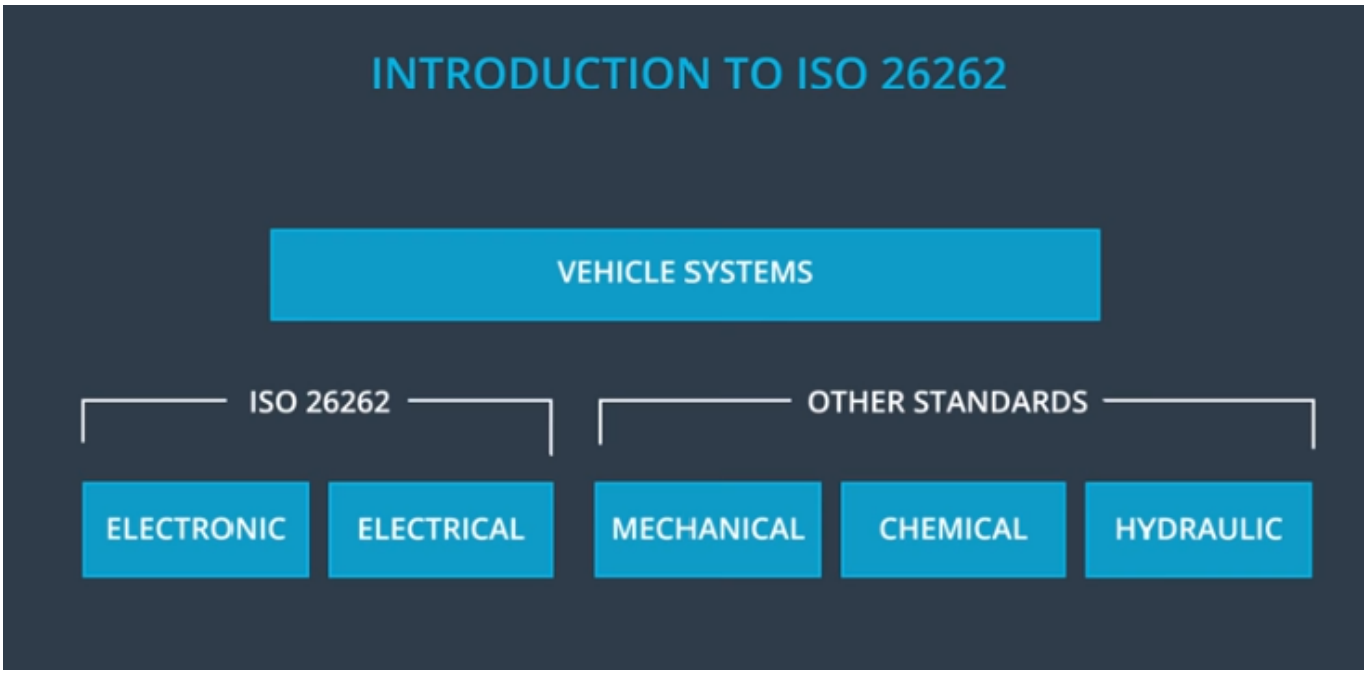
Do and Don'ts

- Functional safety only looks at the electrical and electronic system malfunction.
- Functional safety does not test for nominal performance.
- If a potential electrical malfunction could cause the battery fire, that could be a part of a functional safety analysis. The battery chemicals generally would be part of chemical system safety.
- Autonomous vehicle technology is so new that standards like ISO 26262 do not yet even consider certain issues related to self-driving cars such as machine learning algorithms.

