Industrial Embedded Systems
- Design for Harsh Environment -

Dr. Alexander Walsch
alexander.walsch@ge.com

IN2244

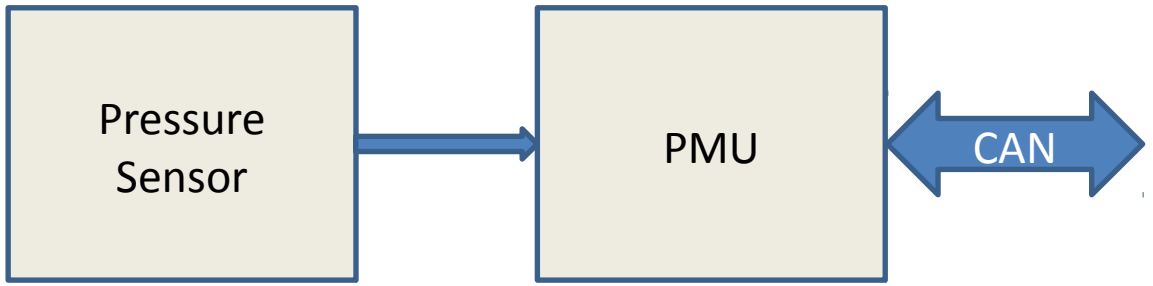
Part IX

WS 2014/15

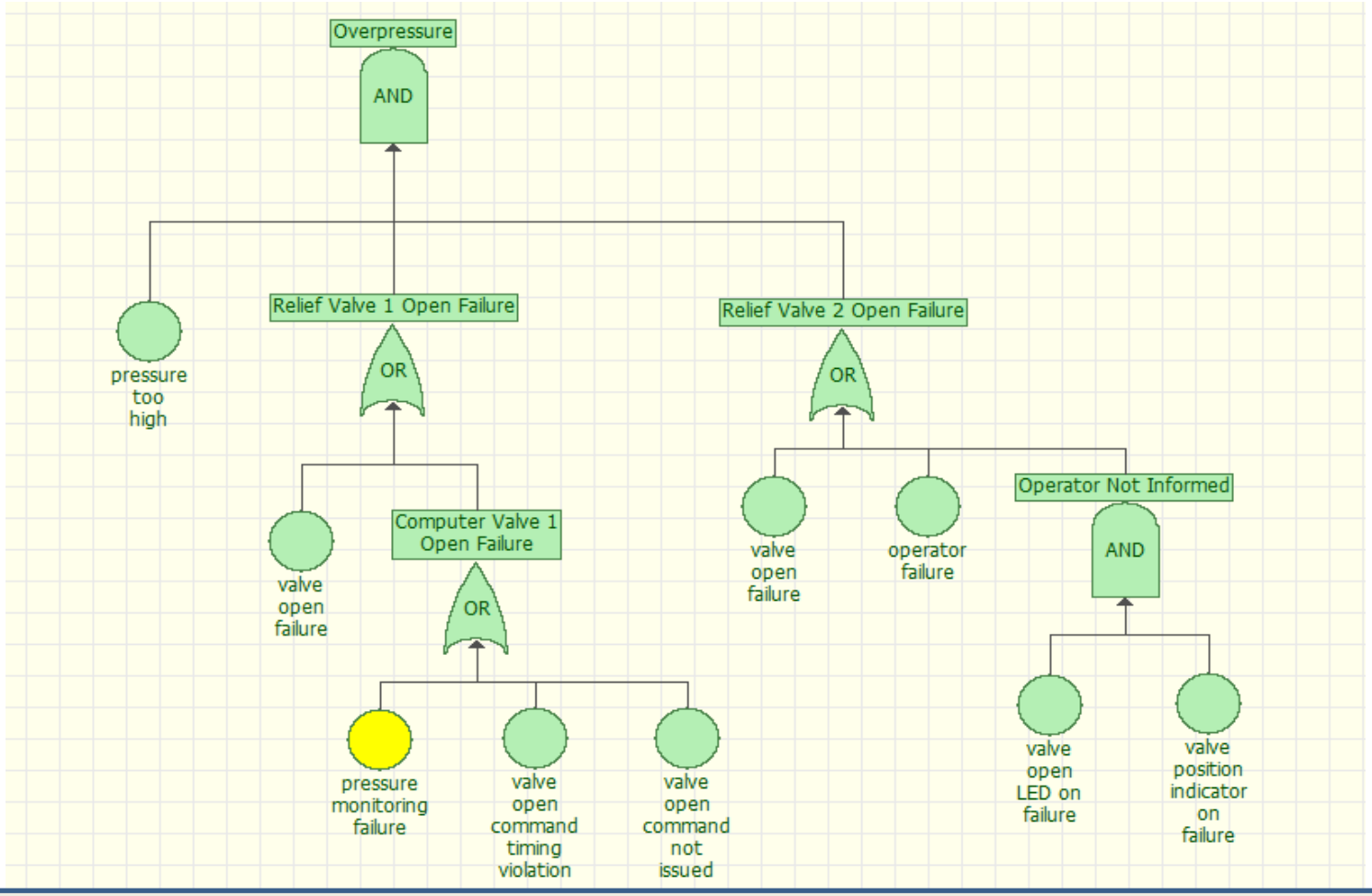
Technische Universität München

Case Study

An electronics component that measures pressure in an industrial environment is to be developed. It connects to our series of 4-20 mA pressure sensors, does a temperature compensation, and communicates the value via a CAN interface. We are part of the development