System Level Fault Injection Simulation Using Simulink

Wai Yuen Tang, Marcelo Mizuki, Mitch Norcross, Fengying Qiao

15 Trafalgar Square, Nashua, NH, USA, Transportstraat 1, 3980 Tessenderlo, Belgium

Abstract

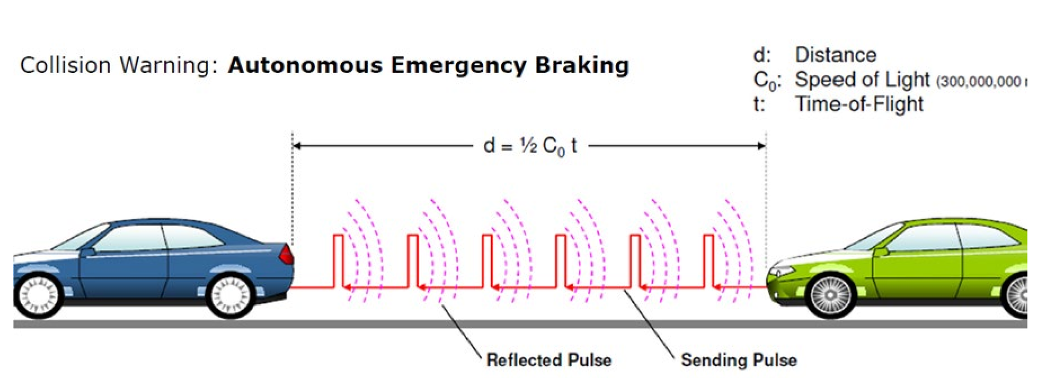
- Fault injection simulation is used to verify a LIDAR design.
- A system level behavioral model is created using Simulink to represent the system.
- FMDEA is implemented to identify the sub-blocks with the highest risk.
- Faults are modeled and generated at the targeted blocks of the system
- The mission and diagnostic behaviors are simulated with and without fault.
- This method successfully identified undetectable faults
- The model can be adjusted easily to evaluate changes to the design or the diagnostic.

Fault Injection

- There are three approaches to fault injection:
  - **Hardware Implemented**: using physical perturbation on hardware.
  - **Software Implemented**: using software to alter the timing and data of the hardware
  - **Model Implemented**: model and simulate the DUT in a computer system.
- For ASIC design, physical system is generally not available during the design phase. Hence model implemented fault injection is used.
- The DUT can be modeled at various abstraction levels, e.g. behavioral , schematic, layout. Modeling with lower abstraction level gives better accuracy, but the simulation takes longer. The appropriate abstraction level depends on the verification goal.
- Not all faults are significant. Some faults, at some locations, can only cause minor effect to the overall system. They are therefore categorized as **safe failures** (in contrast with **dangerous failures**).

LIDAR

- LIDAR is a distance measuring device based on the Time of Flight principle.
- The targeted market is automotive industry, where reliability is a critical requirement.
- Applications includes: Autonomous braking, Blind spot monitoring, and self-driving.



