Model-Based Software Design

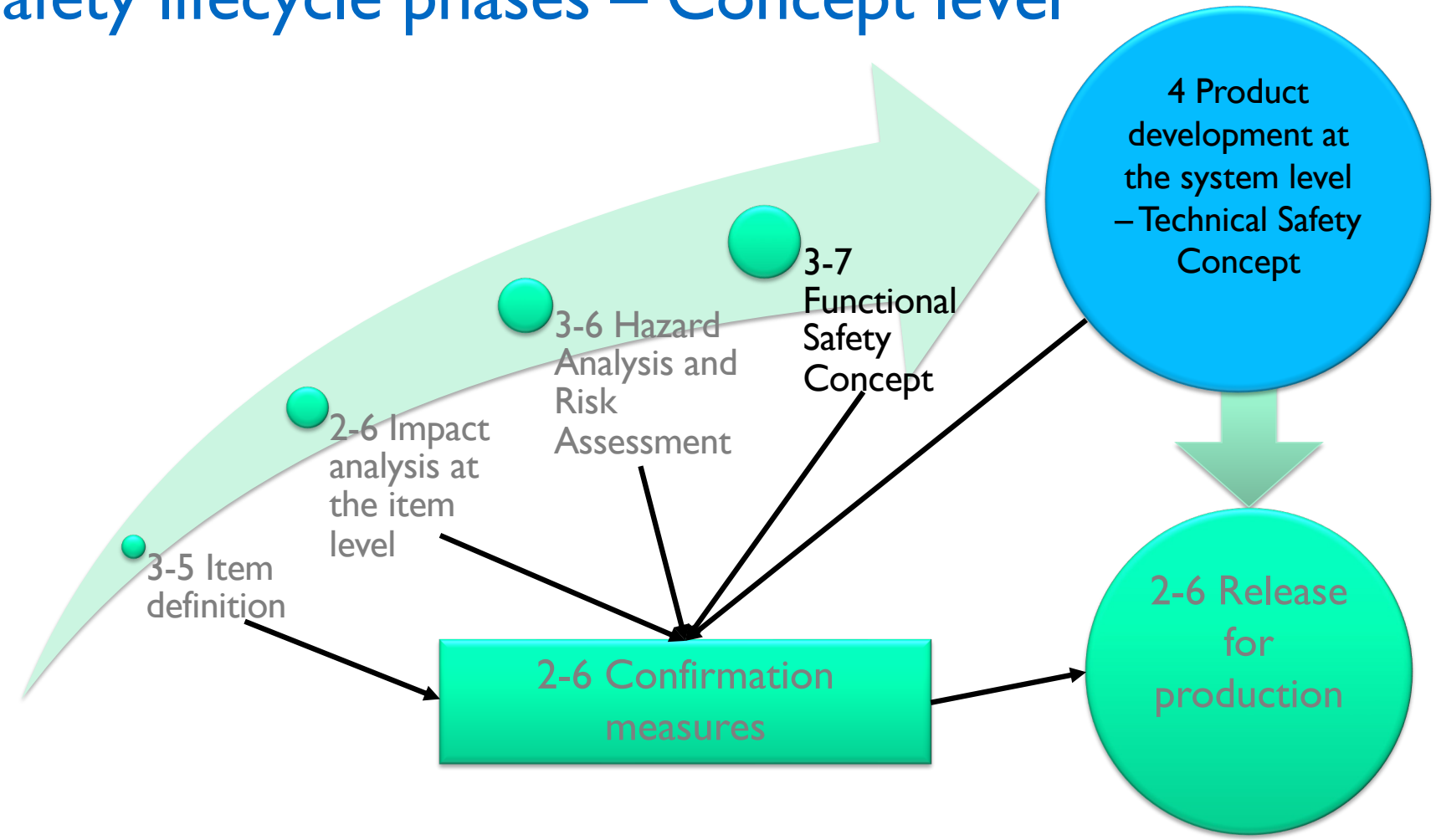
Assignment #3

Jacopo Sini
Politecnico di Torino
Dip. Automatica e Informatica
jacopo.sini@polito.it

