UNIVERSITY OF Hull

IMBSA 2014

Exploring the Impact of Different Cost Heuristics in the Allocation of Safety Integrity Levels

2014

Luís Azevedo
E-mail: L.P.Azevedo@2012.hull.ac.uk

Outline

- (A)SIL Allocation and Decomposition
- Automatic and Optimal Allocation of SILs
- ASIL Cost Impacts on a Hybrid Braking System (HBS)
- Conclusions

What are Safety Integrity Levels (SILs)?

- SILs specify the stringency of requirements applicable to the development and validation of safety-critical systems.

Part of Safety Standards

- IEC 61508 - SILs
- ARP4754A - Development Assurance Levels or DALs.
- ISO 26262 - Automotive SILs or ASILs;

5 ASILs

- ASIL QM - ASIL D
- Least strict - most strict

ASILs are:

- **Assigned** to hazards;
- **Inherited** by Top Level Safety Requirements (Safety Goals -SG)
- **Allocated** and **Decomposed** throughout the architecture:
  - ASIL QM = 0; ASIL A = 1; ASIL B = 2; ASIL C = 3; ASIL D = 4.

If the failure of *element* directly violates *SG*:

$$ASIL_{element} = ASIL_{\mathrm{SG}}$$

If the failure of *elements i* jointly violate *SG*:

$$\sum ASIL_{element}(i) = ASIL_{SG}$$

Challenges with ASIL Allocation

- **Complexity of modern safety-critical systems**
  - The trend is for architectures to become SoS with complex networked architectures;
  - In the process, the amount of work required from the safety engineer makes manual ASIL allocation **practically impossible**

    → the standard fails to give guidance on automated support

Challenges with ASIL Allocation

- **In ISO 26262, the goal is to find an ASIL allocation that fulfills a set of system level integrity requirements.**
  - ASILs dictate different development efforts and in the end **costs.**

Example of 2 components, **C_1** and **C_2** assuring a SG of ASIL B

- C_1 (ASIL QM) + C_2 (ASIL B)
- C_1 (ASIL A) + C_2 (ASIL A)
- C_1 (ASIL B) + C_2 (ASIL QM)

Challenges with ASIL Allocation

- **In ISO 26262, the goal is to find an ASIL allocation that fulfills a set of system level integrity requirements.**
  - ASILs dictate different development efforts and in the end **costs.**

Example of 2 components, **C_1** and **C_2** assuring a SG of ASIL B

Illustrative ASIL cost function

ASIL	QM	A	B	C	D
Cost	0	10	100	1000	10000

- C_1 (ASIL QM) + C_2 (ASIL B): 0 + 100 = 100;
- **C_1 (ASIL A) + C_2 (ASIL A): 10 + 10 = 20;**
- C_1 (ASIL B) + C_2 (ASIL QM): 100 + 0 = 100.

Challenges with ASIL Allocation

- **In ISO 26262, the goal is to find an ASIL allocation that fulfills a set of system level integrity requirements.**
  - ASILs dictate different development efforts and in the end **costs.**

ASIL Allocation is a complex combinatorial problem where the satisfaction of integrity requirements is a constraint that must be met, while the real objective is the optimisation of cost.

The impacts of different cost heuristics

- The concern about cost implications of ASILs is already evident in the automotive domain;
- We want to show that the "optimal satisfaction" of integrity requirements is defined by the nature of the ASIL cost heuristic.
- We use an automated method for ASIL allocation and apply it to the case study of a Hybrid Braking System.

