FUNCTIONAL SAFETY ANALYSIS OF ADAS/AD SYSTEMS

Frank Benders, Geert Verhaeg

Systems Architecture Study Group Meeting, Océ, Venlo, 5 June 2018

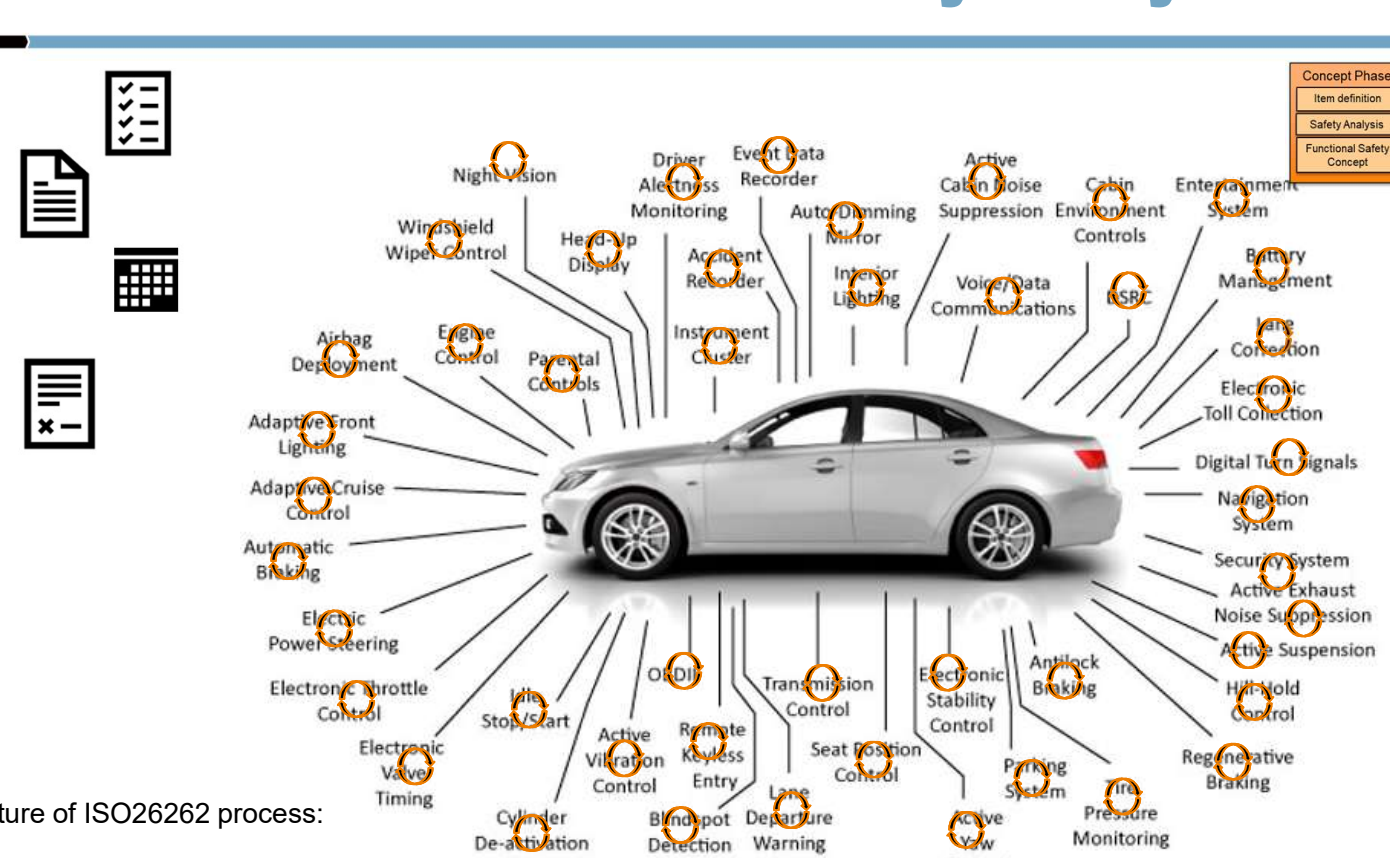
TNO innovation for life

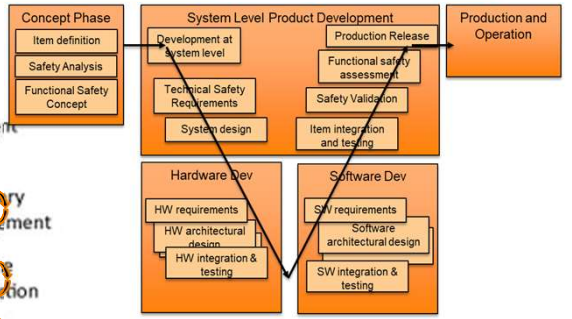
Motivation: System Safety Analysis

The ISO26262 process:

Define Item → **Hazard Analysis & Risk Assessment** → **Define Safety Goals** → **Derive Functional Safety Requirements** → **Obtain Technical Safety Requirements** → **Testing System Compliance**

Motivation: Vehicular Safety Analysis

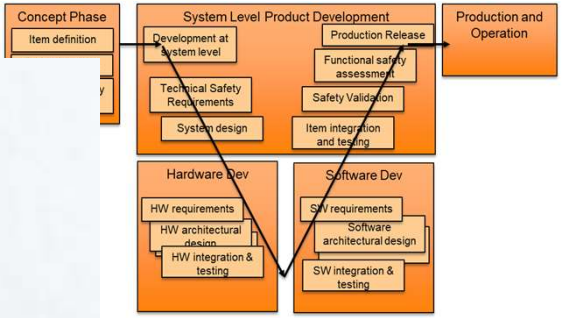




Picture of ISO26262 process:

Define Item → **Hazard Analysis & Risk Assessment** → **Define Safety Goals** → **Derive Functional Safety Requirements** → **Obtain Technical Safety Requirements** → **Testing System Compliance**