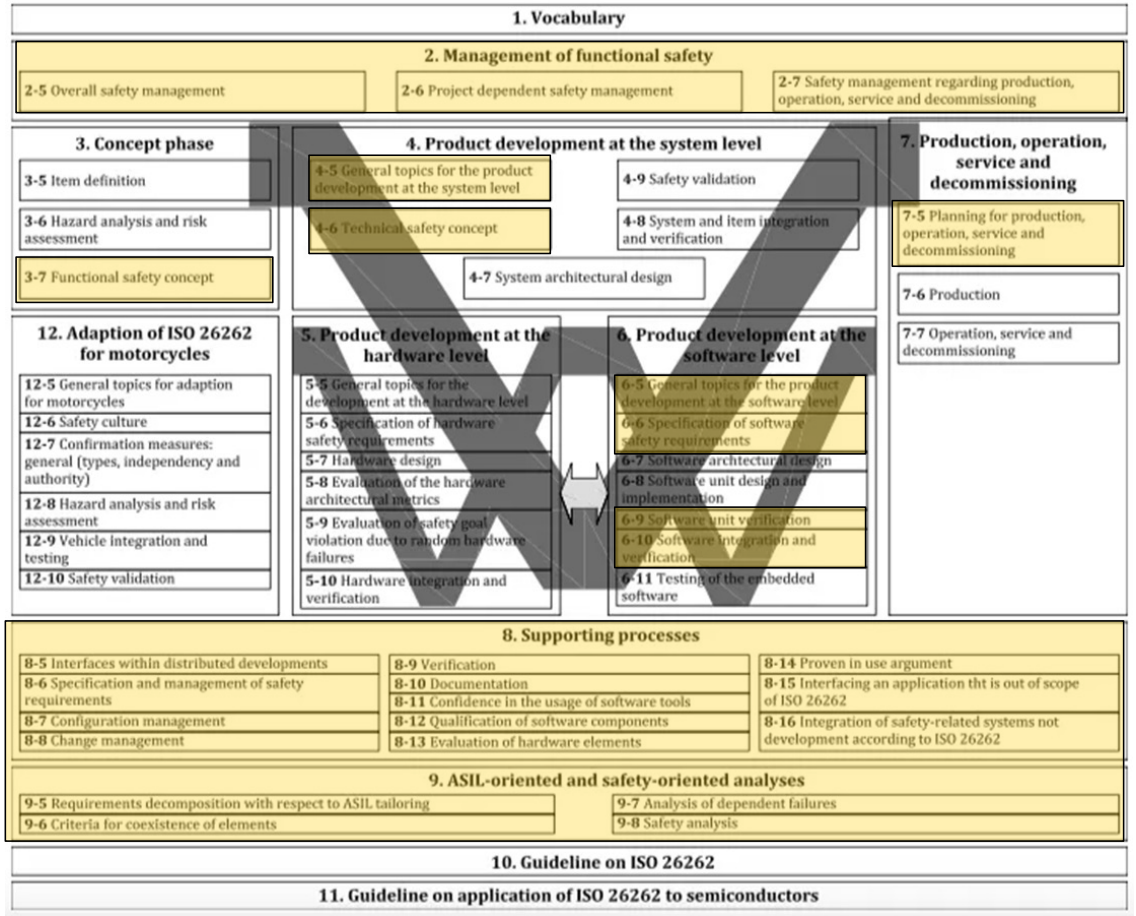
Laboratories organization

- 4 Assignments on the One pedal system:
  - **#1** Item identification and Hazard Analysis and Risk Assessment
    13/03/2025 Room 11T – 20/03/2023 Room 11T - Deadline: ~~06/04/2025~~ 16/04/2025.
  - **#2** Controller and physical model development by MathWorks Simulink (version 2024b)
    27/03/2025 Room 11T – 03/04/2025 Room 11T – 10/04/2025 Room 11T - Deadline: 14/05/2025.
  - **#3** Functional Safety Concept - Implementation of the safety functions in the controller
    17/04/2025 Room 11T 08/05/2025 Room 11T - Deadline: 14/05/2025 (updated).
  - **#4** Code generation (Controller only) and implementation on Arduino (simulated with SimulIDE)
    15/05/2025 Room 11T - Deadline: 01/06/2025.