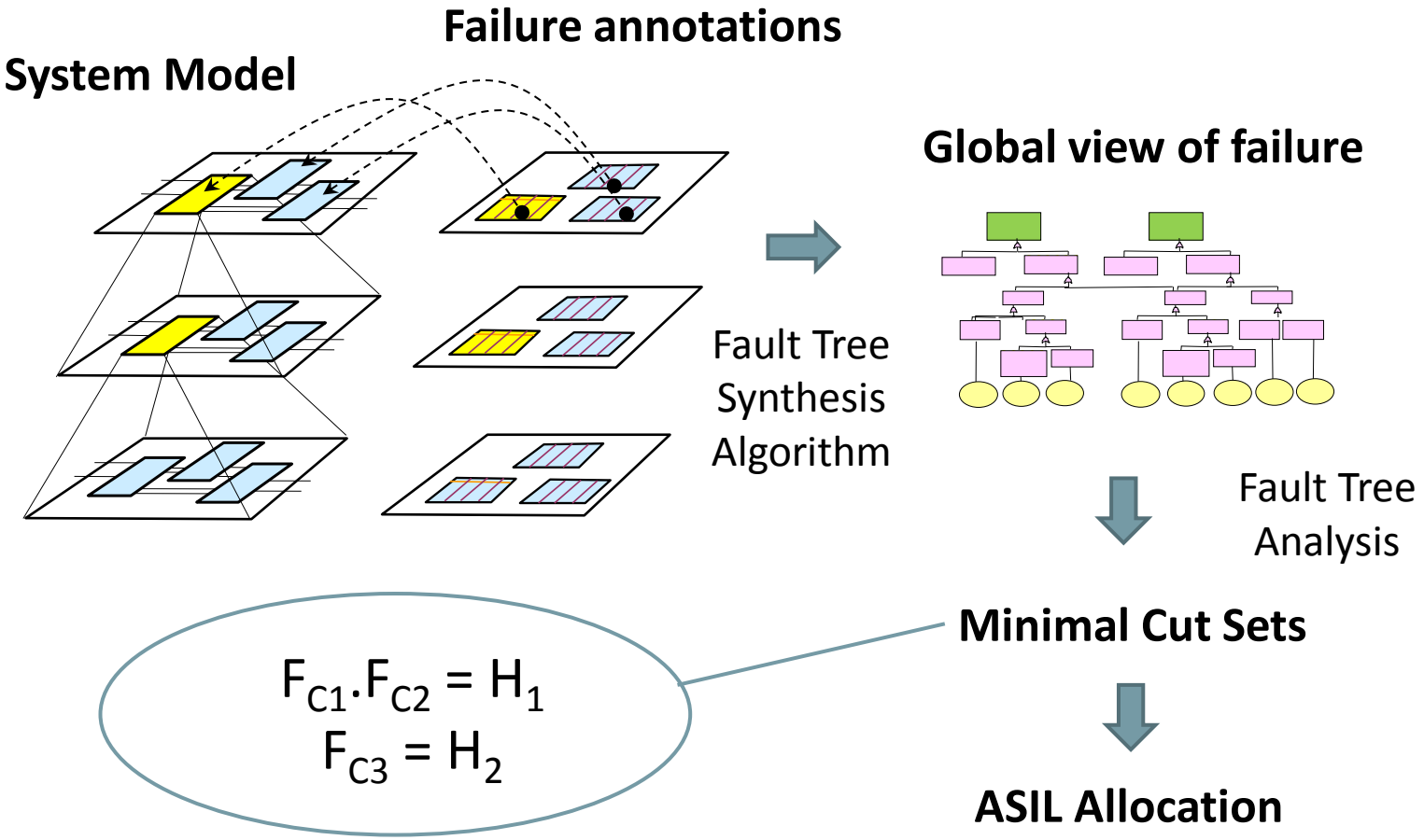
Manual ASIL Allocation is difficult and error-prone.

HiP-HOPS* – A Solution

- Model-based Safety and Reliability Analysis Tool
- Automation of ASIL Allocation based on Fault Tree Analysis