The Basics of Functional Safety

- Identify Hazards
- Evaluate the risk
- Using System Engineering to Lower Risk

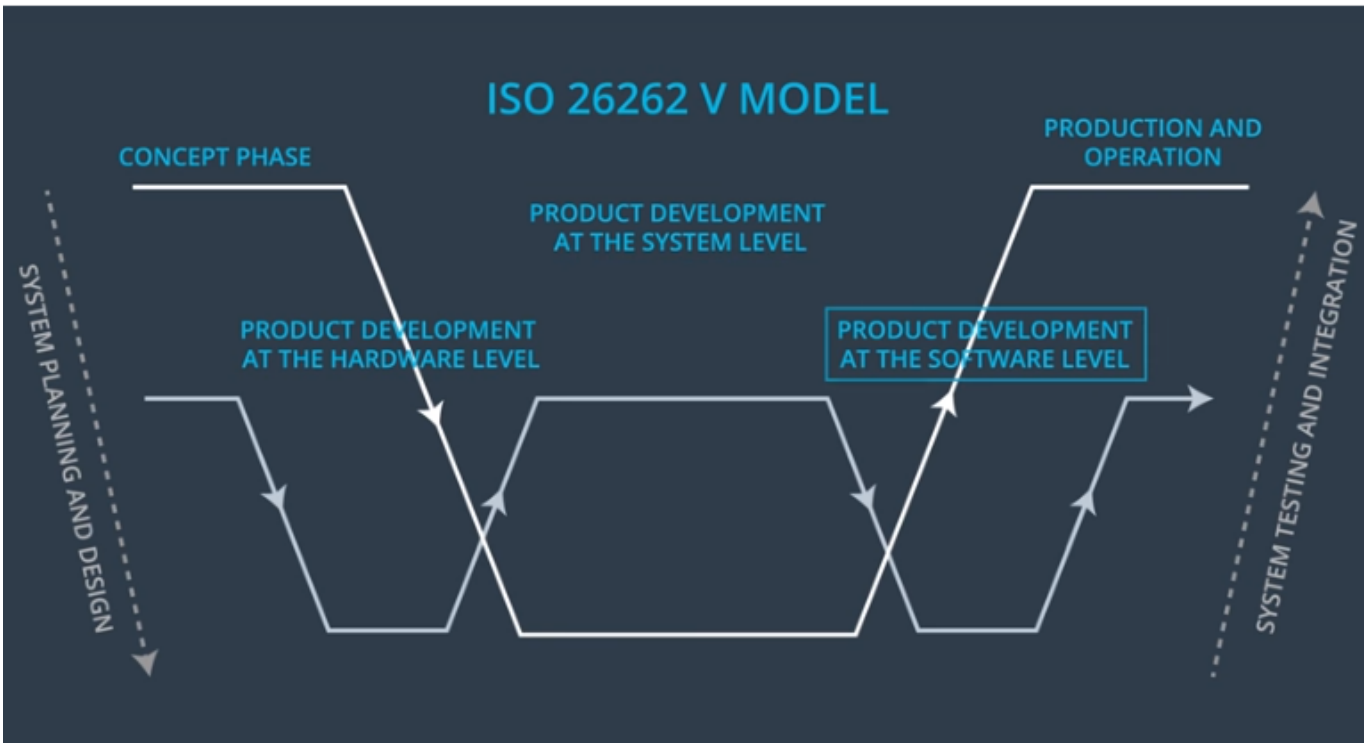
ISO 26262



The ISO 26262 functional safety standard follows the V model.

