Industrial Embedded Systems
- Design for Harsh Environment -

Dr. Alexander Walsch
alexander.walsch@ge.com

IN2244

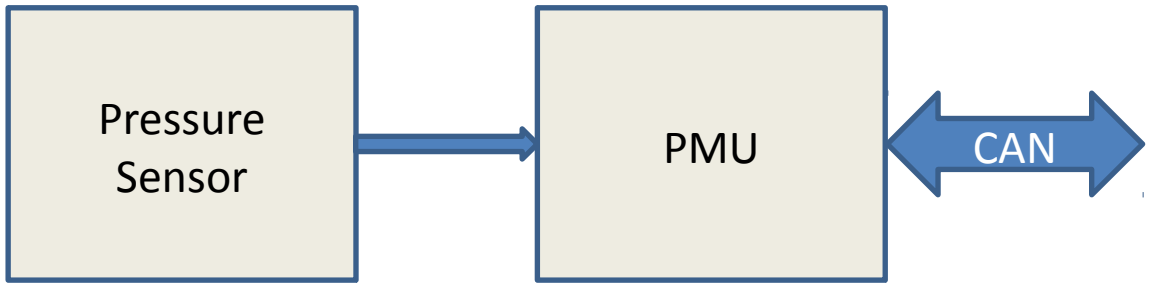
Part IV

WS 2013/14

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).



PMU Customer Requirements

- Material cost < $50
- Improve reliability
- Physical size 50 x 25 x 10 mm
- Standard/Certification: IEC61508 SIL3 in 1oo2 architecture
- Operating temperature -40 °C to +85 °C
- PIC uC preferred
- Application area: process industry (O&G, power plants, …)

PMU Requirements Analysis

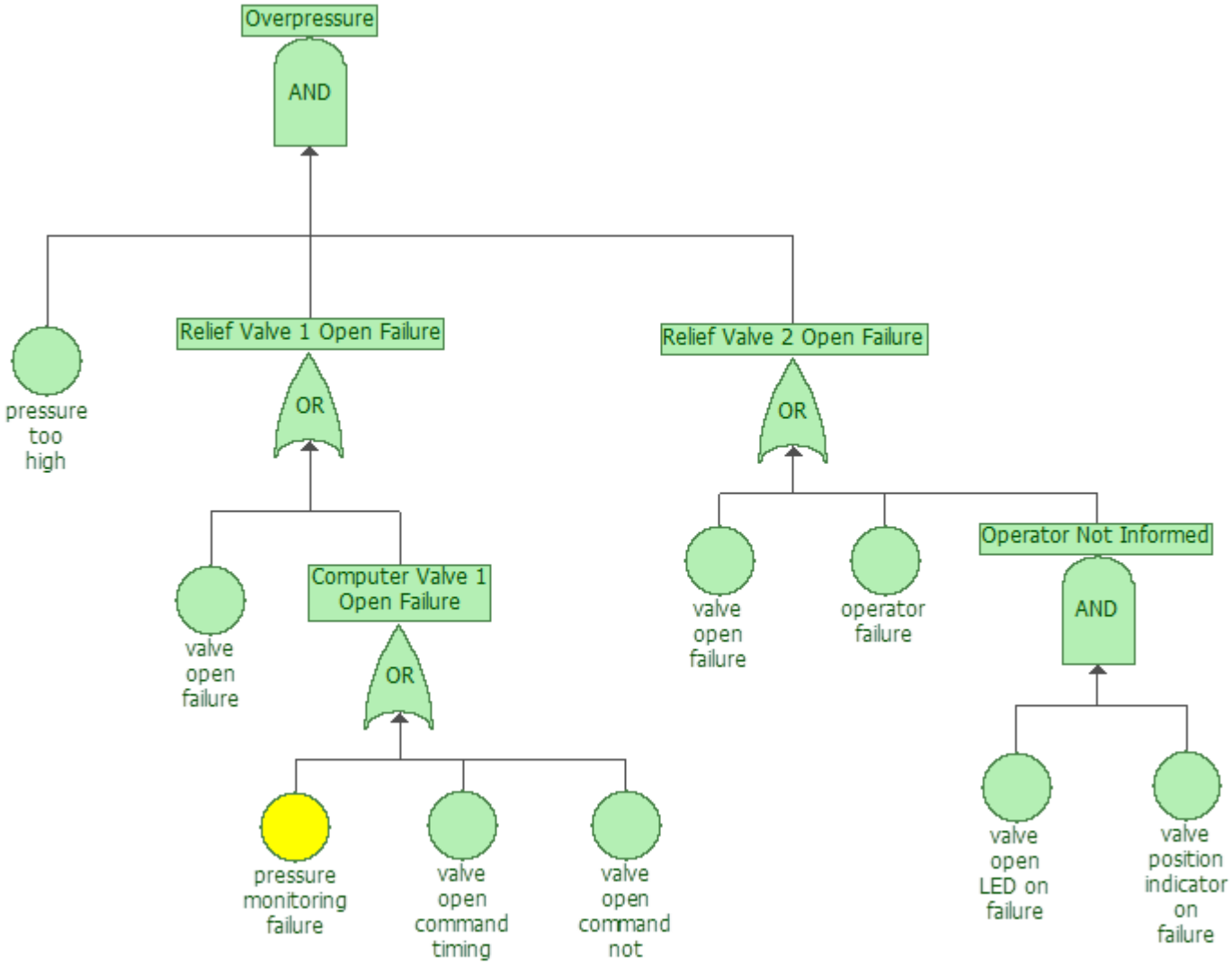
- Certainly the requirements are not sufficient. According to the last lectures we develop the following approach
  - See if we need a feasibility study
  - Look at reliability. Can we improve our present solution (if any)? Does the result influence our system architecture?
  - Is there a safety aspect? Does the result influence our system architecture?
  - We need to answer ourselves the questions on functional (what?) and non-functional (how well?) requirements.
  - We write down our findings in technical terms (requirements specification) following the outline given in the last lecture.
- In addition we use all internal guidelines and templates (which will be different from business to business)