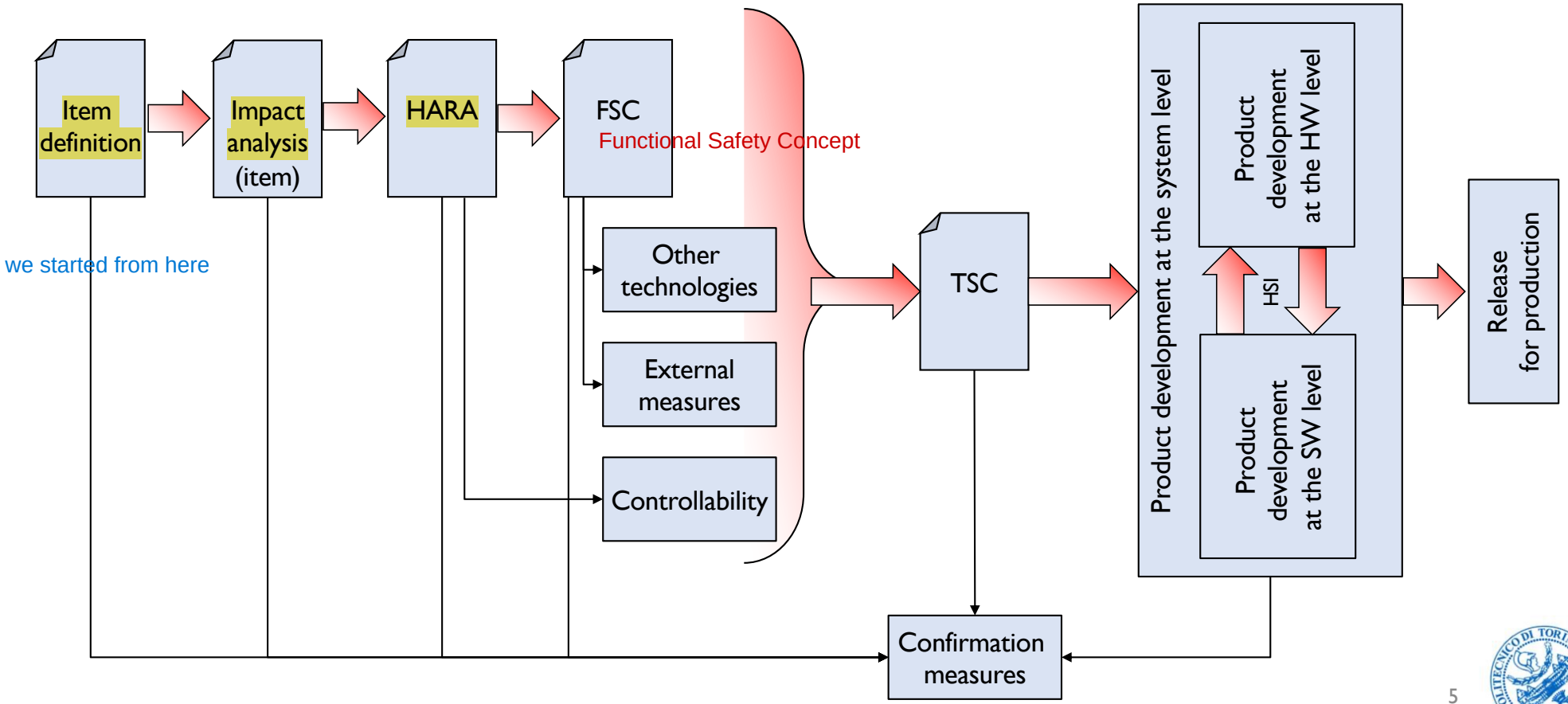
Safety lifecycle phases – Concept level



Phases under consideration for safety activities planning

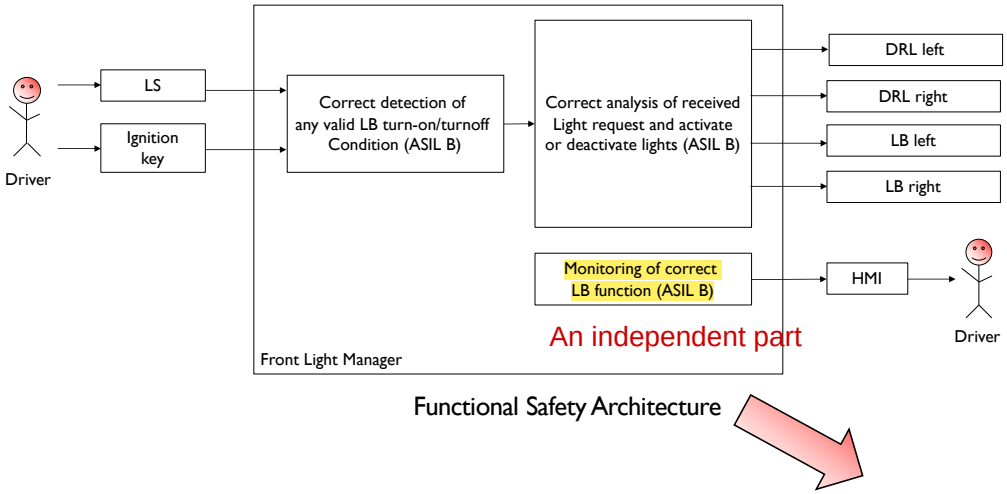


Overall project-dependent safety management



Architecture of the item – From functional…

First, make this one for one-pedal

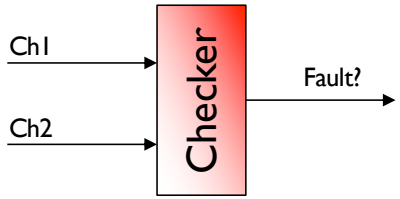


Functional Safety Architecture

?

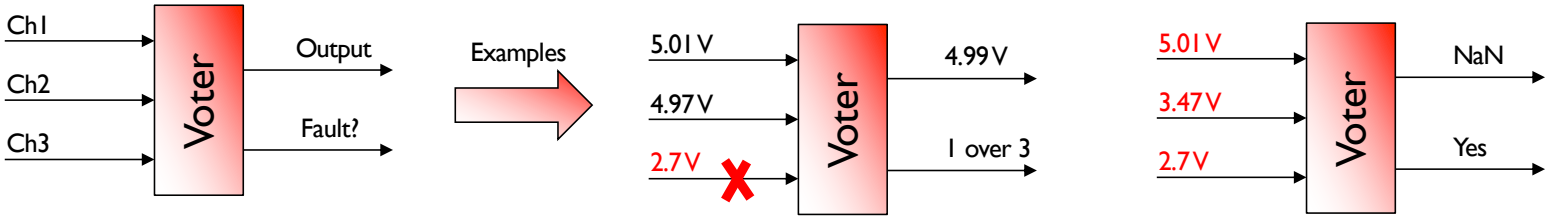
Safety concepts

- Fail-Safe approach
  - Continuous monitoring of the critical data paths, by redundancy and cross-checks between the paths/copies
  - Plausibility checks (in range, relationships between physical parameters)
    - For example, produced torque and currents in an electrical motor



If there is a mal function, we turn off the electric motor. However, in some applications, this may not be possible: if in an aircraft there is a malfunction in the engine, we cannot turn it off. Since the functionality itself is safety relevant.

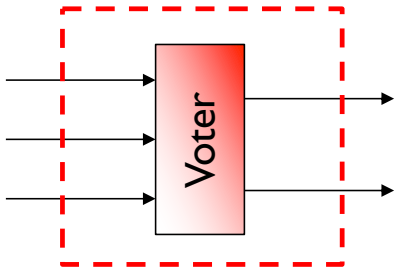
- Fail-operational
  - Critical data have multiple paths (channels), allowing for having at least three different sources (TRM, Triple Redundancy Module) directly measured or indirectly computed from other measurements for which physical relationships are known, given that these measurements are not already considered as a path in the TRM.
  - The channels shall guarantee Freedom From Interferences FFI (not share a common root failure cause) between each other.
  - Voting is needed to exclude the outlier channel or, if the channels all disagree, detect the failure.



It's not enough just to check whether there is misbehavior. We need to put in place some strategies to continue the functionality at the cost losing some performance.