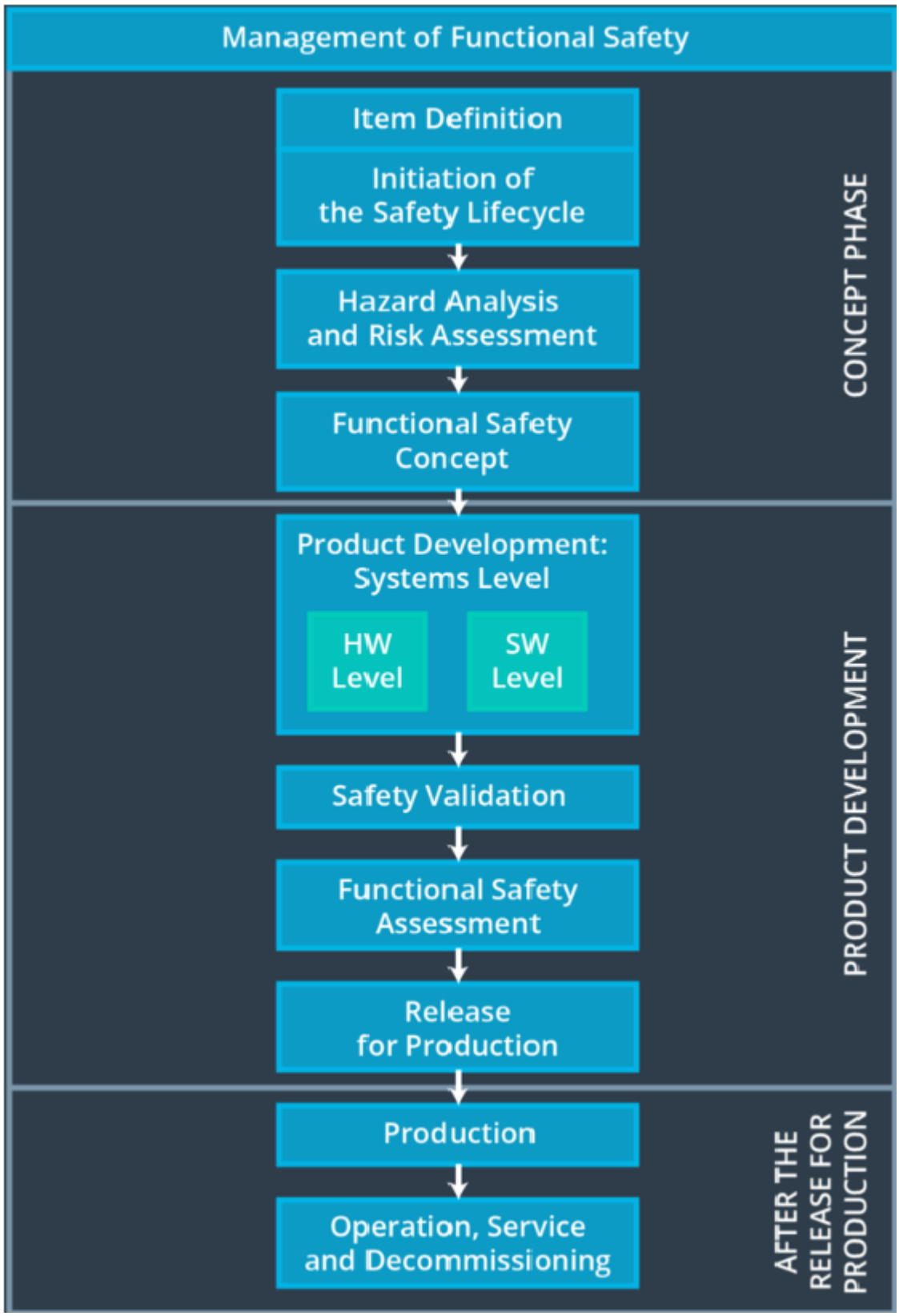
- *Requirements engineering* Define what the system is going to do
- *Designing or modifying a system architecture* Design what the system will look like
- *Test the system* to make sure it behaves as expected
- *Integrate the system* into larger systems