QFD

Safety

- Safety is an application system approach. The safety function and its safety integrity is critical on the application system level (a process industry application in this case).
- Requirements on safety integrity are based on a risk analysis (last lecture).
- Safety integrity requirements can also be based on market analysis.
- For the PMU our marketing organization communicated:
  - SIL3 in a 1oo2 configuration (duplex) – the competitor probably has some similar quality metric in the data sheet

Application System Safety FTA



Preliminary Hazard Analysis
- System & Software Considerations -

- Identify hazardous software function
- Ask critical questions and come up with software requirements
- Include possible software defects

Subsystem:				Preliminary Hazard Analysis						Last Update:			
						Risk				Risk			
Number	System Item	Hazard	Causes	Effects	Project Phase(s)	FMRI	Value	Cat.	Recommended Action	FMRI	Value	Cat.	Comments

PMU Safety Function

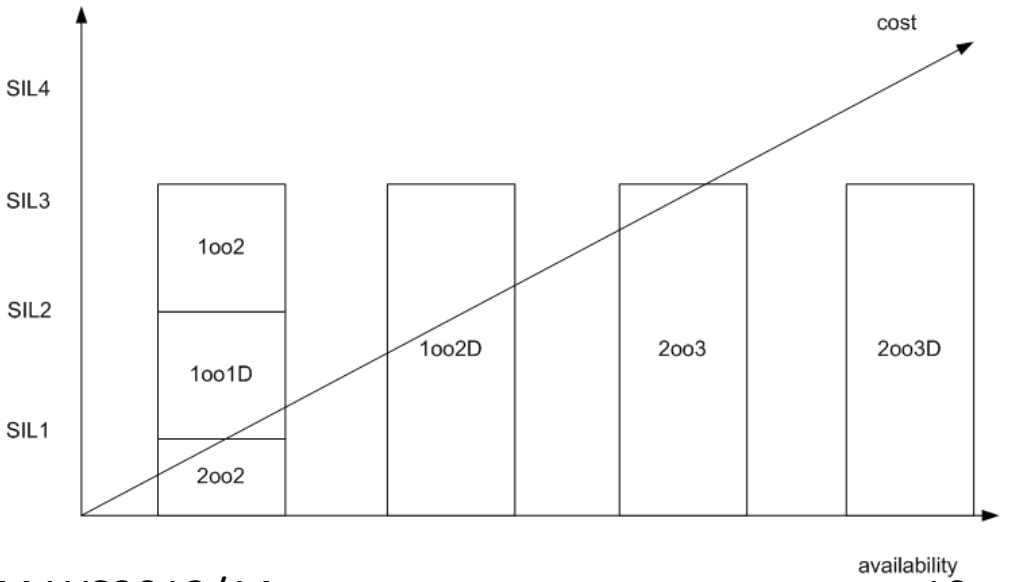
- Wrong pressure readings can lead to hazardous states and possibly to harm at the application system level.
- Imagine:
  - Over pressure in vessels (chemical industry), oil and gas pipelines, or wells in oil and gas exploration
- Pressure readings must be correct (normal function) and faults at the PMU level (external or internal) need to be detected and communicated.
- Therefore, the safety function can simply be phrased like: "*The PMU shall communicate a temperature compensated pressure reading*".
  The message indicating a violation signals the "safe state". This can be used in a fail-safe or a fail-operational approach.