**Hierarchically Performed Hazard and Origin Propagation Studies*

HiP-HOPS - Automated Framework for ASIL Allocation



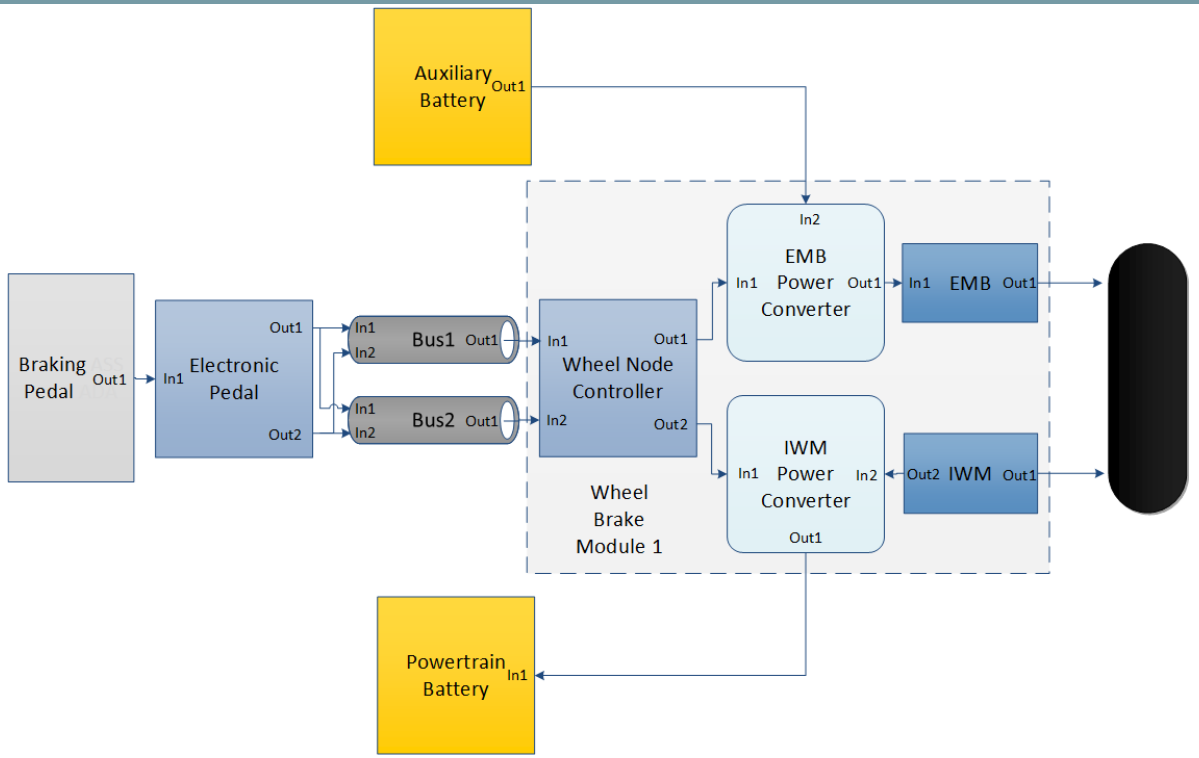
HiP-HOPS – Towards a more refined allocation of ASILs

- HiP-HOPS assigns ASILs to component failures;
- This allows for a more refined allocation of requirements;
- It works as a recursive method where the "subsystem" can be treated as a "system" that has multiple SGs and ASILs.
- This approach, we believe, could be one worth considering in the future evolution of ISO 26262.

HiP-HOPS – Finding cost efficient ASIL Allocations

- ASIL Allocation produces a vast solution space;
- HiP-HOPS includes sophisticated optimisation techniques capable of finding cost efficient ASIL allocations in real world architectures.
- Initial work included implementations of Genetic Algorithms;
- Significant improvements were found in both solution quality and processing efficiency using a Tabu Search technique.