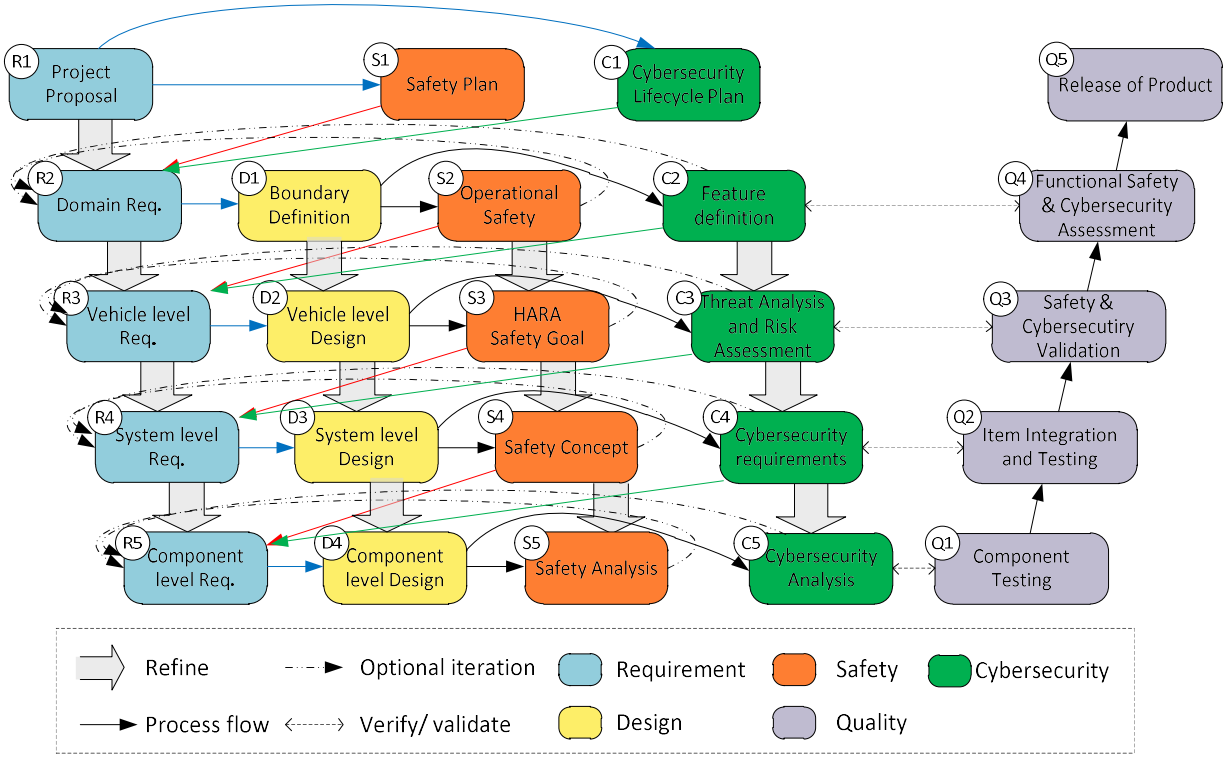
Motivation: Vehicular Safety Analysis



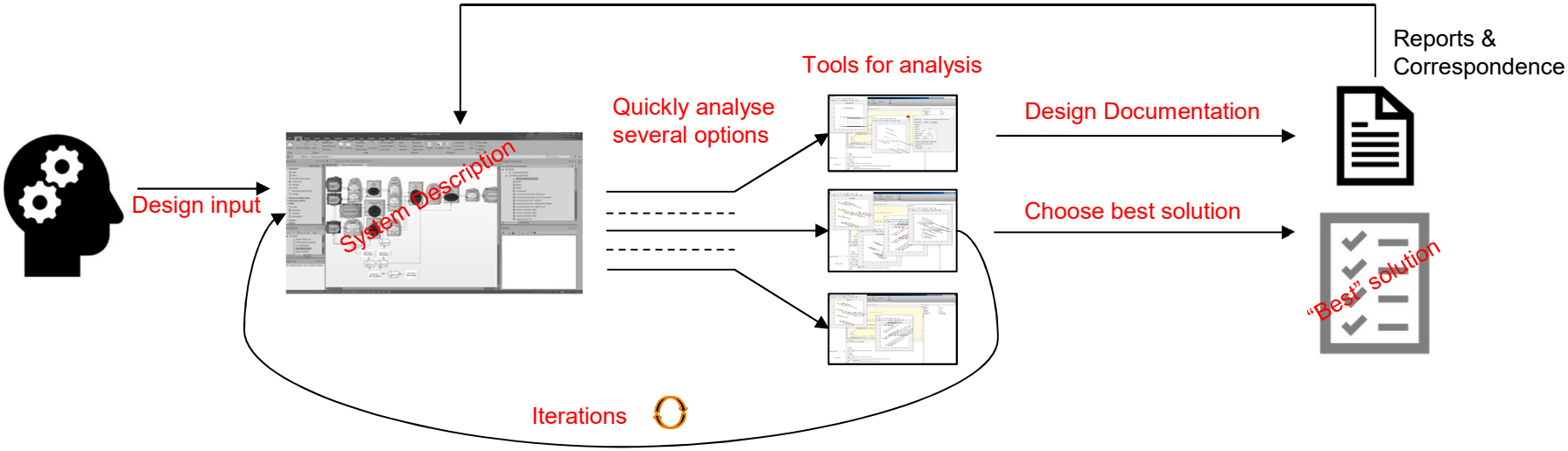
Picture of ISO26262 pro

Define Item → Hazard Analysis & Risk Assessment → Define Safety Goals → Derive Functional Safety Requirements → Obtain Technical Safety Requirements → Testing System Compliance

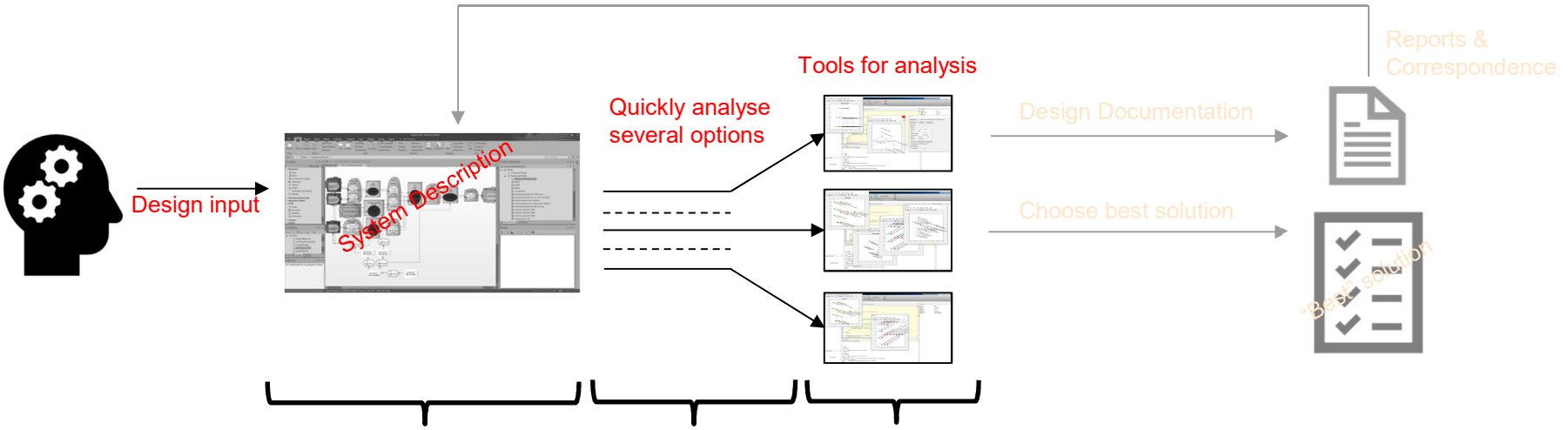
System engineering process - automotive



Motivation: Safety Analysis Tooling



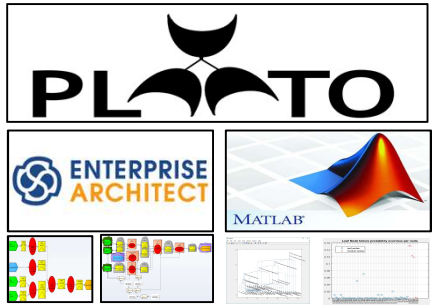
Tool: Focus



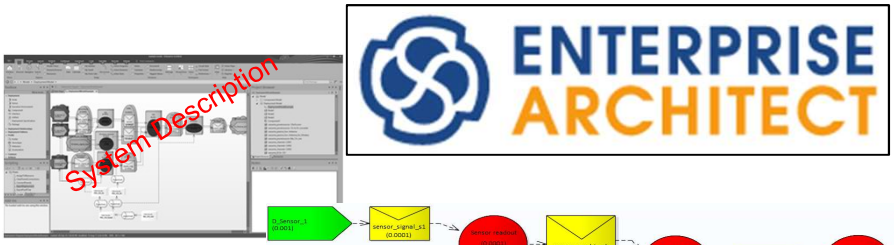
Develop a multi purpose system description