Safety Function Integrity

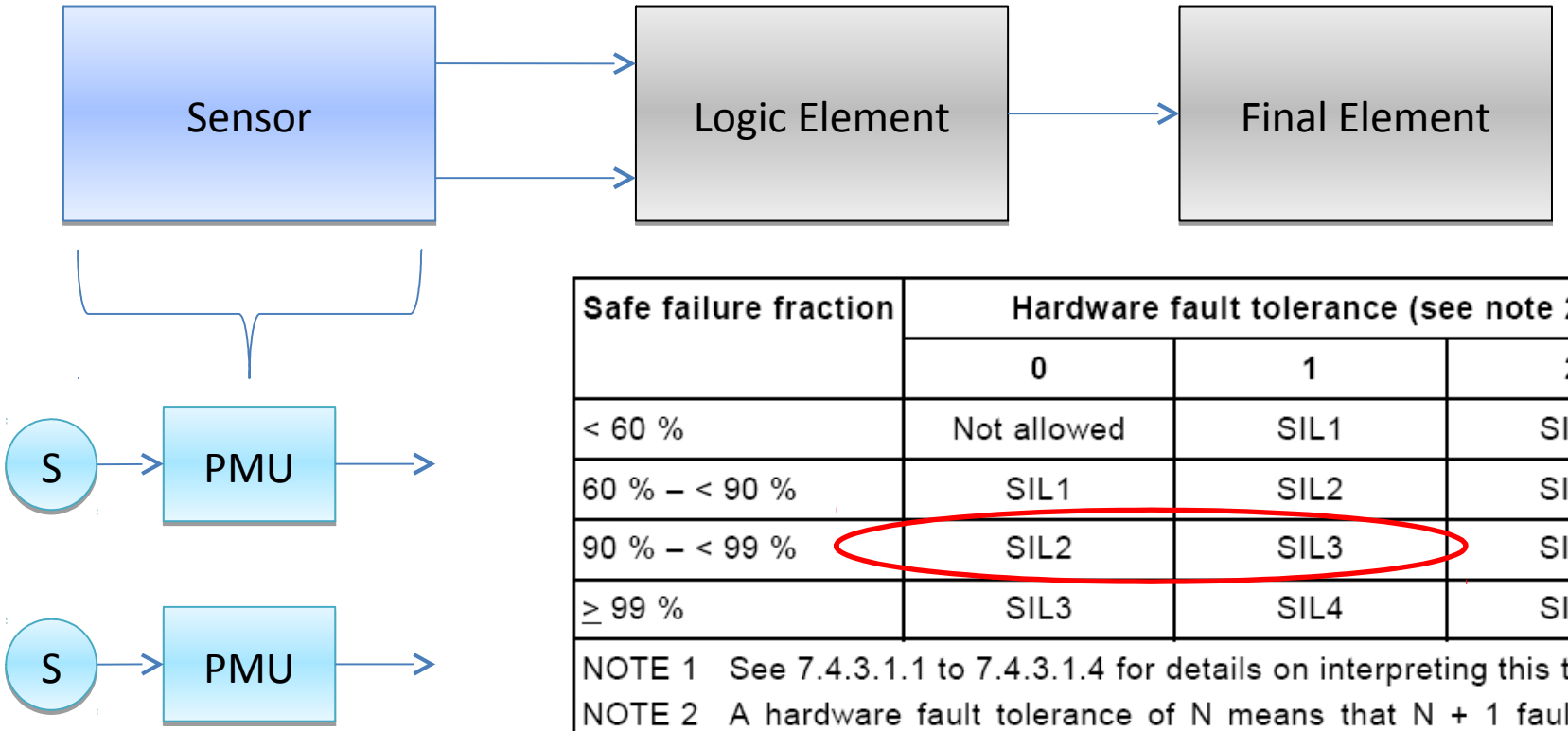
- From marketing we know that the SIL of the PMU shall be 3 in a 1oo2 configuration.
- We need to understand now what effort that means in terms of developing the hardware and software for this system.
- Looking back a lecture we came across this:
  - high and low demand of safety function and the failure table
  - Architecture and SIL ratings

SIL	High demand	Low demand
4	$10^{-9} \leq$ PFH $\leq 10^{-8}$	$10^{-5} \leq$ PFD $\leq 10^{-4}$
3	$10^{-8} \leq$ PFH $\leq 10^{-7}$	$10^{-4} \leq$ PFD $\leq 10^{-3}$
2	$10^{-7} \leq$ PFH $\leq 10^{-6}$	$10^{-3} \leq$ PFD $\leq 10^{-2}$
1	$10^{-6} \leq$ PFH $\leq 10^{-5}$	$10^{-2} \leq$ PFD $\leq 10^{-1}$

Source:
IEC61508



Safety Function Integrity II



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.

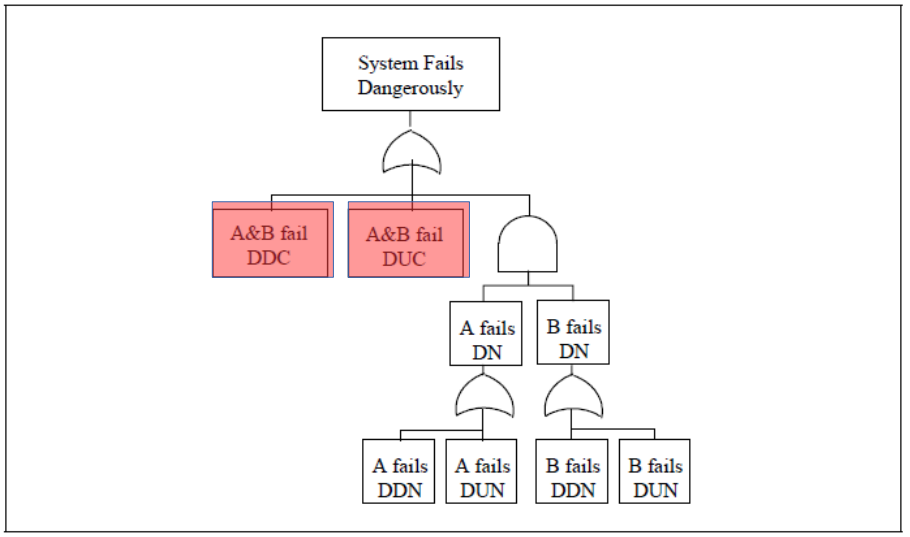
NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function.