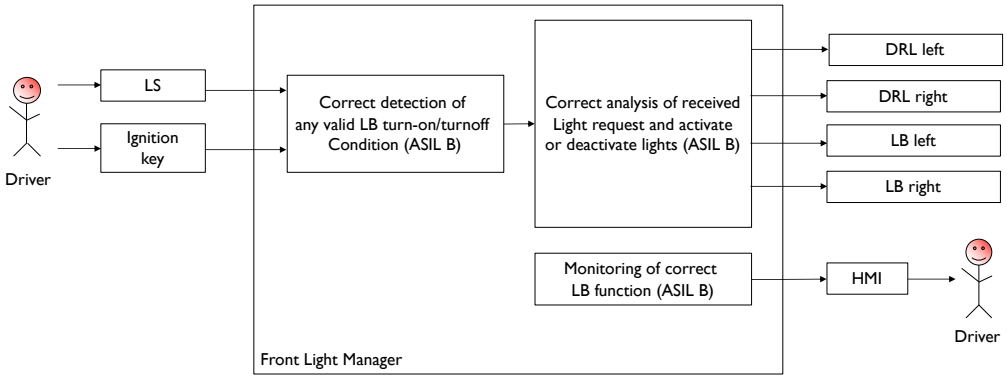
Testing Use Simulink test suit for testing.

- Unit tests are performed on each single software component, by isolating it.

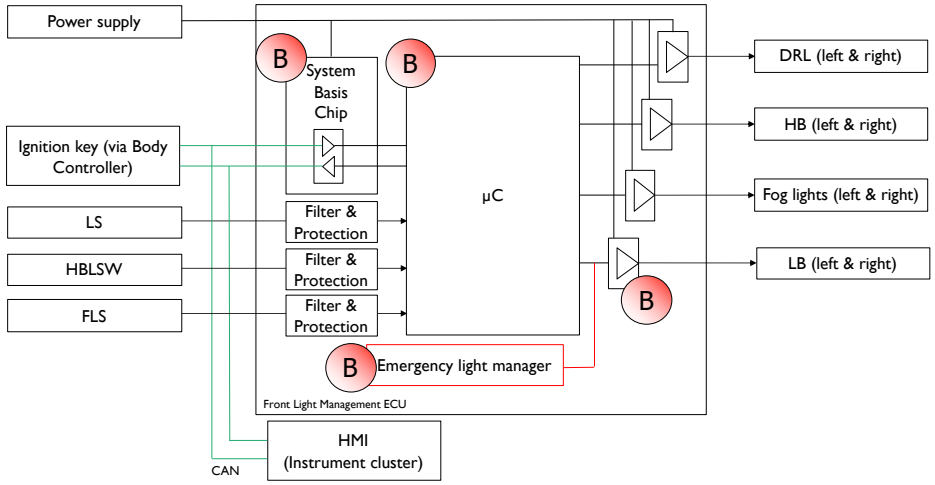


- In the integration testing, the software components are tested while interacting between each other.
- In both unit and integration tests, verify:
  - That the checkers are capable of detecting the faults.
  - That the triggered safety mechanisms are capable of bringing the system into the appropriate safe state.
  - For TRMs, that the outlier is properly excluded and, in case all channels disagree, that they properly recognize the faults.

Architecture of the item – … to technical



Functional Safety Architecture

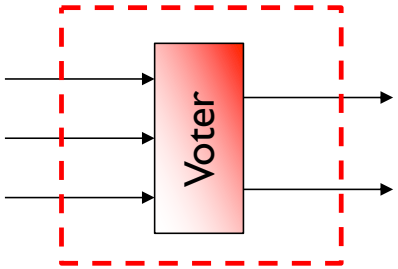


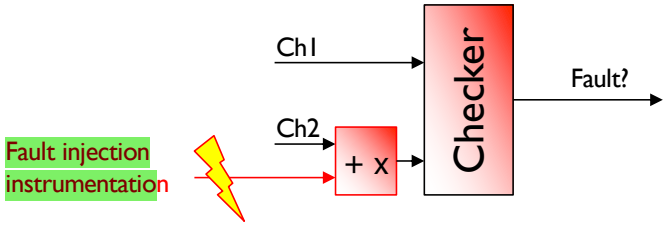
Preliminary [Technical] Architecture

Objectives of this laboratory

The objectives of this laboratory are to:

- Perform some parts of the **Functional** and **Technical Safety Concept** analysis, according to ISO26262, of a "one pedal controller" for a car.
- Implement some of the *safety concepts* in the Simulink model of the controller developed for the Assignment #2.
- Perform unit and integration tests on the implemented safety-related functionalities.
  - In the report, insert screenshots to demonstrate the test results.
  - For the unit test it is suggested to use Simulink Test environment which allows getting the coverage while, for the integration tests, it is suggested to inject faults in the data paths by directly instrumenting the model.





for the integration

Thanks for your attention