Set up the connection with tools for safety analysis

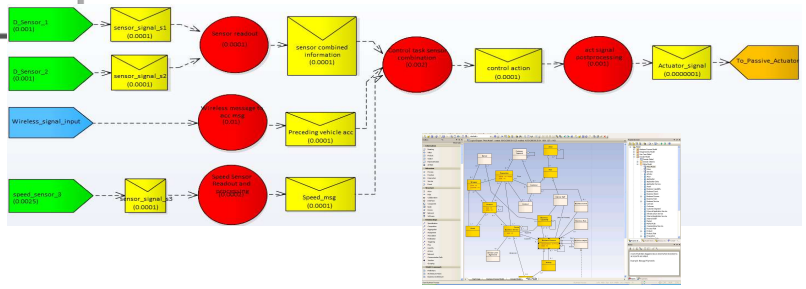
Develop tool for easy analysis



Tool: System Description

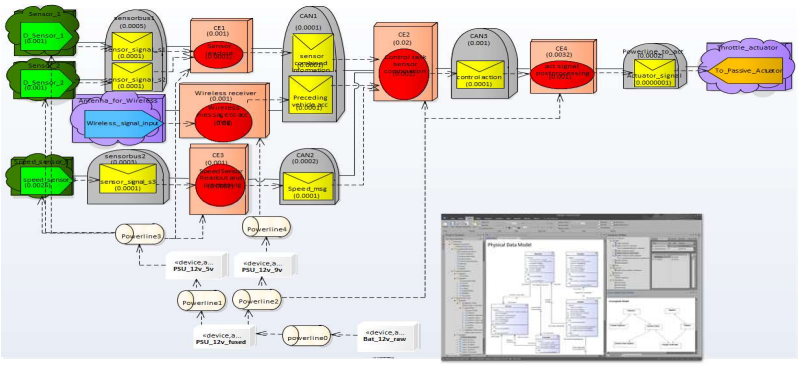


Function model



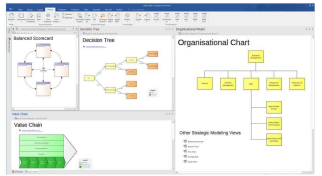
Hardware model

Deployment



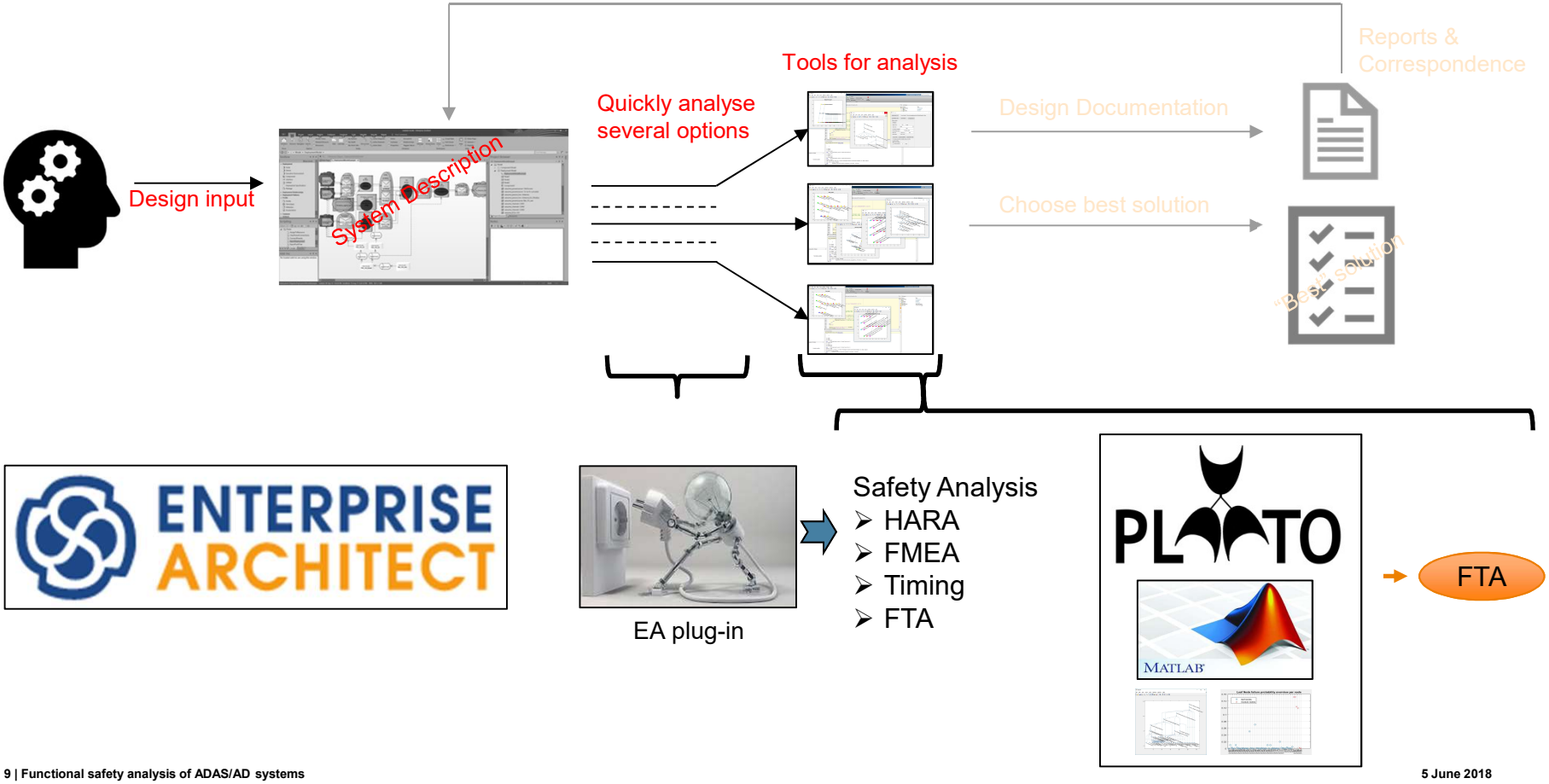
- Structure
- System Details
- Definitions
- Other Diagrams

- Assumptions
- Decisions
- Documentation

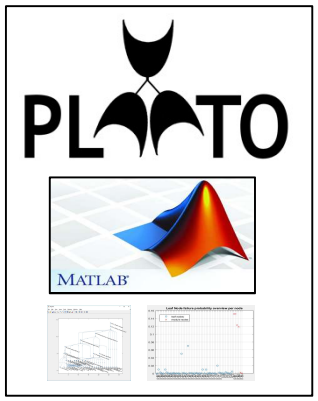


- Hazard Analysis and Risk Assessment
- Requirements
- Etc.

Tool: Connection to analysis



Tool: Fault Tree Analysis introduction



Fault tree analysis

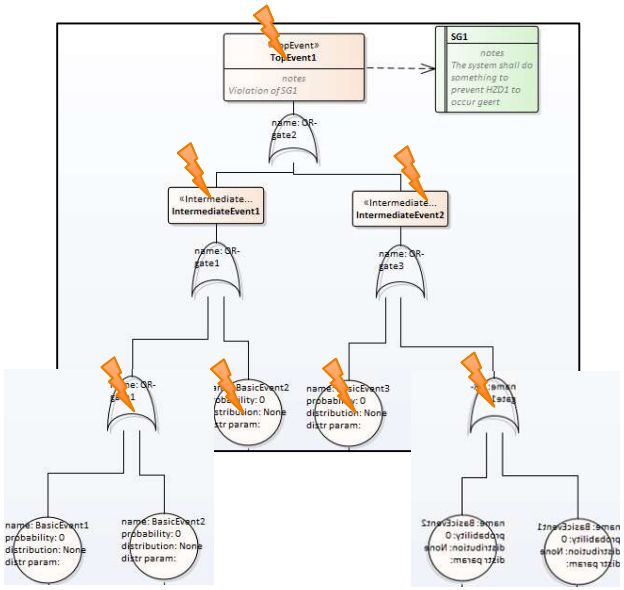
Top to bottom approach

Natural approach to work towards increasing detail

Scope can be chosen for proper level of abstraction

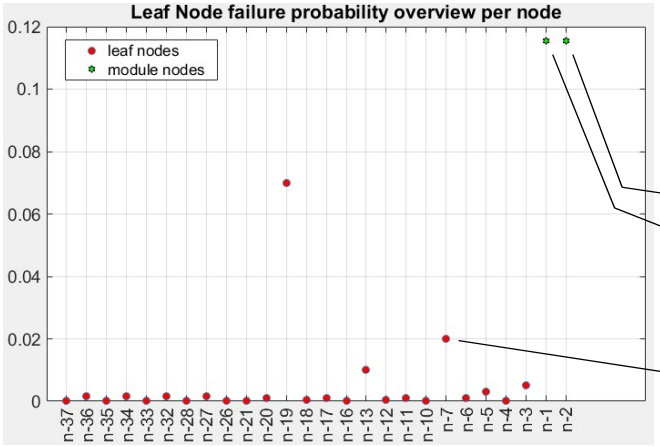
Automatable and extensible

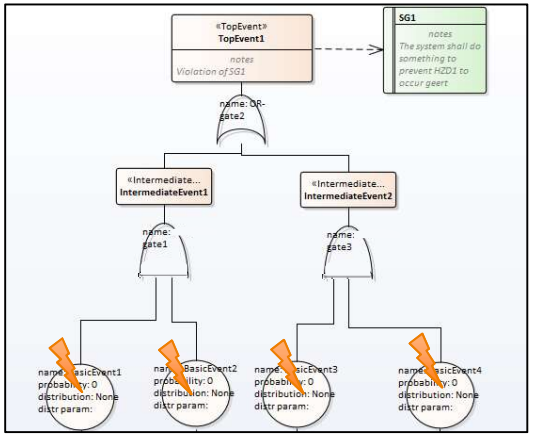
Gives quick insight into the susceptibility to faults