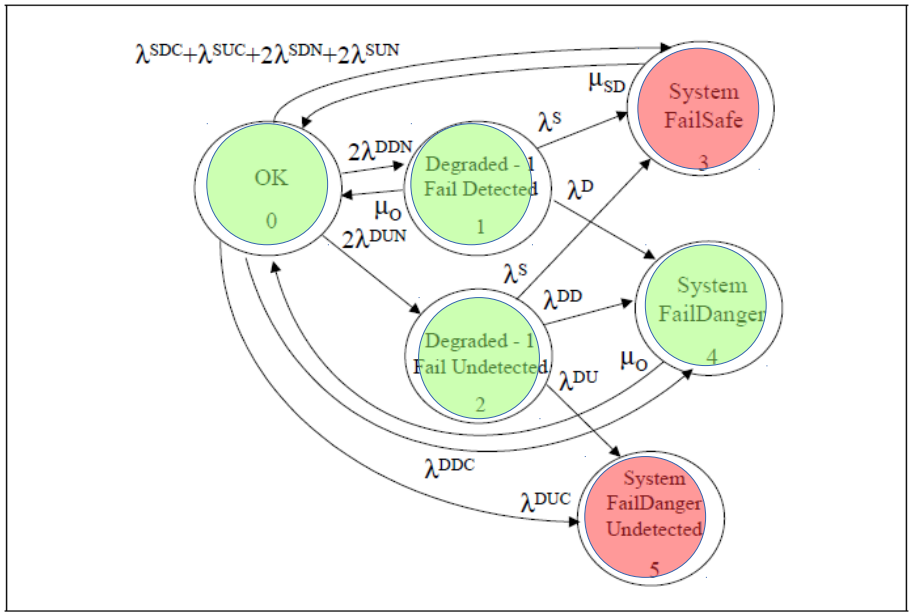
NOTE 3 See annex C for details of how to calculate safe failure fraction.

Source: IEC61508

Safety Function Integrity Modelling

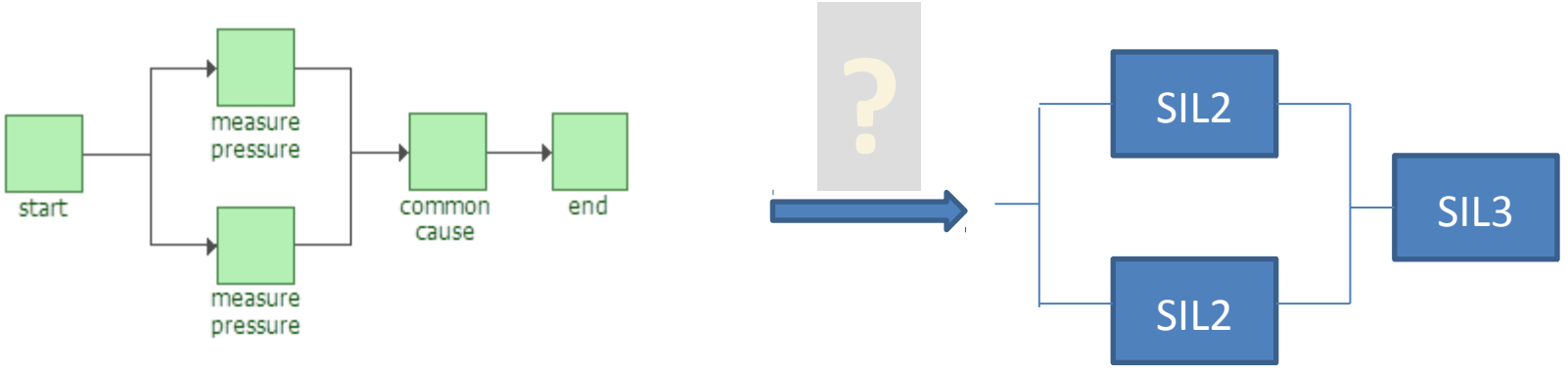
- Both channels need to fail dangerously in order to enter a hazardous application system state.
- However, for continous mode safety functions a difference in output will trigger a decision (e.g shutdown) at a higher control system layer.





Requirements for a Single Channel

- 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.

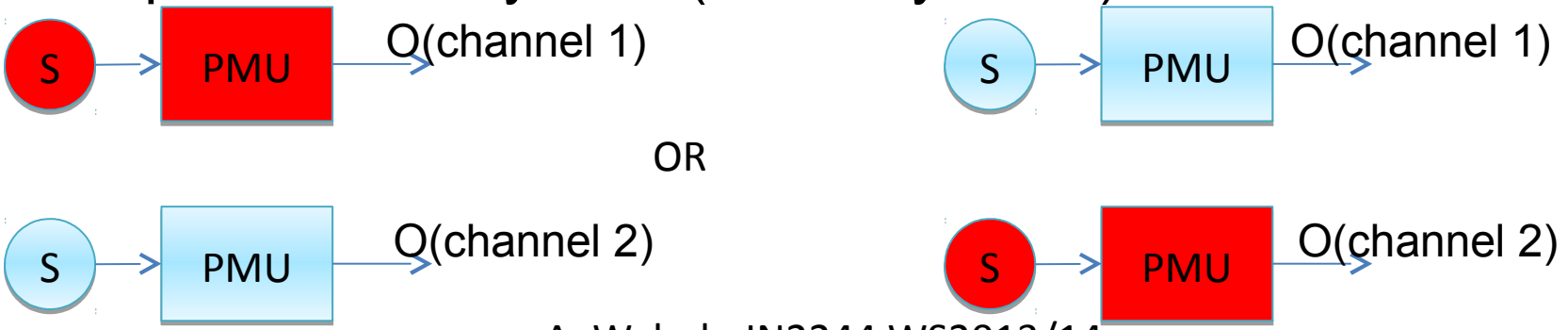


Requirements for Single Channel II

- A 1oo1D architecture for a single channel would meet the SIL2 requirement.
  - uC + additional diagnostic circuit
- SIL3 for software is required (common cause failure).
- SFF = 90% - < 99%
- Process safety time: the deadline on reporting internal or external faults to prevent hazardous states (application specific)