team that designs this component (ME, EE, CS). The component is referred to as PMU (Pressure Measurement Unit).



Preliminary Hazard Analysis (FTA)



What makes the „pressure monitoring“ functionality fail (activate the hazard)?

PHA (FMEA)

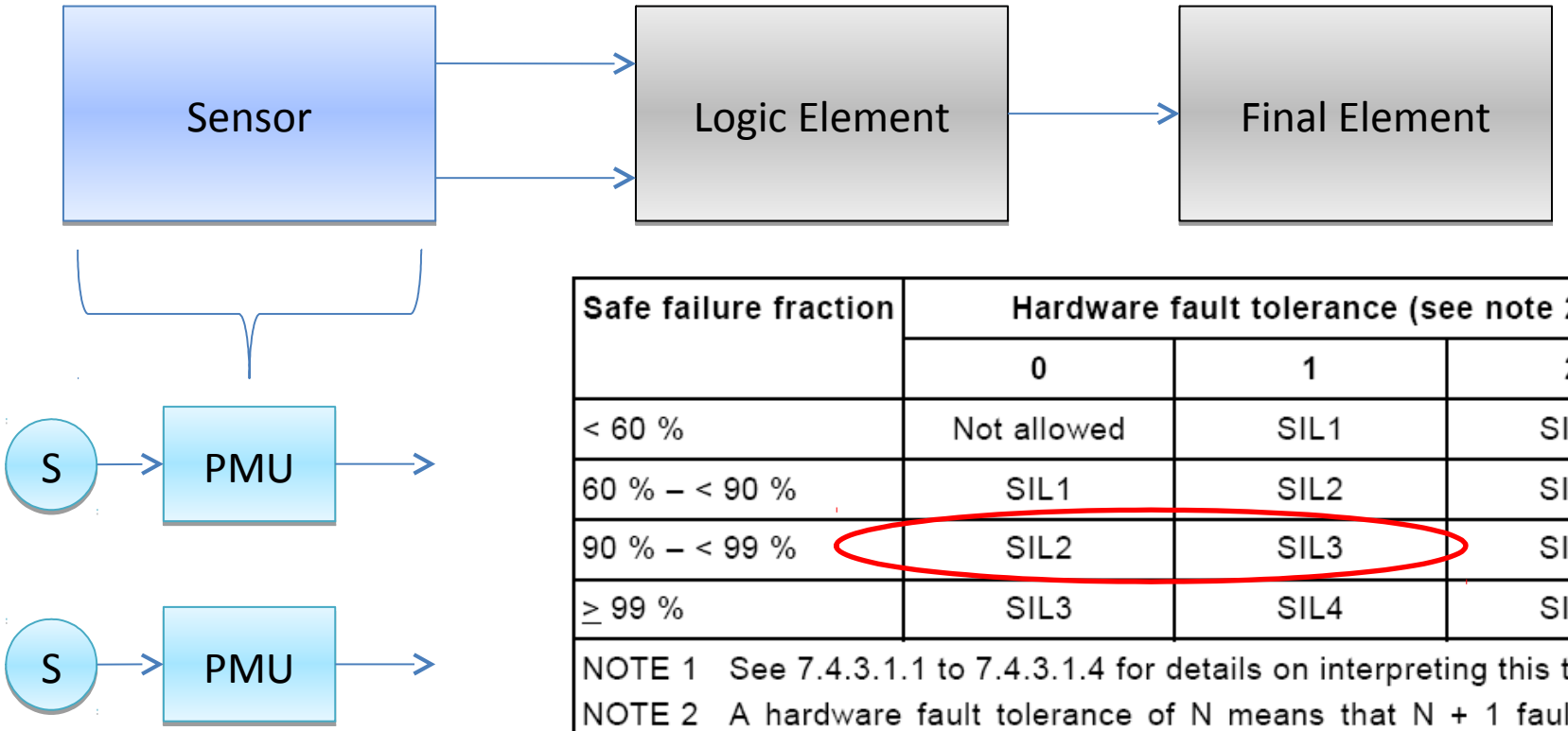
function (activates hazard)	potential failure (e.g. its state)	effect of failure (e.g. its consequence)	cause	preventive measures
Pressure monitoring	PMU HW			
	PMU SW			
	Timing			
	Input failure			
	Output failure			
	Configuration (limits)			