V Model



Flattened V Model

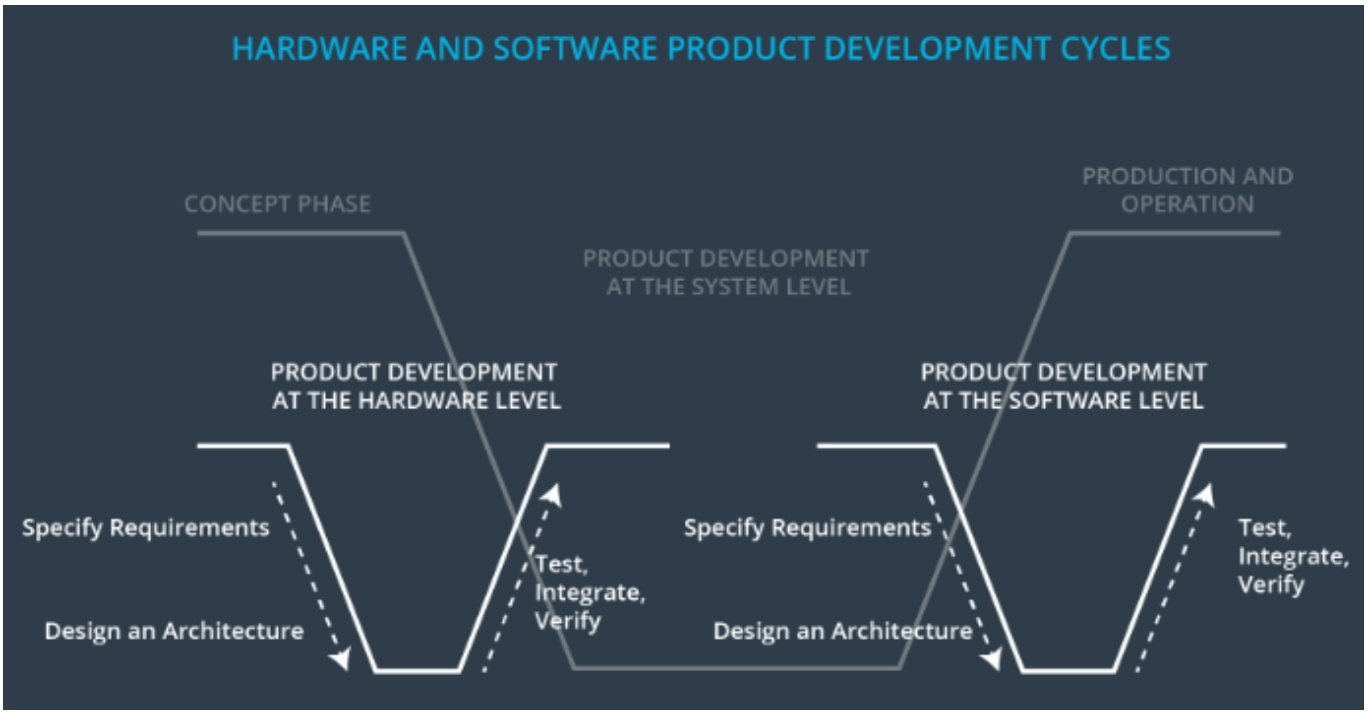
Flatten out the V model to see it from a linear perspective.