Reliability for 1oo2 Configuration

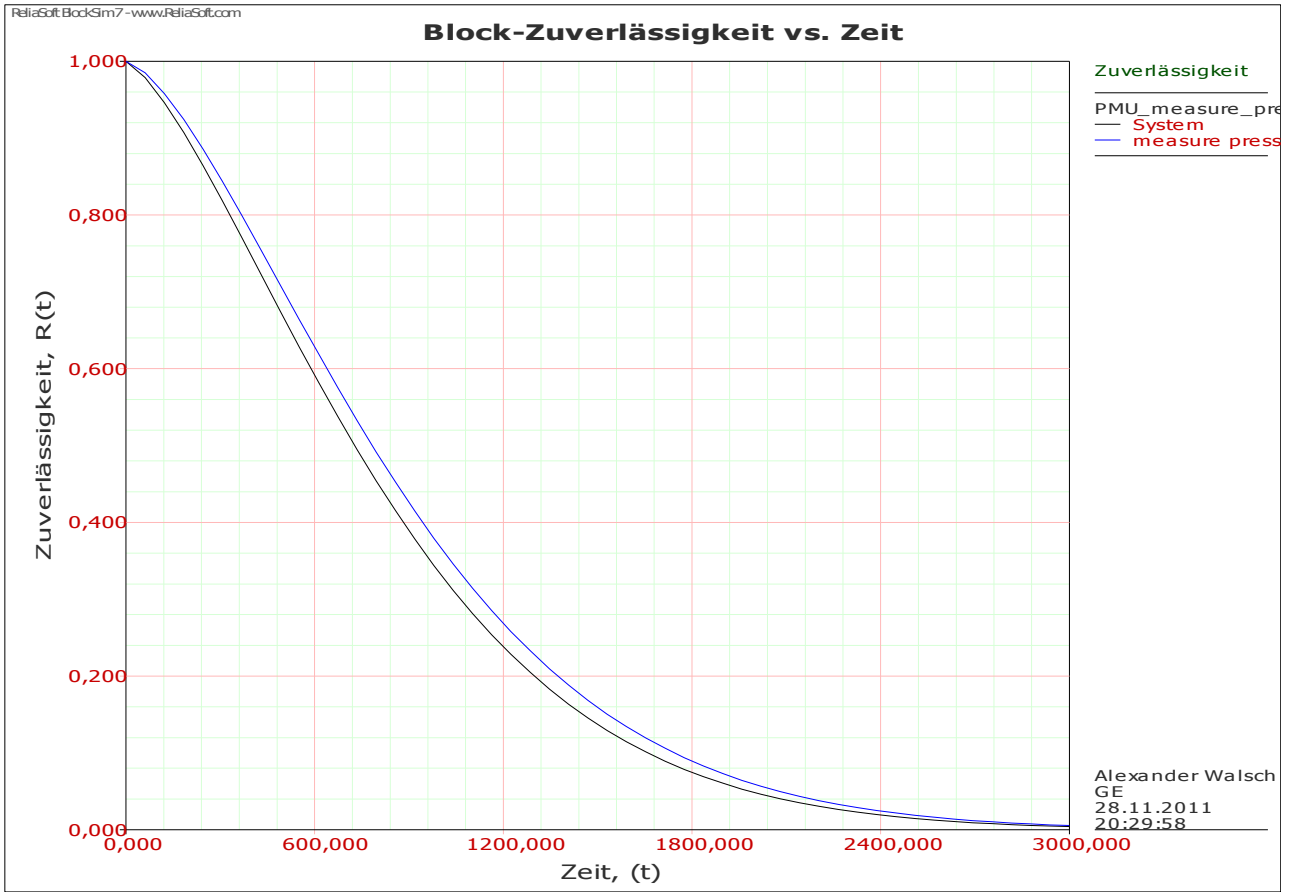
- Reliability of 1oo2 (lecture #2):
  In normal operation a precise and accurate pressure measurement is required
  (measure pressure = functional requirement)
  (precise, accurate = non-functional requirement)
- A PMU can fail safe or dangerously. In both cases two different readings will be provided to the upper level control system. Which one is the correct one? $O(channel\,1) \neq O(channel\,2) \Rightarrow safe\ state$
- The system will enter a fail-safe mode meaning the safety function is not performed anymore (reliability issue).



Reliability of 1oo2 Configuration

- Both channels have to deliver a valid result (no detected faults, within limits) in normal operation.

$$R_{1oo2} = R^2_{Simplex} < R_{Simplex}$$



PMU Requirements Specification

Document No.	Prep By	IN2244	REV					Sheet 1
	AWH	System Requirements Specification - PMU	ECN					Of 12