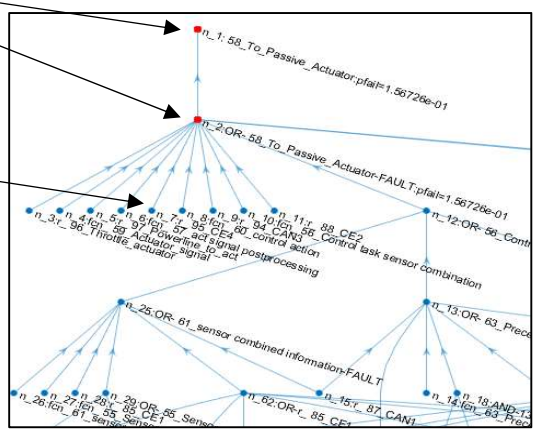


Tool: Fault Tree Analysis

- Fault Tree analysis options:
  - Cut-sets e.g. TOP = (A&B)|(C&D)
  - Independent structures
  - Probability of failure

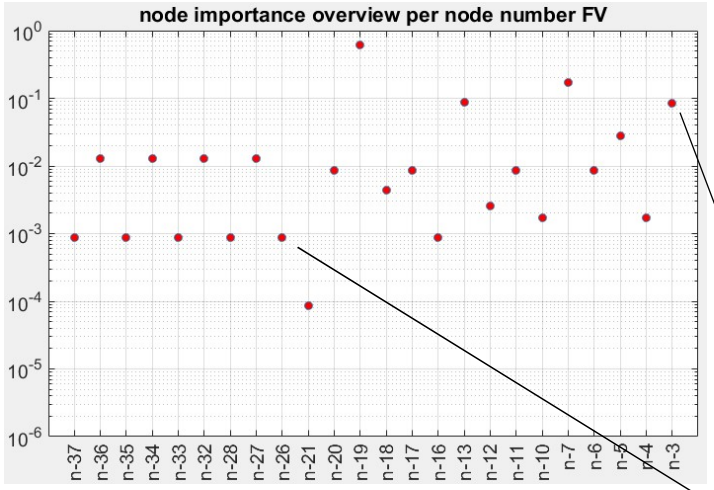


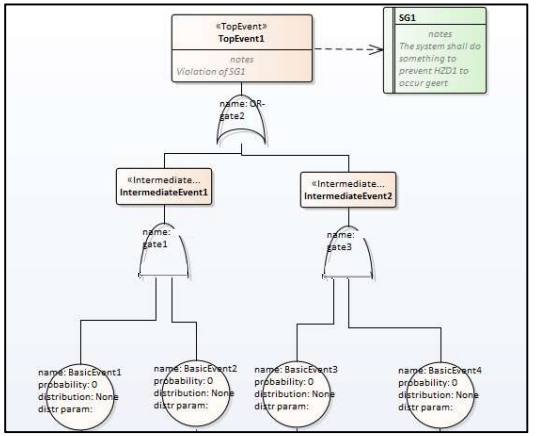


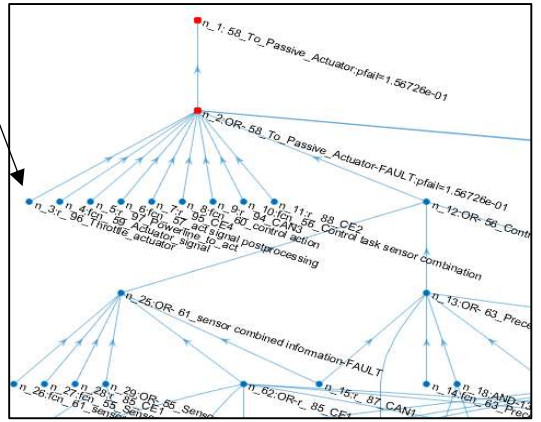


Tool: Fault Tree Analysis

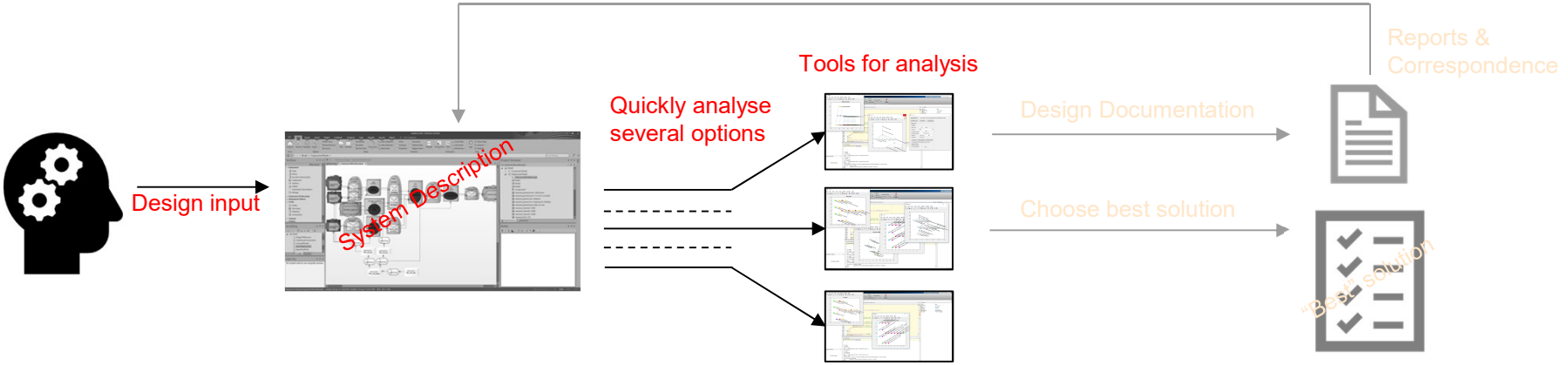
- FT analysis options:
  - Cut-sets e.g. TOP = (A&B)|(C&D)
  - Independent structures
  - Probability of failure
  - Importance metrics
    - Birnbaum
    - Fussell-Vesely