ISO26262: ASIL classification

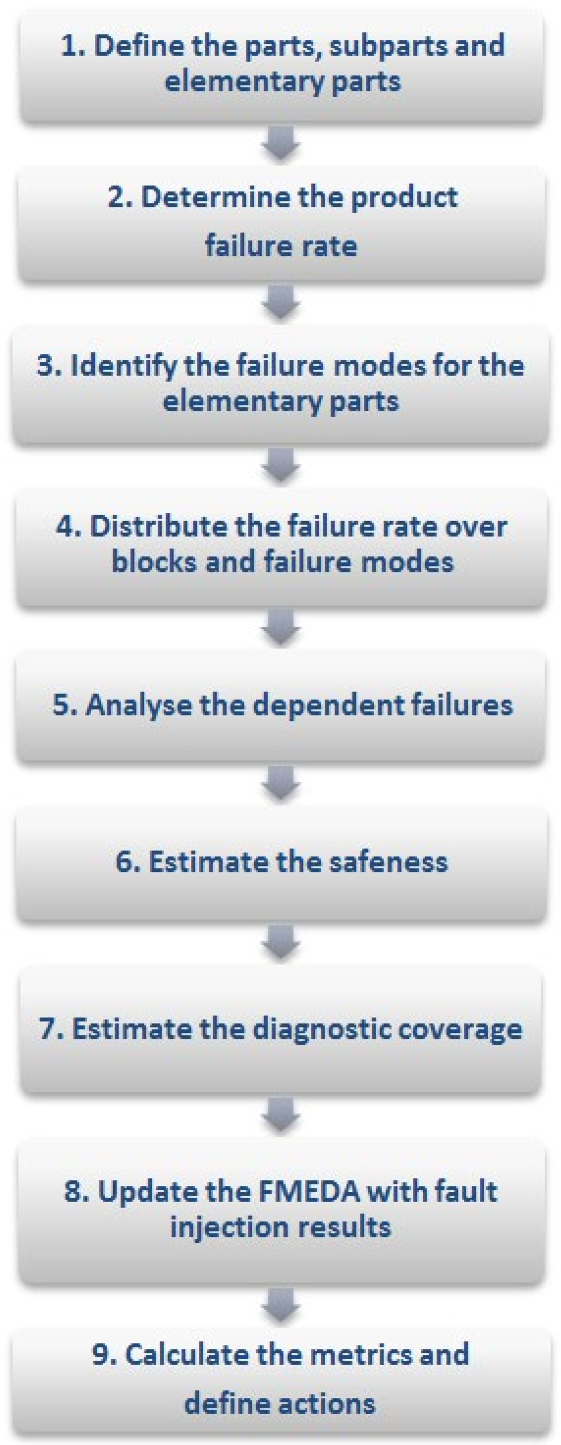
ISO26262 processes an automotive specific risk-based approach to determine the system's integrity level, known as Automotive Safety Integrity Level (ASIL). There are four integrity levels from the lowest of ASIL A to the highest of ASIL D. At each level there are various recommended actions, for example: fault injection for ASIL B or higher.

FMEDA workflow

A standard functional safety workflow is followed in designing this LIDAR chip, it is called Failure Mode, Effects, and Diagnostic Analysis (FMEDA). It is used to **identify the design blocks with high residual fault** (RF) rate.

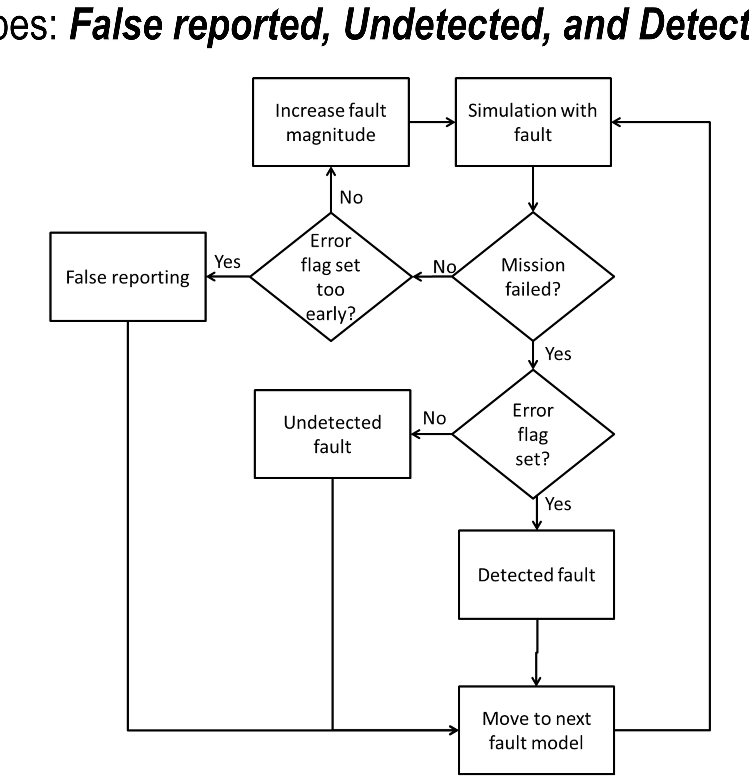
The blocks with the highest RF are modeled in Simulink, and fault injection is executed.