System Requirements Specification

for

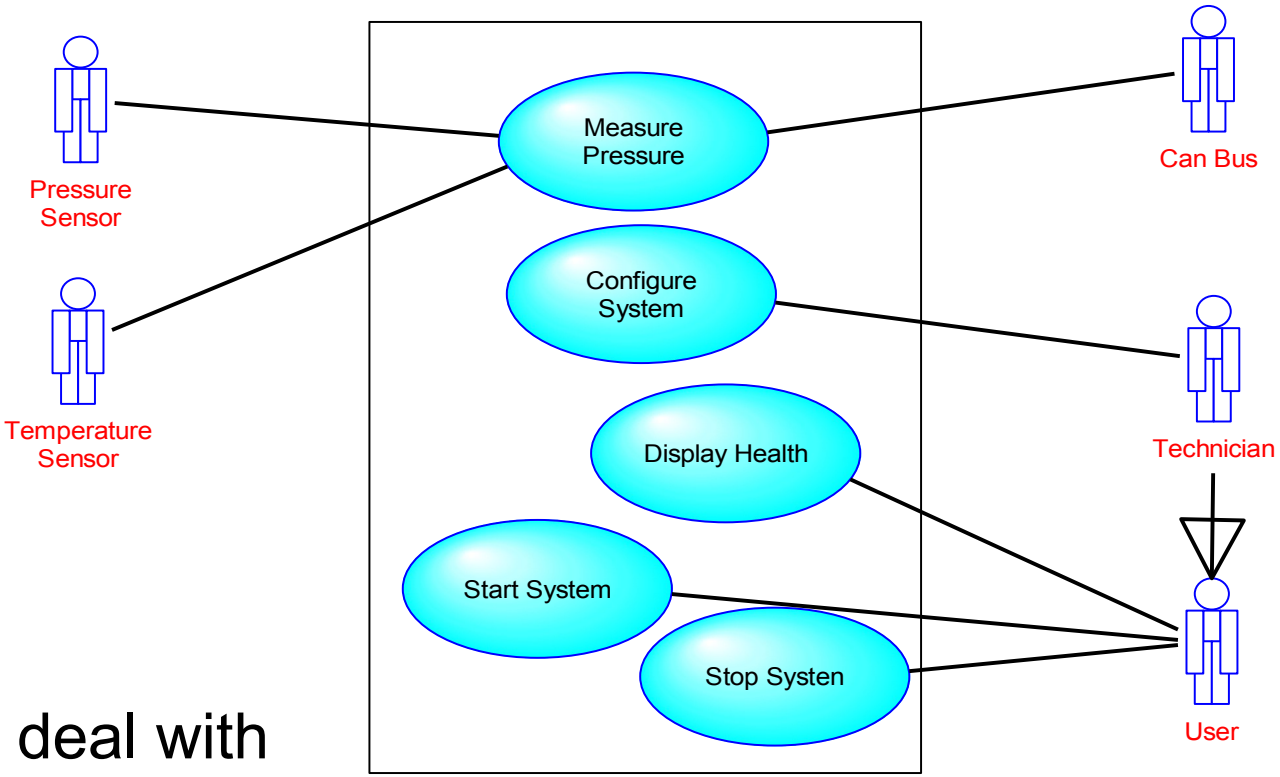
Pressure Measurement Unit (PMU)

Preliminary Information

Backup

PMU – Functional Requirements Analysis

- Use case diagram
- Behaviorally related sequences performed by an actor.
- Actors = external users, systems, components
- system border
- View on the ideal world, deal with deviations from expected behavior later



PMU – Functional Requirements Analysis II

- Pre-conditions and post-conditions are the states of the system before and after successful execution of the use case. These can often be cross-referenced to the states in the system modes diagram.
- Non-functional requirements (see previous lecture)
- Alternate courses are a selection of alternative courses (fault conditions) and scenarios can be listed.
- Example screen layouts are illustrations of screens associated with the use case, including sample user data where available.
- Ties exceptions (faults, errors) and non-functional requirements to a use case
- Sequence diagrams can be added – however, they do not add new information at this stage.

PMU – Functional Requirements Analysis III

- Measure Pressure:

Description	A request is received from the CAN bus. A temperature compensated pressure reading is sent as response.
Pre-condition	The system must be in 'Running' state.
Post-condition	The system will be in 'Running' state.
Non-functional Requirements	Pressure is read with a maximum cycle time of 100ms, output accuracy is 2%, precision is 0.5%.
Alternate Courses	Pressure outputs are in a range equivalent 0 - 16 bar. The valid temperature ranges from -45°C to +85°C. If either range is violated it must be signalled via CAN.

- Configure System:

Description	A request for configuration is communicated to the system. The requester is a technician which is equivalent to someone with restricted access rights. During configuration the system is not accepting CAN requests. The system reports valid configuration.
Pre-condition	The system must be in 'Active' state.
Post-condition	The system will be in 'Active' state.
Non-functional Requirements	Access should be protected by a password. The configuration data shall be stored in non-volatile memory.
Alternate Courses	All configuration options are checked for validity. If the configuration data are not valid the system signals the 'Error' state.

PMU – Functional Requirements Analysis IV

- Display Health:

Description	Health of the system is requested by a user. The system displays health using LEDs. Three LEDs are used. Green for 'Running', Red for 'Error', and yellow for all other system states. The LEDs are visible from outside the system such that the user gets visual feedback.
Pre-condition	The system must be in 'Active' state.
Post-condition	NA
Non-functional Requirements	NA
Alternate Courses	NA

- Start System:

Description	Power is applied and the system starts. The system performs a self test. Upon successful completion the system automatically enters the 'Running' state.
Pre-condition	The system must be in 'Inactive' state
Post-condition	The system will be in 'Active' state
Non-functional Requirements	The system shall be in 'Running' state in less than 10s.
Alternate Courses	If the system detetcts a fault the 'Error' state shall be entered. In this case the system shall report the error state in less than 10s.