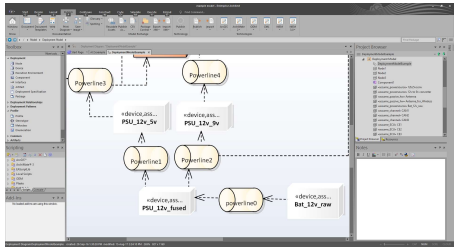
Tool: Next steps

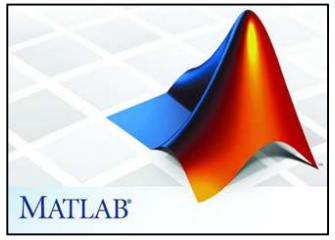


- HARA
- FTA
- FMEA
- Timing

- Test this tool
- Update the system model

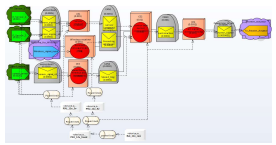
SUMMARY - Fault Tree Generation



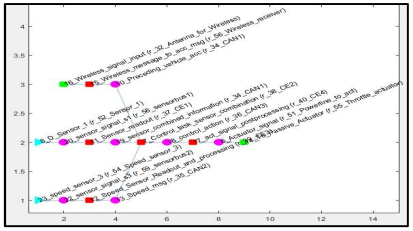


Function model

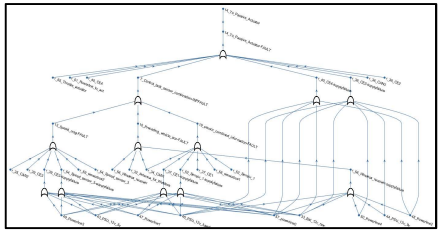
Deployment



System Description



Generate Fault Tree From System description

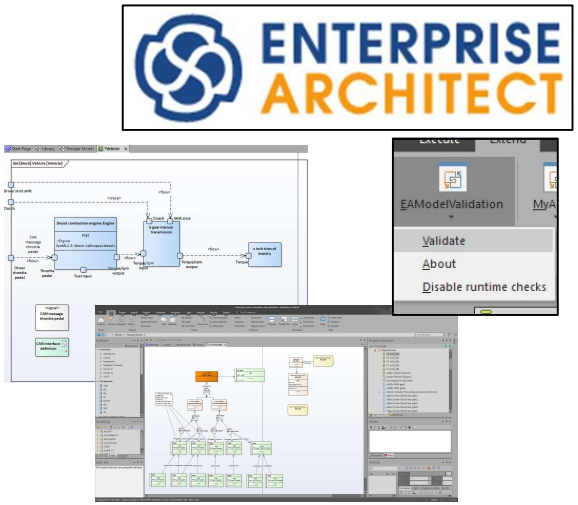


Fault-tree processing

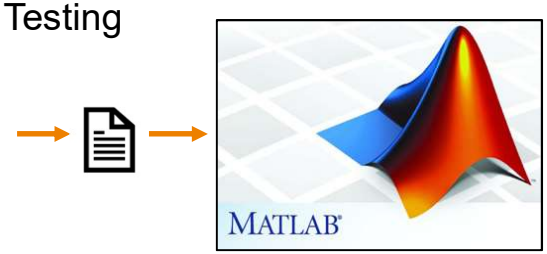
SUMMARY - Tooling overview

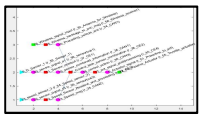
TNO innovation for life

Architecture description and validation

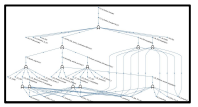


Documentation, Analysis of Structure and Safety and Testing





Generate Fault Tree from system description



Fault-tree processing

HARA/Requirements synchronization

HARA/Requirements

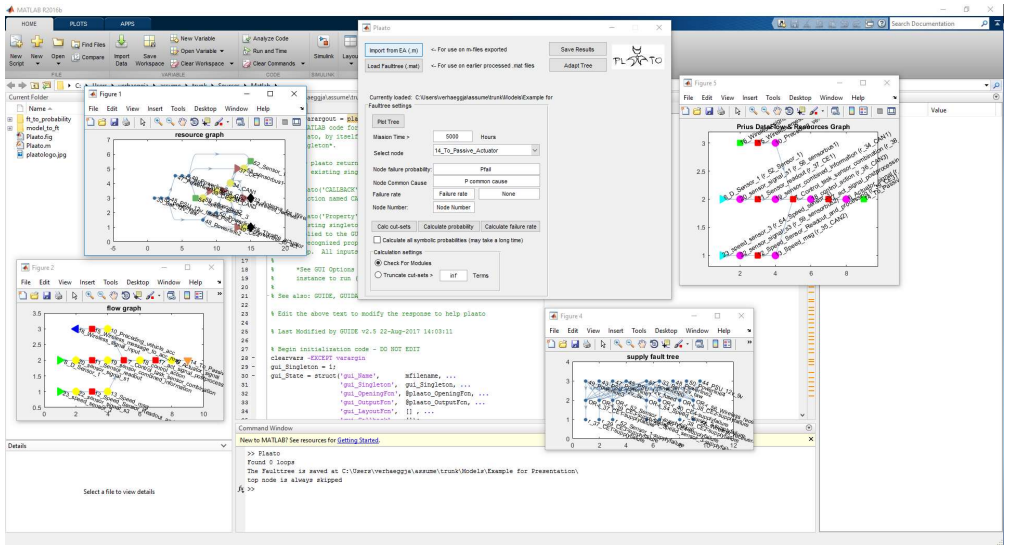
Functionality
Operational situation
Scenarios
Hazards
Hazardous event
Exposure
Safety Goal
Controllability
Risk
Requirements
ASIL