The HBS

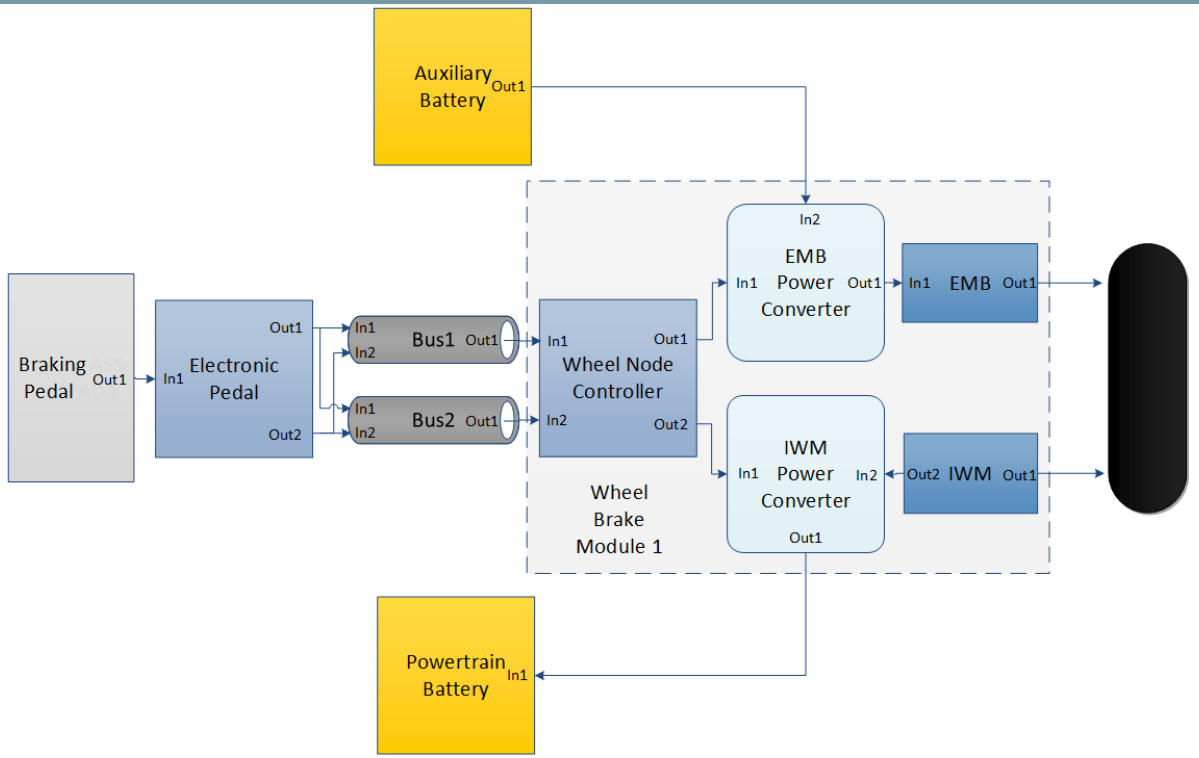


Hazards:

- No braking after command (H1) – ASIL D
- Wrong value braking (H2) – ASIL A

- H1 = Omission of EMB.out1 AND Omission of IWM.out1
- H2 = Value deviation of EMB.out1 OR Value deviation of IWM.out1

The HBS



- 24 Failure Modes identified;
- Total search space size of 5^{24} (≈5.96×10^{16})

Experimentation with Different ASIL Cost Functions

- Two ASIL Cost Heuristics have been considered;
- They serve the purpose of demonstrating the cost influence in choosing a set of ASILs for a given system design.

Cost Function/ ASIL	ASIL QM	ASIL A	ASIL B	ASIL C	ASIL D
Experiential I	0	10	20	40	50
Experiential II	0	20	30	45	55

Two ASIL Cost Heuristics

	Optimal Solutions				
	Exp-I Cost: 390	Exp-II Cost: 585			
Components' Failure Modes	**#1**	**#1**	**#2**	**#3**	**#4**
Braking Pedal Omission	4	4	4	4	4
Braking Pedal Value	1	1	1	1	1
Electronic Pedal Omission 1	2	4	4	4	4
Electronic Pedal Omission 2	2	0	0	0	0
Electronic Pedal Value 1	1	1	1	1	1
Electronic Pedal Value 2	0	0	0	0	0
Bus1 Omission	2	0	4	0	4
Bus2 Omission	2	4	0	4	0
WNC Omission 1	2	0	0	4	4
WNC Omission 2	2	4	4	0	0
WNC Value 1	1	1	1	1	1
WNC Value 2	1	1	1	1	1
Auxiliary Battery Omission	2	0	0	4	4
Auxiliary Battery Value	1	1	1	1	1
Powertrain Battery Omission	2	4	4	0	0
Powertrain Battery Value	1	1	1	1	1
EMB Power Converter Omission	2	0	0	4	4
EMB Power Converter Value	1	1	1	1	1
IWM Power Converter Omission	2	4	4	0	0
IWM Power Converter Value	1	1	1	1	1
EMB Omission	2	0	0	4	4
EMB Value	1	1	1	1	1
IWM Omission	2	4	4	0	0
IWM Value	1	1	1	1	1