What makes the „pressure monitoring“ functionality fail (activate the hazard)?

PMU Customer Requirements

- Material cost < $50 per PMU – includes software royalties
- Standard/Certification: IEC61508 SIL3 in 1oo2 architecture
- PIC uC preferred
- Application area: process industry (O&G, power plants, …)

Safety Function Integrity



Source:
IEC61508

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

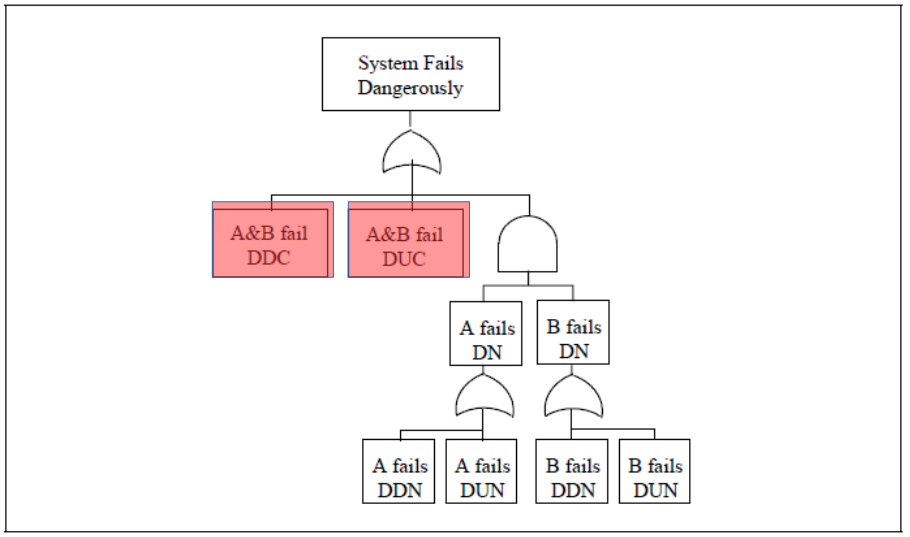
NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.