Document generation & Linking

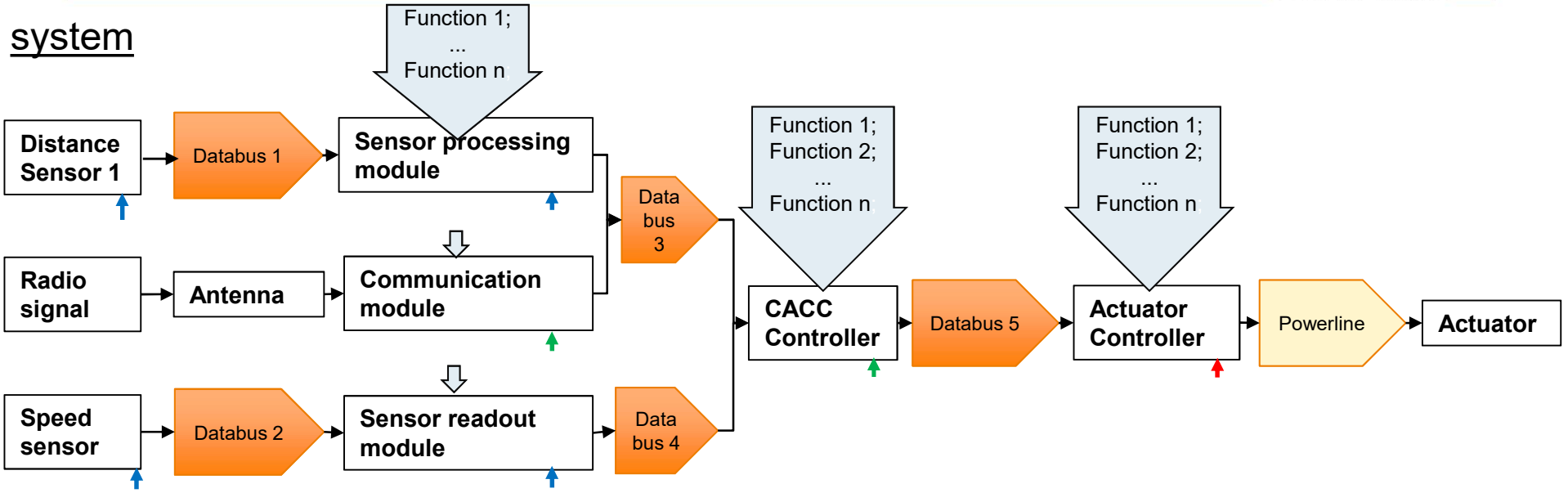
Testing and validation

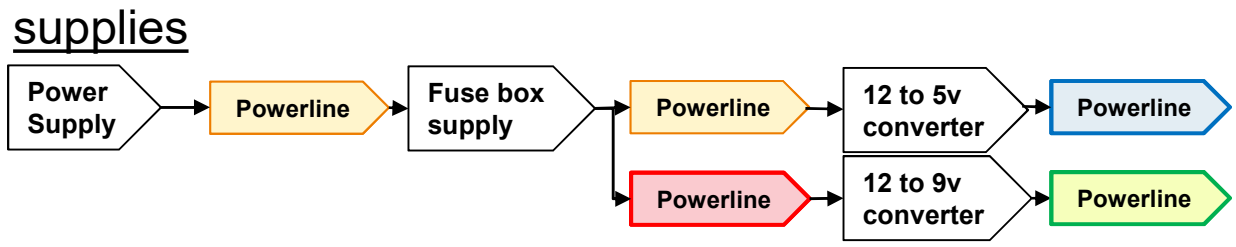
Demo: content

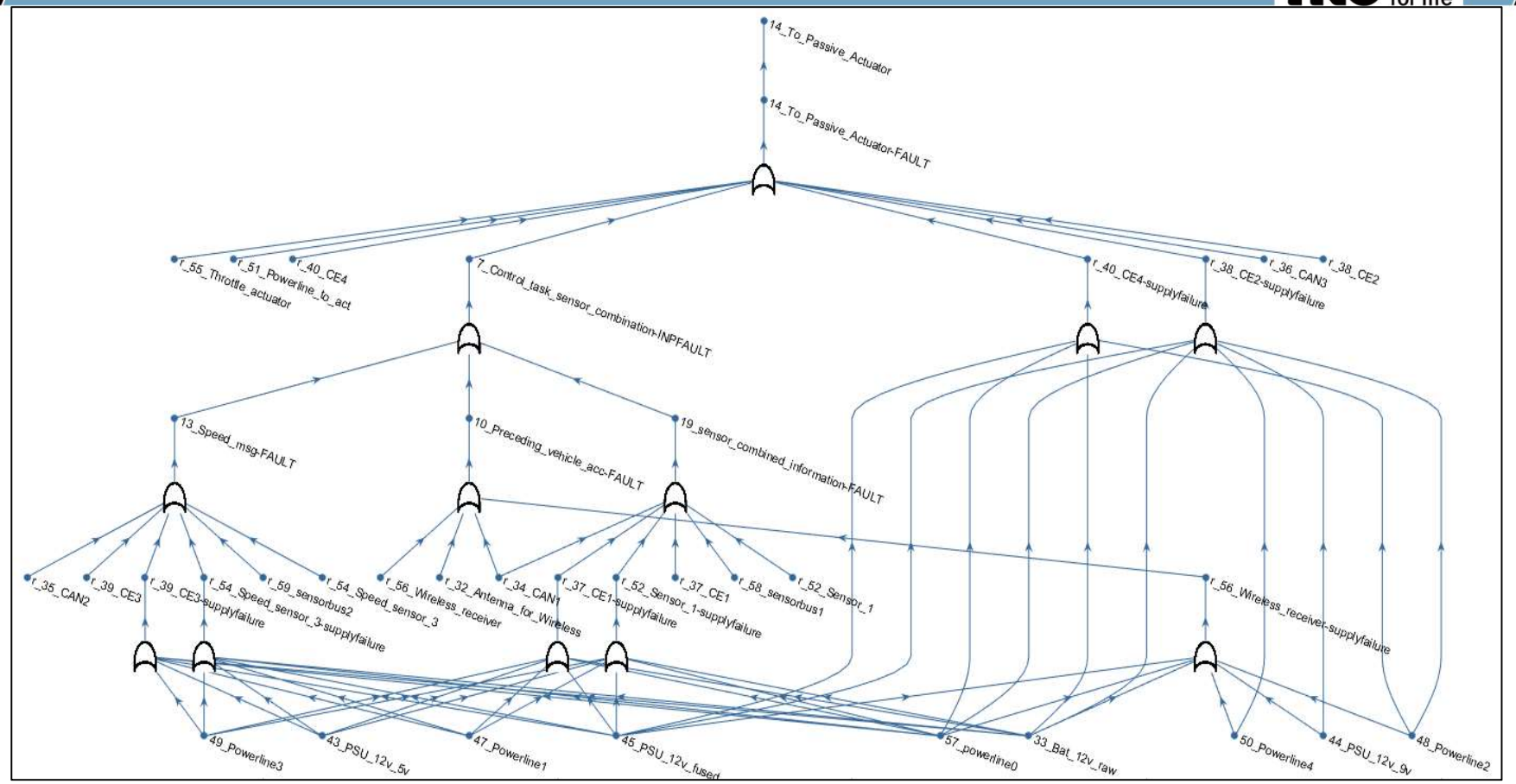
- A short demo of the tool
- Analysis of a simplified version of a CACC system