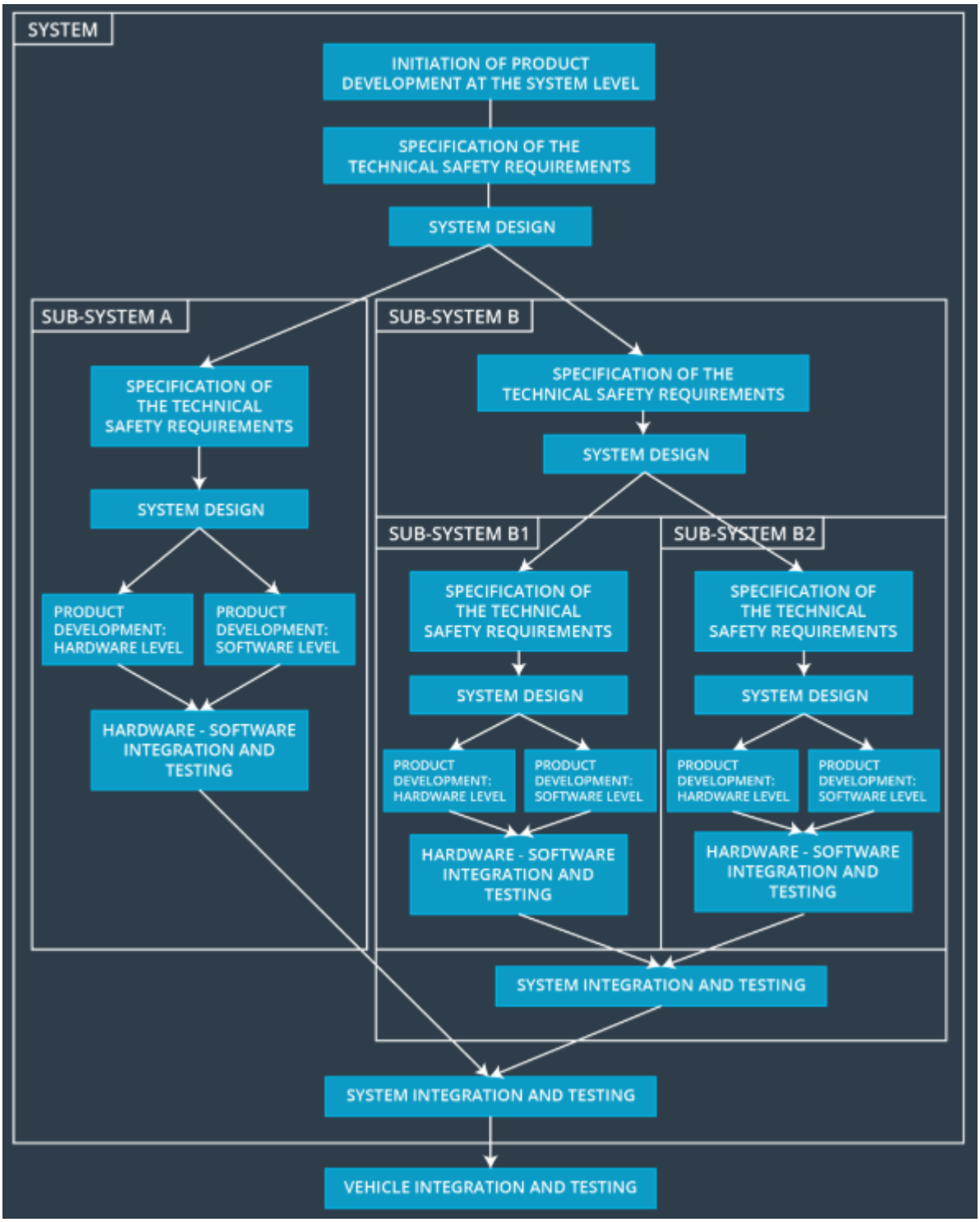
Hazard Analysis and Risk Assessment

ASIL

Hardware and software



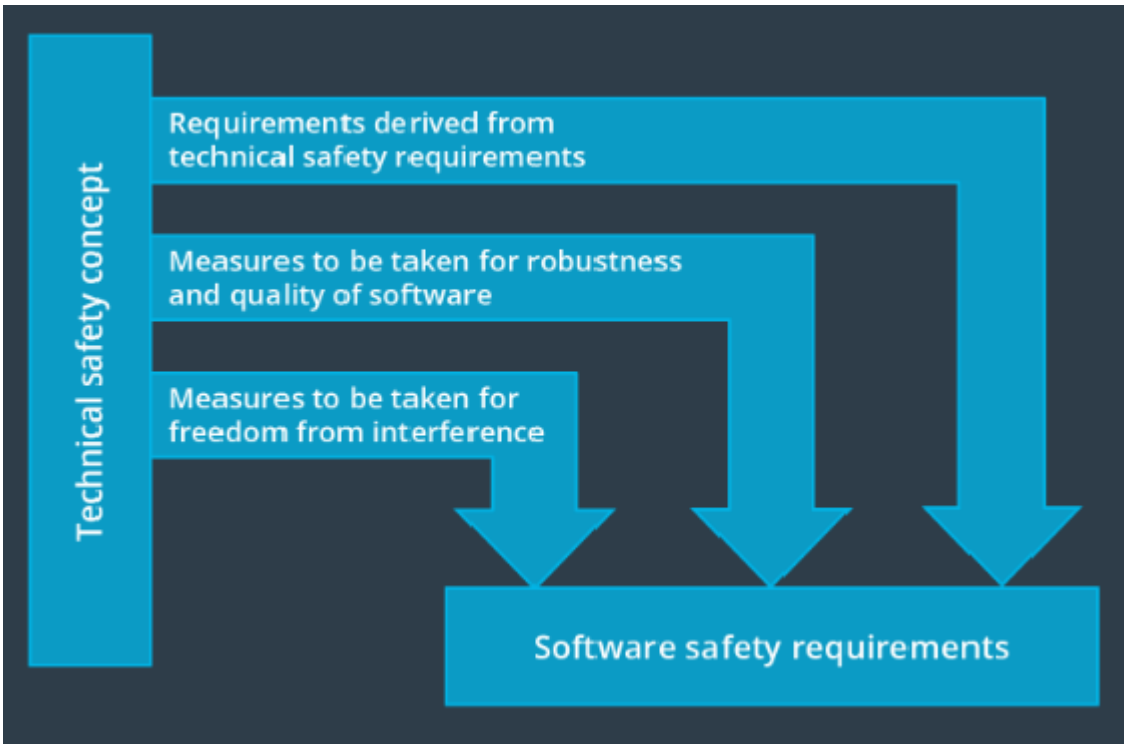
Functional safety project



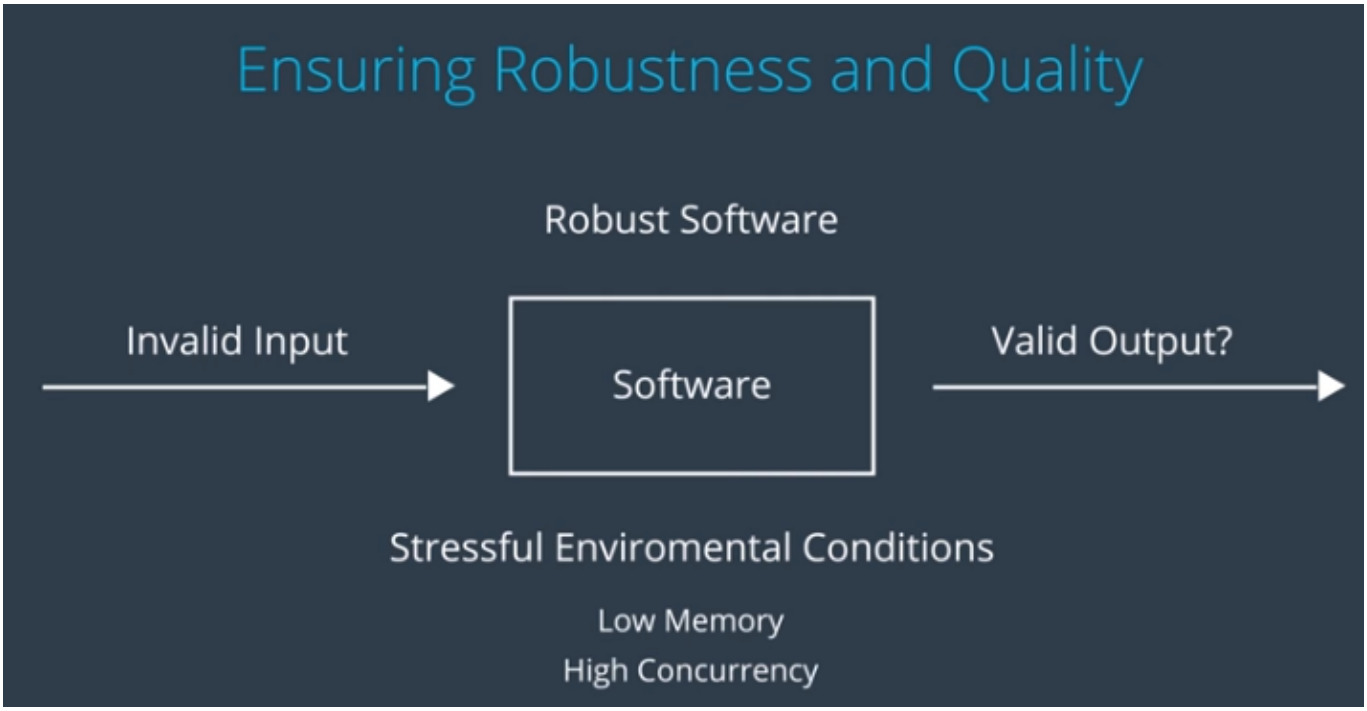
Software safety requirements

The software requirements are much more specific than technical requirements. Software requirements specify variable names, signal paths and software protocols and mechanisms.