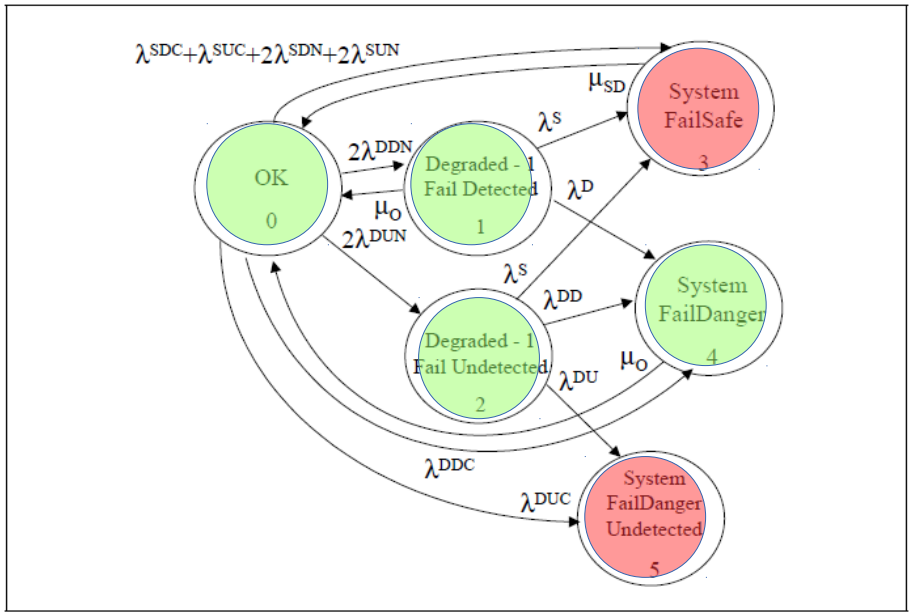
NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function.

NOTE 3 See annex C for details of how to calculate safe failure fraction.

Safety Function Integrity Modelling

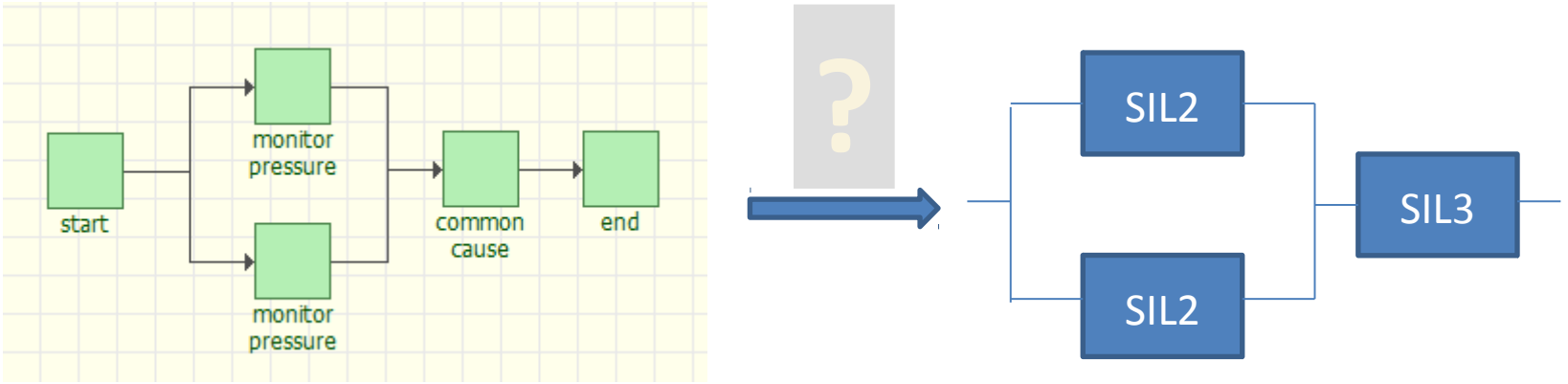
- Both channels need to fail dangerously in order to enter a hazardous application system state.
- However, for continous mode safety functions a difference in output will trigger a decision (e.g shutdown) at a higher control system layer.