Non-Redundant CACC System Model

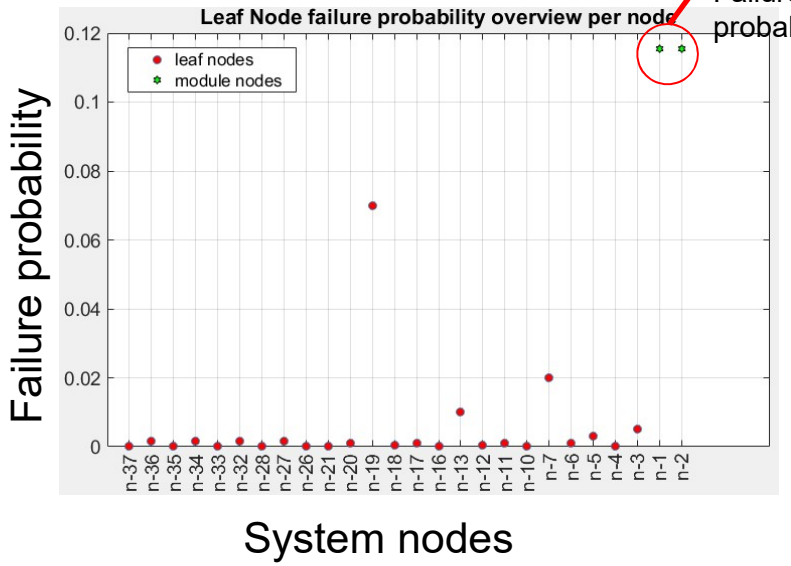


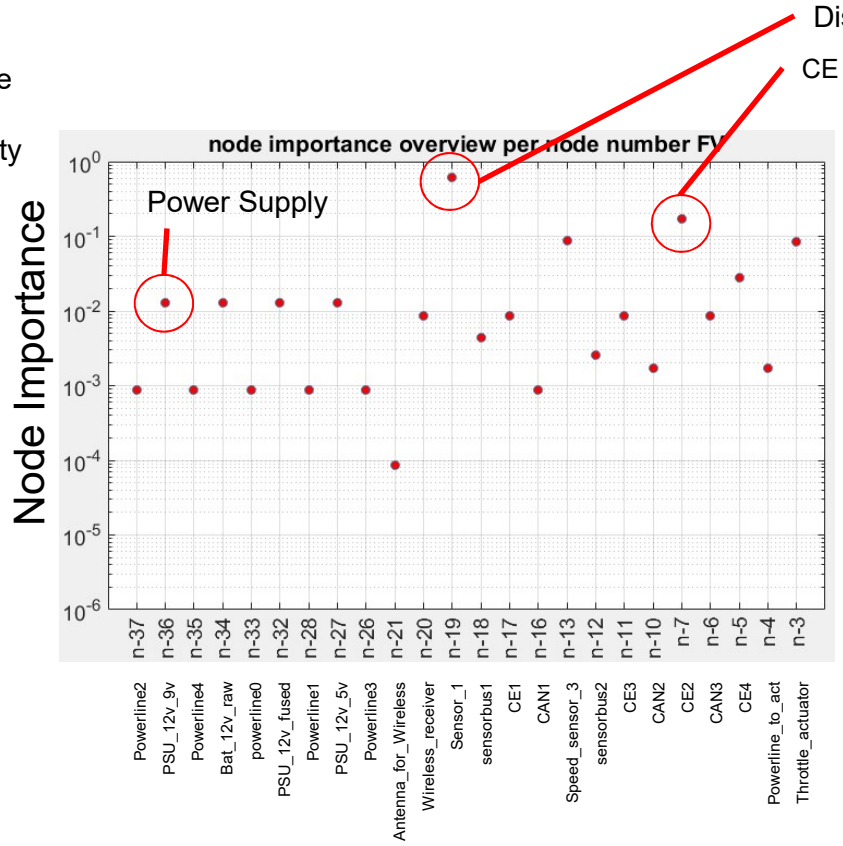



14_To_Passive_Actuator
14_To_Passive_Actuator-FAULT
r_55_Throttle_actuator
r_51_Powerline_to_act
r_40_CE4
7_Control_task_sensor_combination-INPFAULT
r_40_CE4-supplyfailure
r_38_CE2-supplyfailure
r_36_CAN3
r_38_CE2
13_Speed_msg-FAULT
10_Preceding_vehicle_acc-FAULT
19_sensor_combined_information-FAULT
r_35_CAN2
r_39_CE3
r_39_CE3-supplyfailure
r_54_Speed_sensor_3-supplyfailure
r_59_sensorbus2
r_54_Speed_sensor_3
r_56_Wireless_receiver
r_32_Antenna_for_Wireless
r_34_CAN1
r_37_CE1-supplyfailure
r_52_Sensor_1-supplyfailure
r_37_CE1
r_58_sensorbus1
r_52_Sensor_1
r_56_Wireless_receiver-supplyfailure
49_Powerline3
43_PSU_12v_5v
47_Powerline1
45_PSU_12v_fused
57_powerline0
33_Bat_12v_raw
50_Powerline4
44_PSU_12v_9v
48_Powerline2

Analyse FTA results

Failure probability non-redundant system:
0.11561

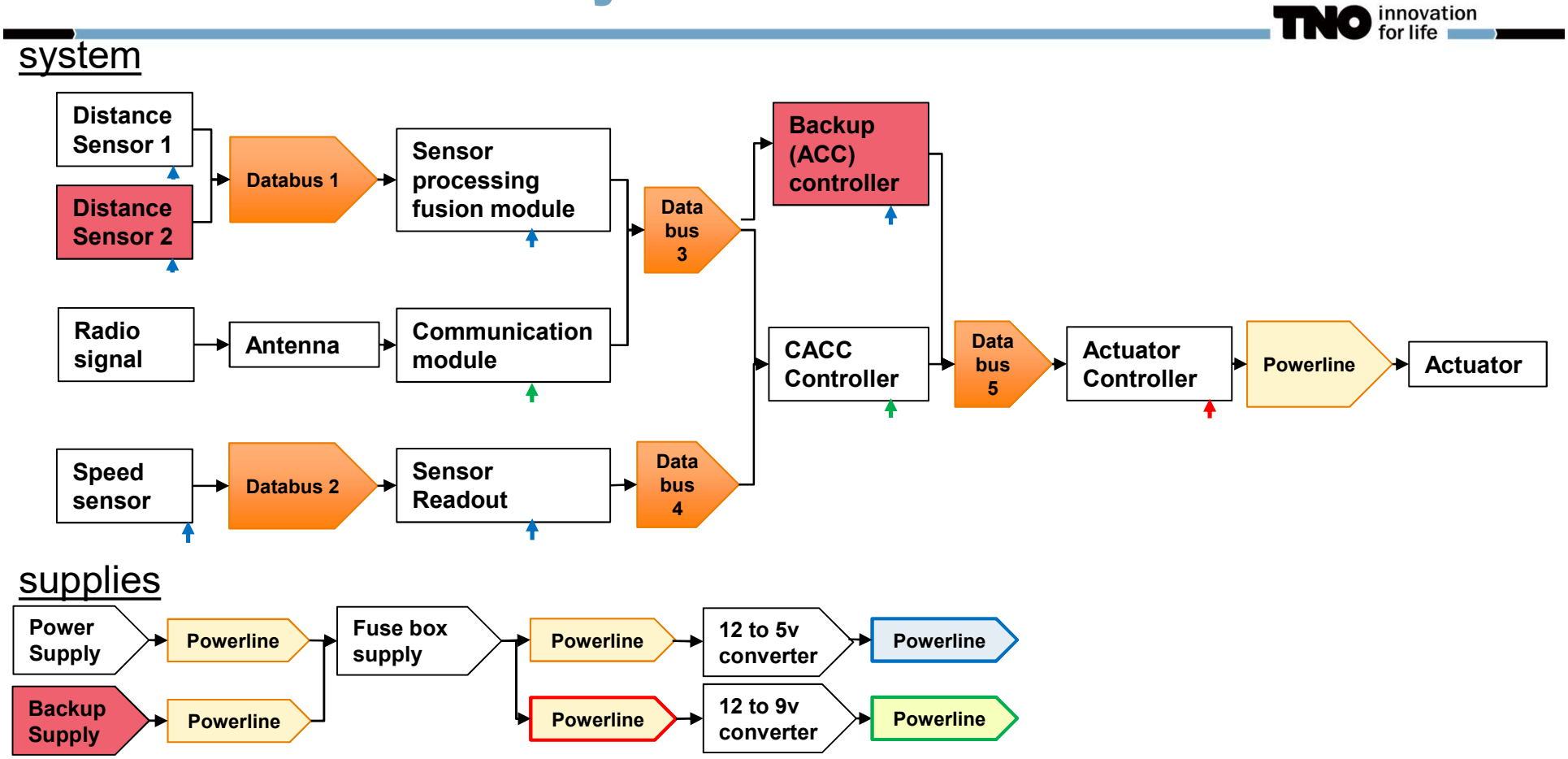




Redundant CACC System Model

- After PLAATO analysis, the following elements were added to the system
  - Backup sensor for Sensor1 (Distance measurement)
  - Backup control function CE1 (CACC controller)
  - Backup battery
  - Additional elements have a failure rate equal to the existing elements

Redundant CACC System Model



System Analysis: Failure Probability

Failure probability:

Non-redundant system: 0.11561

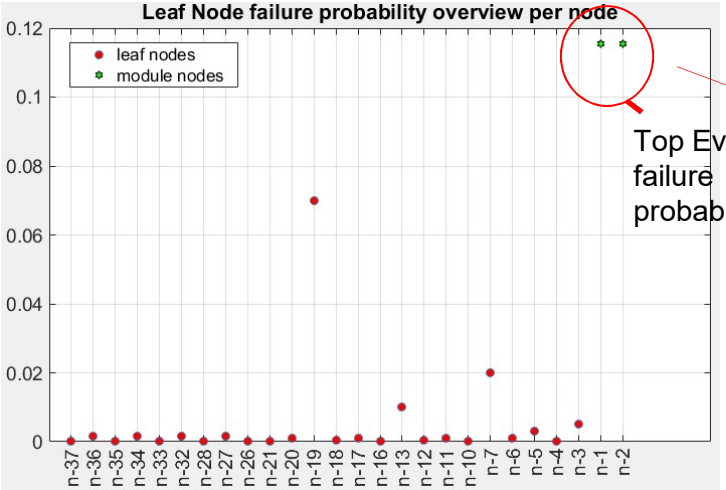
Boolean expression 1:

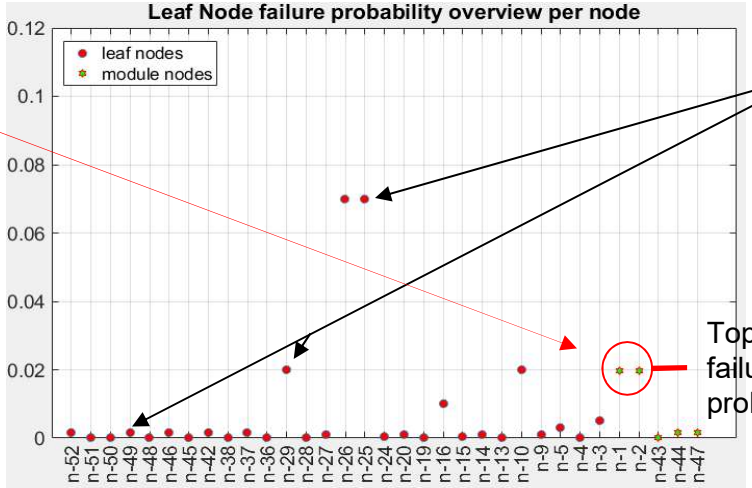
n_3 | n_4 | n_5 | n_6 | n_7 | n_10 | n_11 | n_12 | n_13 |...
n_16 | n_17 | n_18 | n_19 | n_20 | n_21 | n_26 | n_27 |...
n_28 | n_32 | n_33 | n_34 | n_35 | n_36 | n_37