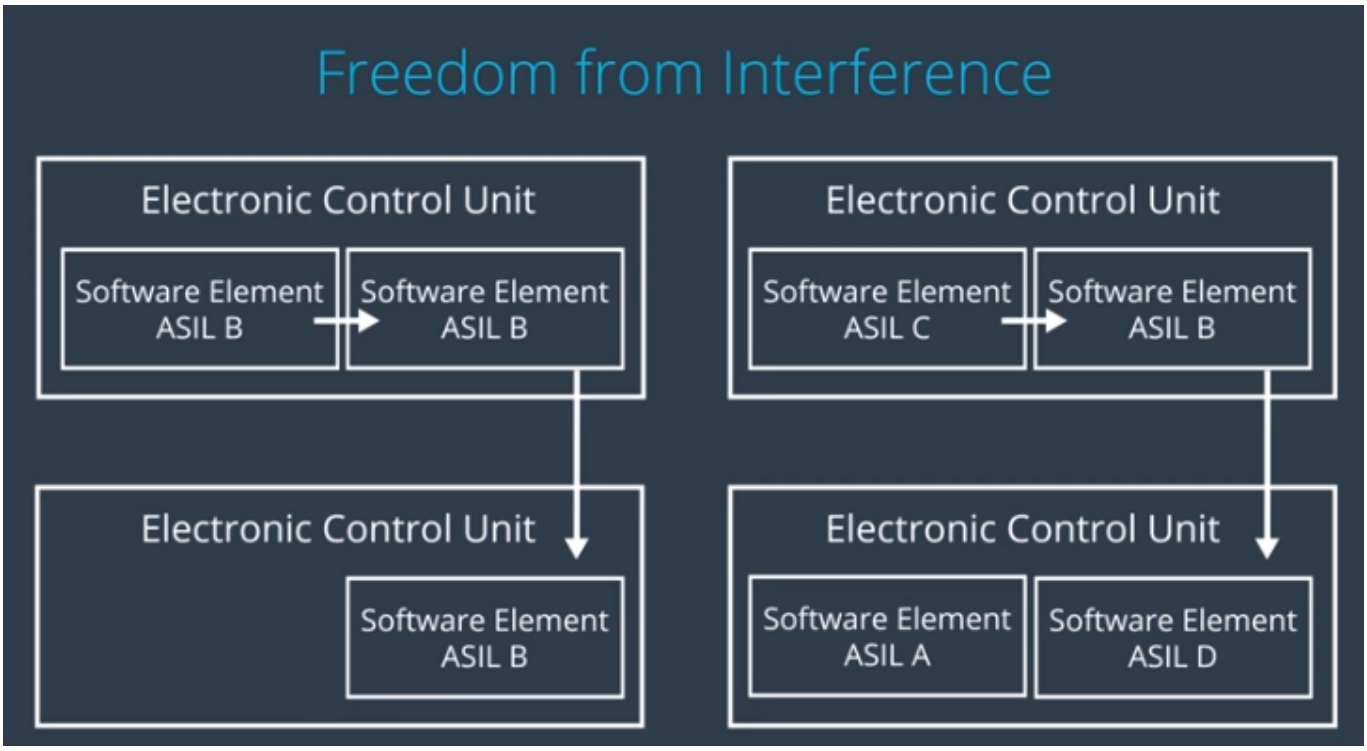
Sources of Software Safety Requirements



Software Robustness and Quality



Freedom from Interference



Types of interference

- Spatial interference
- Temporal interference
- Communication interference

Project Reference

Technical safety requirement

Software safety

In the next section we will discuss more about software safety