In this project, four analog blocks are identified with the highest RF.



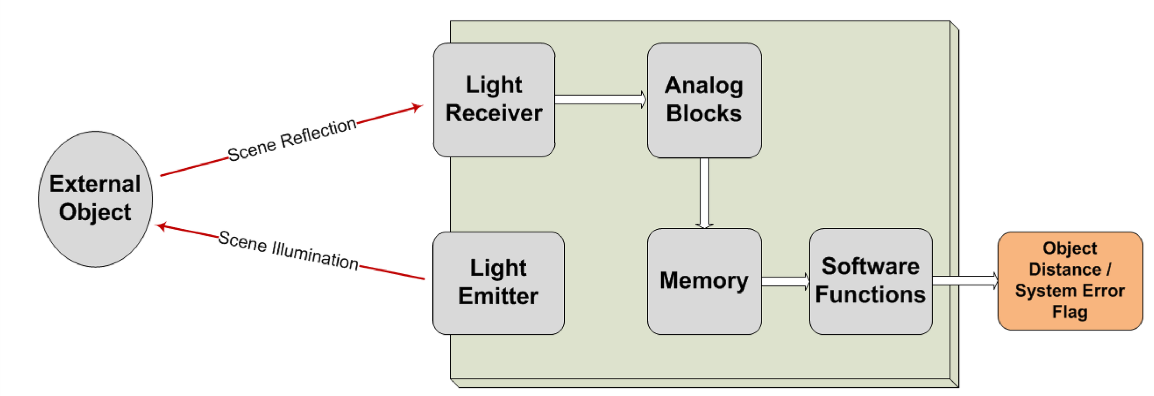
Fault Injection Flowchart

Based on the simulation results each fault can be categorized into 3 types: ***False reported, Undetected, and Detected***