	Optimal Solutions				
	Exp-I Cost: 390	Exp-II Cost: 585			
Components' Failure Modes	**#1**	**#1**	**#2**	**#3**	**#4**
Electronic Pedal Omission 1	2	4	4	4	4
Electronic Pedal Omission 2	2	0	0	0	0
Electronic Pedal Value 2	0	0	0	0	0
Bus1 Omission	2	0	4	0	4
Bus2 Omission	2	4	0	4	0
WNC Omission 1	2	0	0	4	4
WNC Omission 2	2	4	4	0	0
Auxiliary Battery Omission	2	0	0	4	4
Powertrain Battery Omission	2	4	4	0	0
EMB Power Converter Omission	2	0	0	4	4
IWM Power Converter Omission	2	4	4	0	0
IWM Power Converter Value	1	1	1	1	1
EMB Omission	2	0	0	4	4
IWM Omission	2	4	4	0	0

Costs Refinement for More Accurate Optimal ASIL Allocations

- Same cost for a Processing Unit and a HV Battery both developed with ASIL D. Is it realistic?
- Our method has been refined to allow a greater granularity in costs estimation; categories of components can be created.

	Programmable Electronics	Electronic Low Voltage	Electronic High Voltage
	Electronic Pedal	Auxiliary Battery	IWM
	WNC	EMB Power Converter	IWM Power Converter
	Communication Buses	EMB	Powertrain Battery
	-	Braking Pedal	-
Cost Rating	1	3	5

	Optimal Solutions		
	Exp-I Cost: 1030	Exp-II Cost: 1425	
Components' Failure Modes	#1	#1	#2
Braking Pedal Omission	4	4	4
Braking Pedal Value	1	1	1
Electronic Pedal Omission 1	2	4	4
Electronic Pedal Omission 2	2	0	0
Electronic Pedal Value 1	1	1	1
Electronic Pedal Value 2	0	0	0
Bus1 Omission	2	0	4
Bus2 Omission	2	4	0
WNC Omission 1	4	4	4
WNC Omission 2	0	0	0
WNC Value 1	1	1	1
WNC Value 2	1	1	1
Auxiliary Battery Omission	4	4	4
Auxiliary Battery Value	1	1	1
Powertrain Battery Omission	0	0	0
Powertrain Battery Value	1	1	1
EMB Power Converter Omission	4	4	4
EMB Power Converter Value	1	1	1
IWM Power Converter Omission	0	0	0
IWM Power Converter Value	1	1	1
EMB Omission	4	4	4
EMB Value	1	1	1
IWM Omission	0	0	0
IWM Value	1	1	1

	Optimal Solutions		
	Exp-I Cost: 1030	Exp-II Cost: 1425	
Components' Failure Modes	#1	#1	#2
Electronic Pedal Omission 1	2	4	4
Electronic Pedal Omission 2	2	0	0
Bus1 Omission	2	0	4
Bus2 Omission	2	4	0

- ASIL allocation is a complex cost optimisation problem;
- With the Hybrid Braking System it has been demonstrated that:
  - cost consideration allows to identify the most promising solutions;
  - different cost heuristics potentially result in different optimality.

→ work needs to be undertaken within each industry sector to identify plausible cost heuristics so that SIL allocation choices can be made with more confidence.

- Consideration of optimal ASIL allocations is only possible through the use of an automated framework;
- While a definitive cost heuristic is not presently available, our method is flexible; a system designer can use any they find suitable.
- Finally, our approach allows for designers to input costs at different levels of granularity, contributing to a more accurate determination of the best ASIL allocation strategies.

Thank you!