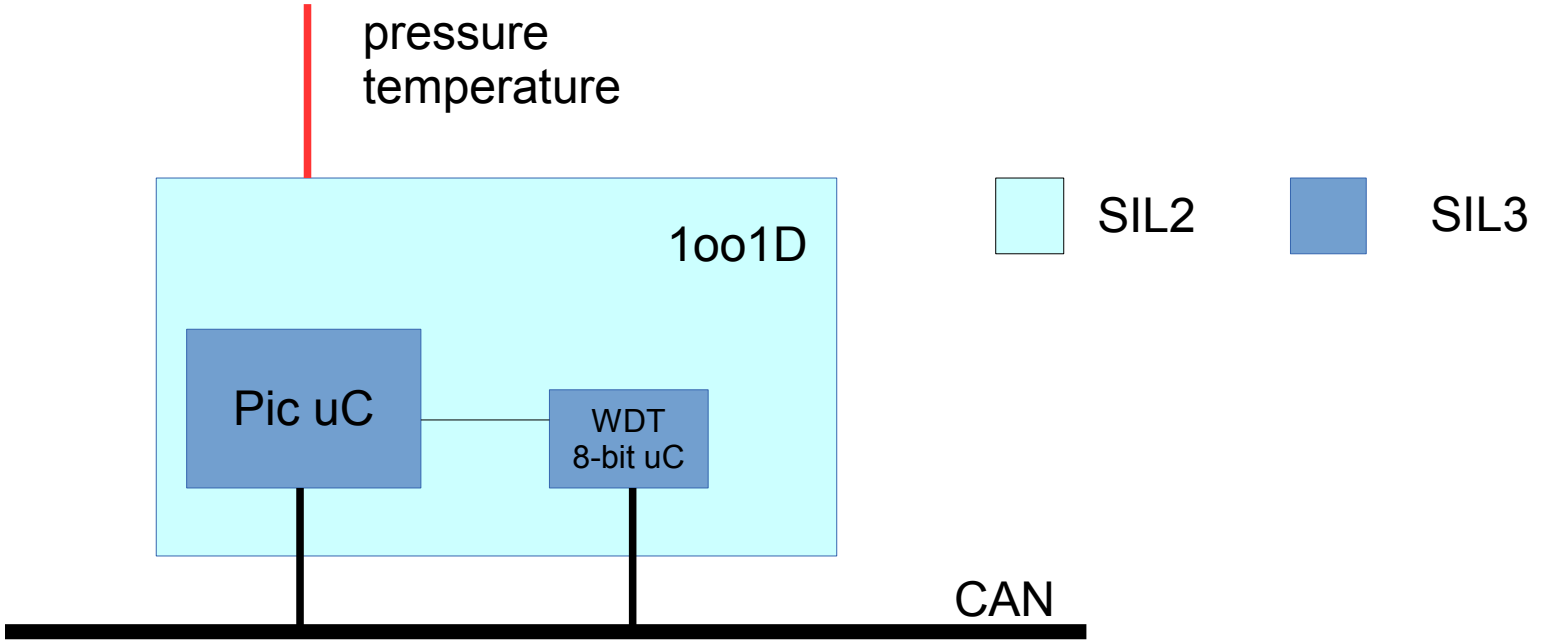


Software Requirements

- How can we include software failures into our model? We can not really but we can state the following:
- The systematic capability needs to match the SIL claimed for a safety function.



Architecture Single Channel



How do we address SIL2 (HW), SIL3(SW) for a single channel?

QFD

Relationships												
Strong	*9*											
Direct	*3*											
Indirect	*1*											
No relationship	*0*											
		Functions or processes affecting customer wishes										
	How important	monitor pressure SW	PIC ac (simple)	1oo1D architecture	configuration SW	simple scheduler	Operating System					
customer requirement												
material cost < 50$	3											
certification	5											
	Total	☆ 0	☆ 0	☆ 0	☆ 0	☆ 0	☆ 0	☆ 0	☆ 0	☆ 0	☆ 0	☆ 0
Requirement Targets												

Relate (ambiguous) customer requirements to (precise) technical requirements.