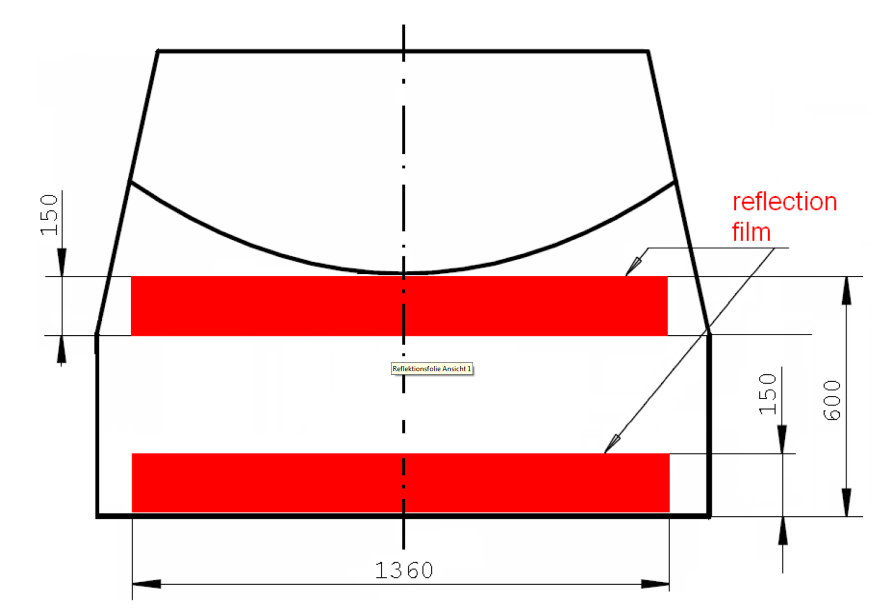


Simulink Model Creation

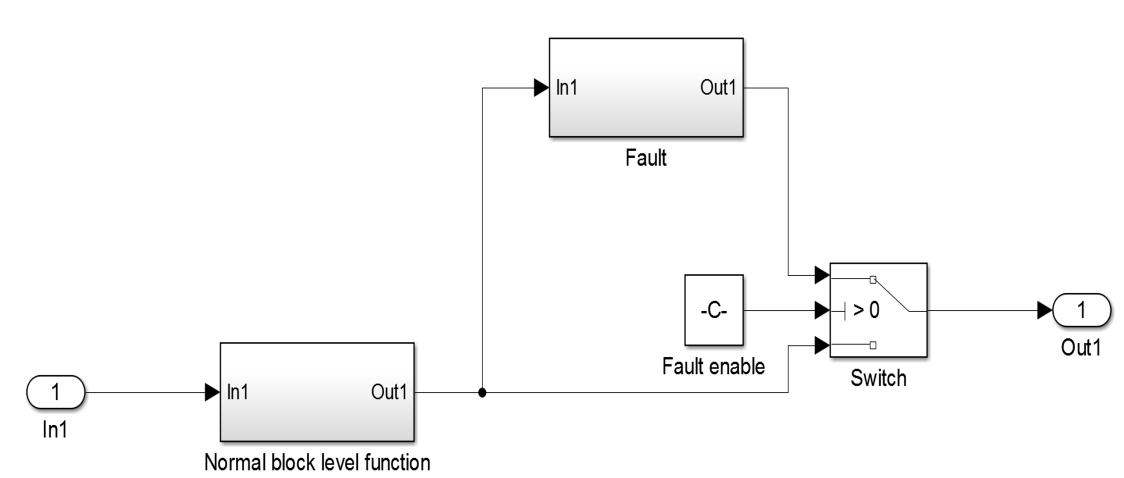
The behavioral DUT model can operate in **mission mode** or **diagnostic mode**. Distance measurement and any system error will be reported to the host. The model consists of some essential analog and software sub-blocks. They are built based on the block level design specification.



Target object is modeled based on the EURO NCAP test protocol for AEB systems. Example target shown is the rear side of a car.



Faults are injected into the targeted analog blocks. The faults can be switched on/off by the user. Also, the fault magnitude can be swept by the testbench. Sweeping the magnitude ensures all faults produce **dangerous failures.**



An extra improvement that can be done is to automate the testbench. A program can be created to execute the steps shown in the fault injection flowchart. It will further minimize human effort and increase reusability**.**

Finding the weak spots and adjusting the design

- The fault injection method is effective in identifying the weak spot of the diagnostic coverage.
- A new diagnostic mechanism can be designed based on the identified weak spot.
- System level model can be adjusted quickly to evaluate the design with the new diagnostic included.

Fault Injection Result of the Original Diagnostic

Analog Blocks / Fault Models (polarity)	Block A	Block B	Block C	Block D
Fault A(+)	ND		ND	ND
Fault A(-)	D		D	D
Fault B(+)	M		M	M
Fault B(-)	D		D	D
Fault C	ND			
Fault D		M		
Fault E(+)			ND	
Fault E(-)			ND	

Fault Injection Result of the New Diagnostic

Analog Blocks / Fault Models (polarity)	Block A	Block B	Block C	Block D
Fault A(+)	D		D	D
Fault A(-)	D		D	D
Fault B(+)	D		D	D
Fault B(-)	D		D	D
Fault C	D			
Fault D		D		
Fault E(+)			ND	
Fault E(-)			ND	

ND: not detected, D: detected, M: marginal, F: false reporting, None: not applicable

Model-Based Fault Injection Pros and Cons

Pros:
- ✓ Time-efficient to build and simulate
- ✓ Reusable
- ✓ Can be implemented in early project phase

Cons
- ○ Lower accuracy compared to circuit level simulation
- ○ Need to validate the design model
- ○ Difficult to describe complex fault models

Contact information

Melexis.com
Inspired Engineering

15 Trafalgar Square,
Ste 100,
Nashua, NH, 03063

T: 603 204 2915
T: 603 897 5149
E: wta@melexis.com