PMU – Functional Requirements Analysis V

- Stop System:

Description	Power is removed.
Pre-condition	The system must be in 'Active' state.
Post-condition	The system will be in 'Inactive'state.
Non-functional Requirements	NA
Alternate Courses	NA

- Summary:
  - Identify the actors: external to the system
  - Identify the use cases:
    "A behaviorally related sequence of interactions performed by an actor in a dialogue with the system to provide some measurable value to the actor"
  - Create a use case diagram
  - Write up use case descriptions
- The graphical notation does not add any information but makes talking to stakeholders sometimes easier

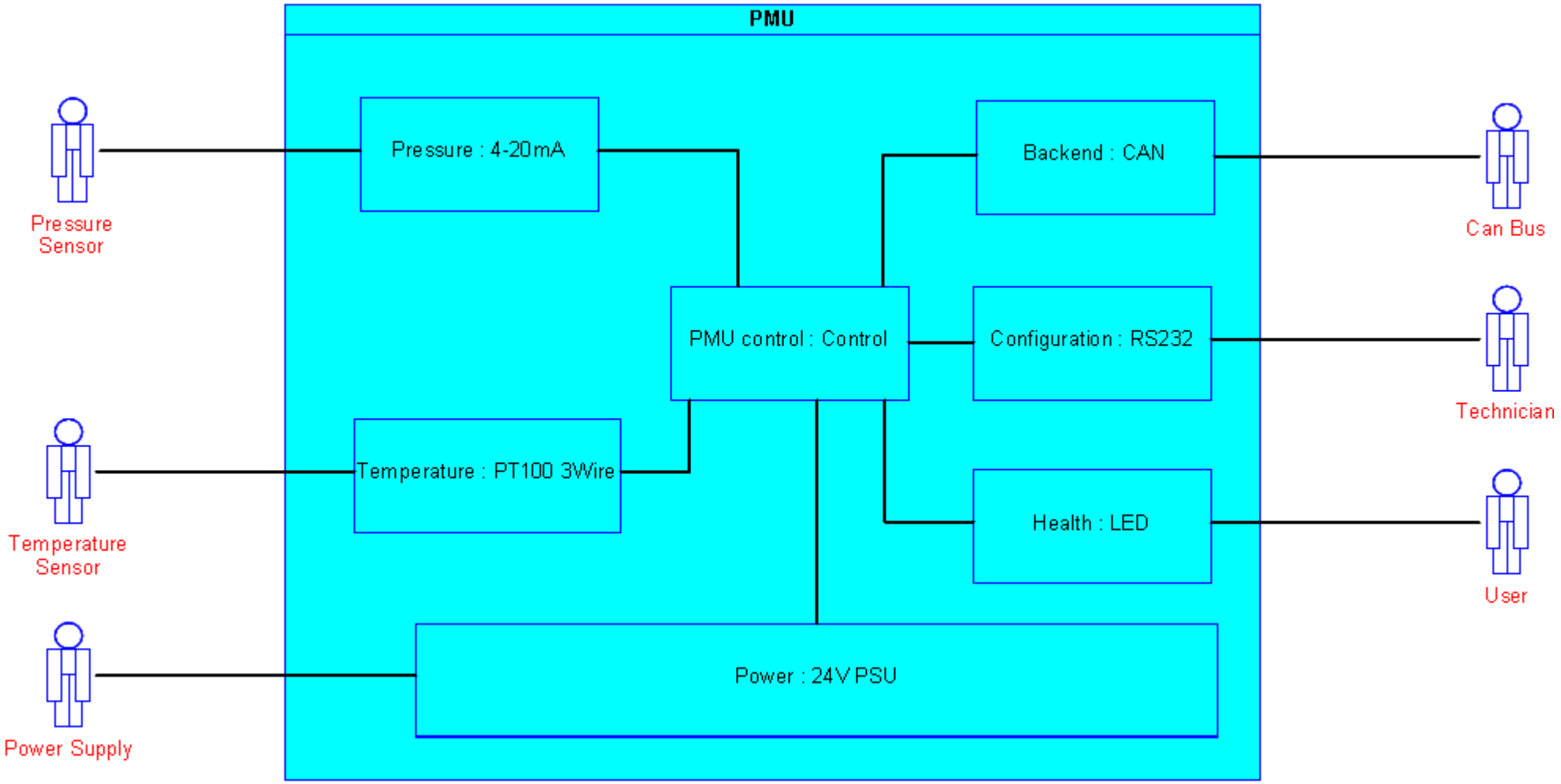
PMU – Functional Requirements Analysis VI

- System Usage Modeling Checklist
  - Scale:
    A manageable number of use cases should be selected – 10 to 20
  - Granularity
    Use cases should be not too high level (e.g. run system) or too low level (too many details)
  - Relevance
    Use cases should display normal actor-system interaction. Fault conditions should be part of more detailed analysis (e.g. in alternate courses)
  - Partitioning
    Use cases describe end-to-end functionality and not generic functions of (to be developed sub-systems)
  - Applicability
    Use case diagrams describe the response to external stimuli. Therefore, they are suited to describe real-time systems on a high level.