Redundant system: 0.019715

Boolean expression 2:

n_3 | n_4 | n_5 | n_9 | n_19 | n_20 | n_24 | n_36 | n_37 | n_38 | n_42 | n_43 | n_50 | n_10 & n_29 | n_13 & n_29 | n_14 & n_29 | n_15 & n_29 | n_16 & n_29 | n_25 & n_26 | n_27 & n_29 | n_28 & n_29 | n_29 & n_51 | n_29 & n_52

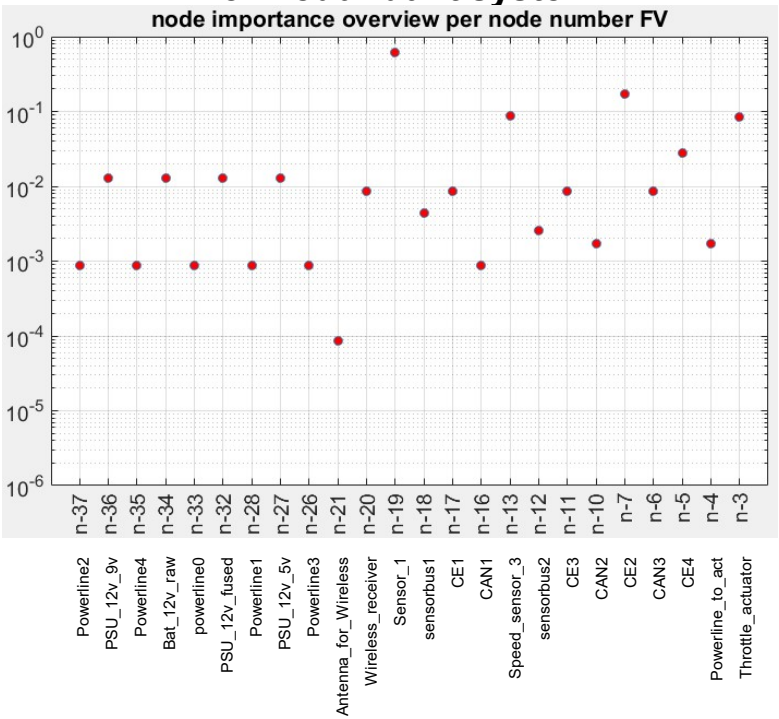




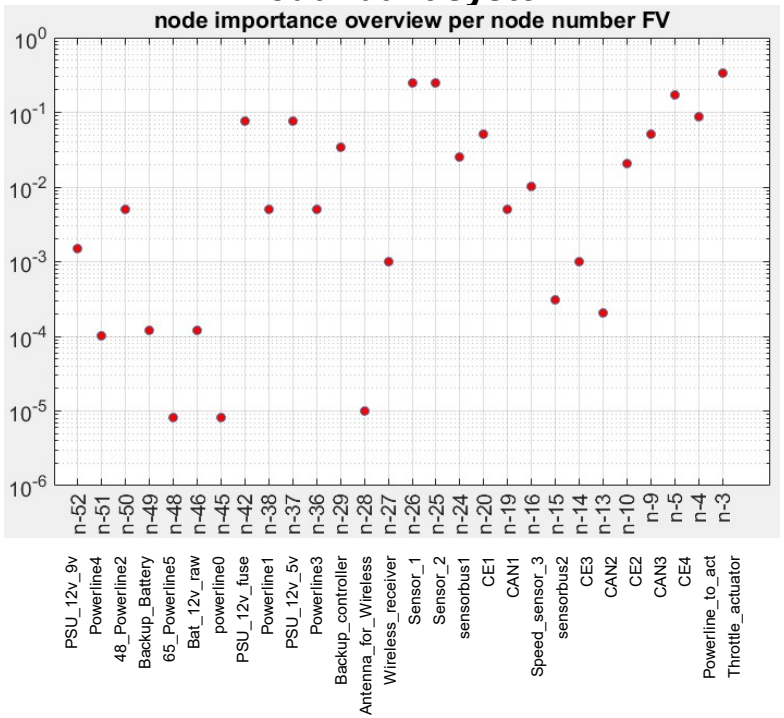
System Analysis: Importance measures

- Risk reduction worth

non-redundant system



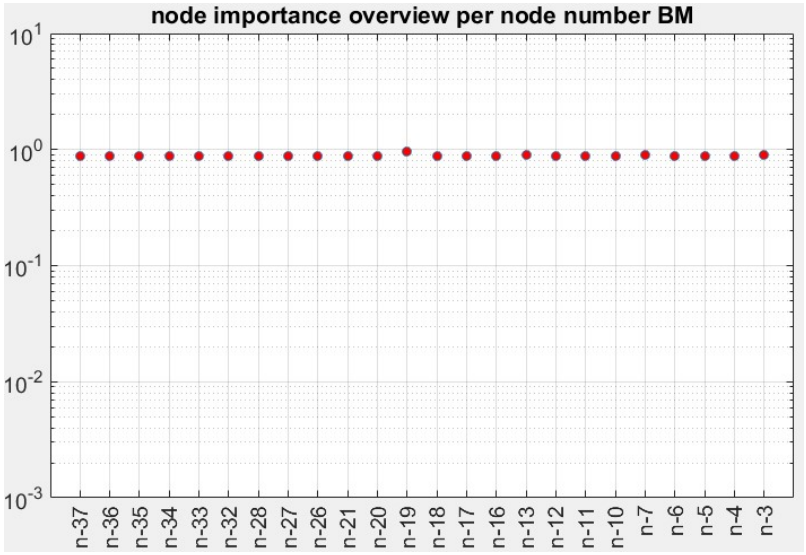
redundant system



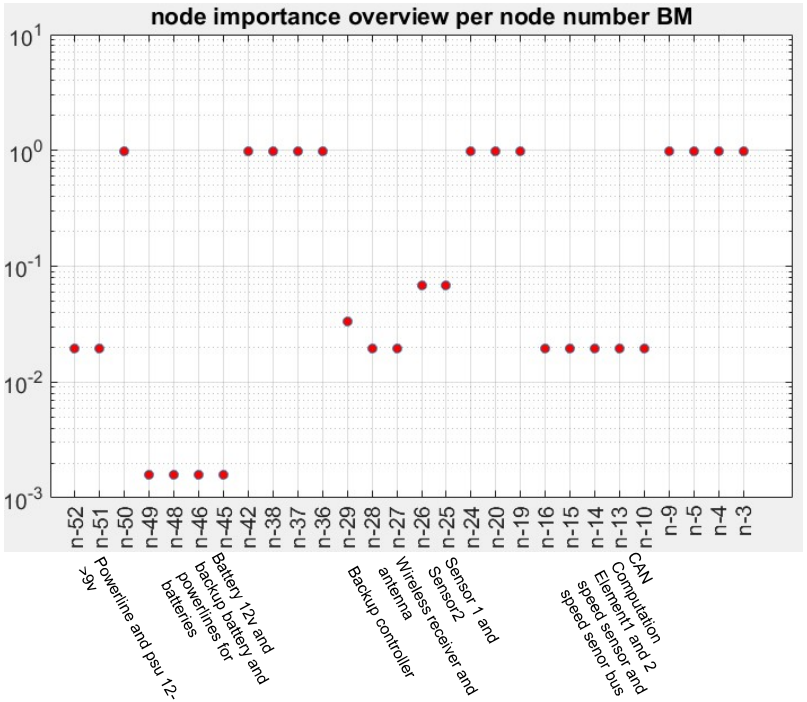
System Analysis: Importance measures

- Birnbaum importance

non-redundant system



redundant system



Thank you for your attention!