Technical Requirements

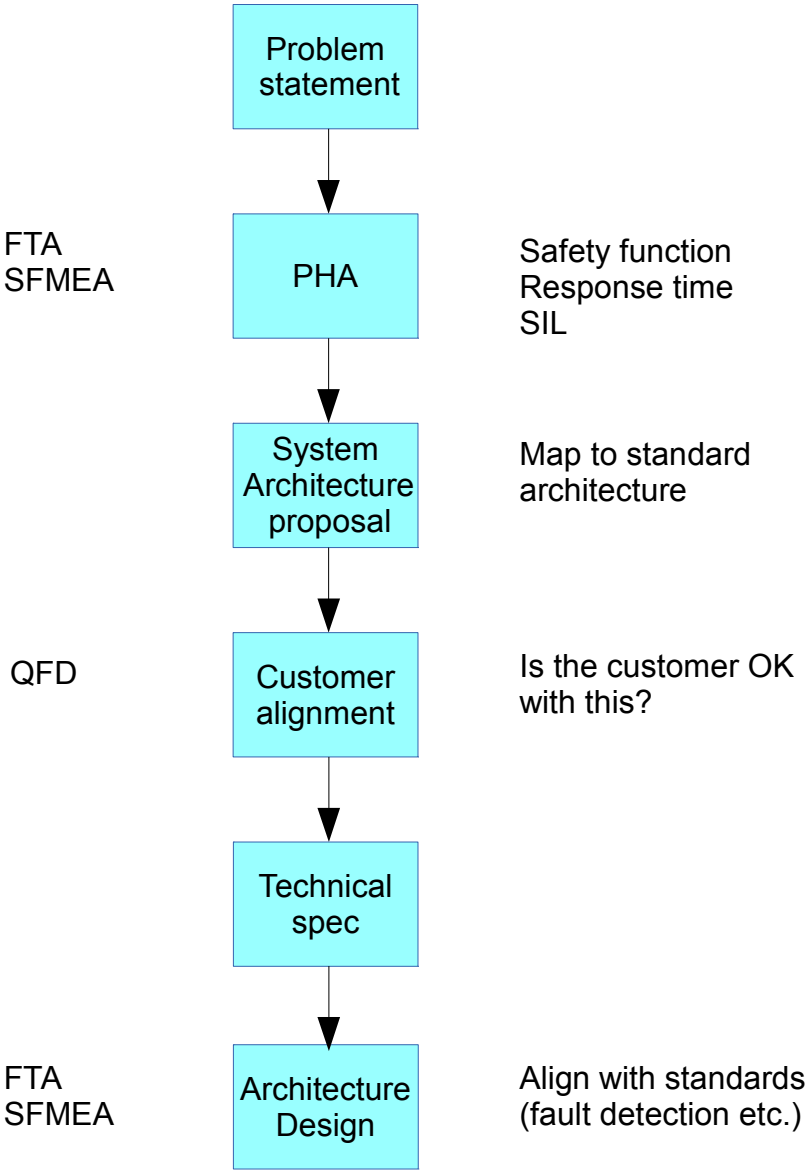
- A 1oo1D architecture for a single channel would meet the SIL2 requirement.
  - PIC uC + additional diagnostic circuit (e.g. 8-bit uC with CAN)
- SIL3 for software is required (common cause failure).
- SFF = 90% - < 99% (determines what diagnostics we need HW/SW)
- Process safety time: the deadline on reporting internal or external faults to prevent hazardous states (HW faults) and normal operation → e.g. 3 seconds

Software: Design FMEA

function	potential failure (e.g. its state)	effect of failure (e.g. its consequence)	cause	preventive measures	IEC 61508 techniques
CPU	register failure				
	execution failure				
	address calculation failure				
	program counter failure				
	stack pointer failure				

How can the HW fail (DC calculation)? How can the SW fail?

Summary


Problem statement
FTA
SFMEA
PHA
Safety function
Response time
SIL
System Architecture proposal
Map to standard architecture
QFD
Customer alignment
Is the customer OK with this?
Technical spec
FTA
SFMEA
Architecture Design
Align with standards (fault detection etc.)