PMU – Functional Requirements Analysis VII

- System Usage Diagram does not tell us:
  - Internal Structure:
    What are the components of the systems that interact with the actors (mechanical, electrical, software), is there a component that controls activity?
  - Interface Description:
    Interfaces are modeled as “classes”. A class name can already be used as a description (e.g. I2C bus)
- But the composite structure diagram does
  - Also focuses on the system border, very high-level structural model
  - Shows what is inside and outside our system

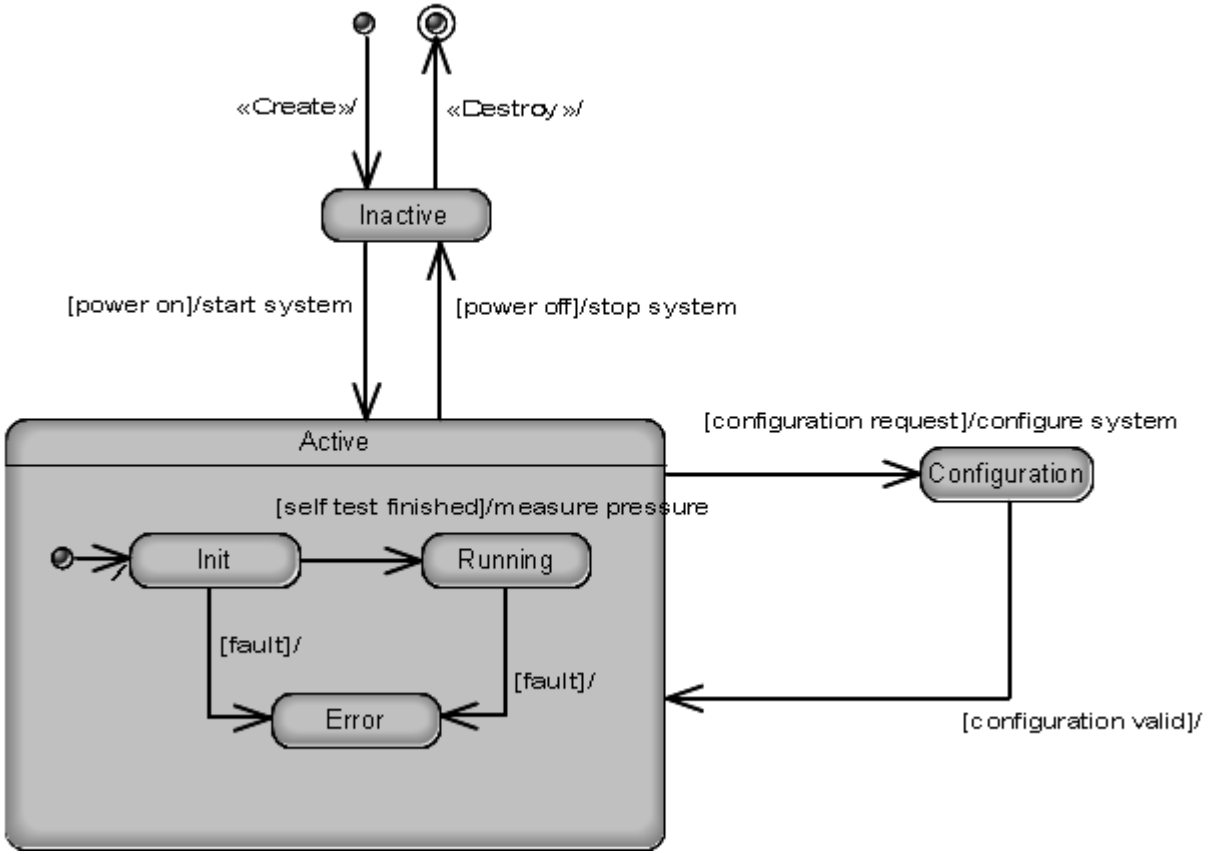
PMU – Scope


PMU
Pressure : 4-20mA
Backend : CAN
PMU control : Control
Configuration : RS232
Temperature : PT100 3Wire
Health : LED
Power : 24V PSU
Pressure Sensor
Temperature Sensor
Power Supply
Can Bus
Technician
User

PMU – Scope II

- Content of Requirements Specification
  - Context structure diagram as in previous slide: shows what is inside and outside the systems responsibility, nature of interfaces:
  - Pressure sensor: 4 – 20 mA, screw terminal, sensor powered externally or by PMU
  - Temperature sensor: PT100 three wire, screw terminal
  - Power: screw terminal
  - CAN: D-sub 9
  - Health: LEDs
  - Config: RS232 – D-sub 9 (PC interface)
  - Interface description can be added to context structure but can also be added as text in the specification

PMU – System States

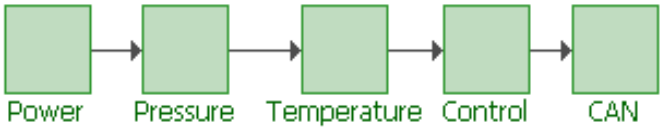


PMU – System States II

- System states: states of the system when viewed as a black box
  - States of the PMU control object
  - States allow or disallow certain use cases
  - State transitions often triggered by actor interaction (see scope in previous slides)
  - Where use cases are shown as actions, it is important to recognize that the action implied is the initiation of the use case, not necessarily its completion.

PMU Reliability

- First we look into a simplex system according to the high level description we have received internally
- We assume reliability metrics from experience or literature.
- We still work at the system border.



MTBF_Power = 2a
MTBF_Pressure = 50a
MTBF_Temp=50a
MTBF_Control=150a
MTBF_CAN=20a

$$\Theta_S = 1.68a$$

PMU Reliability II

- Obviously, power is the system component having the lowest MTBF (2a).
- The function of power is to deliver power to the PMU electronics.
- Power is made of
  - Connectors (mechanics, electronics)
  - Filters, capacitors
  - Step-down converters (do not know exactly what voltage levels at that point) – probably +5V, -5V, +3.3V
- Can we improve power (better MTBF)?
- Does this improvement affect the requirements specification or is it rather a matter of more detailed design?

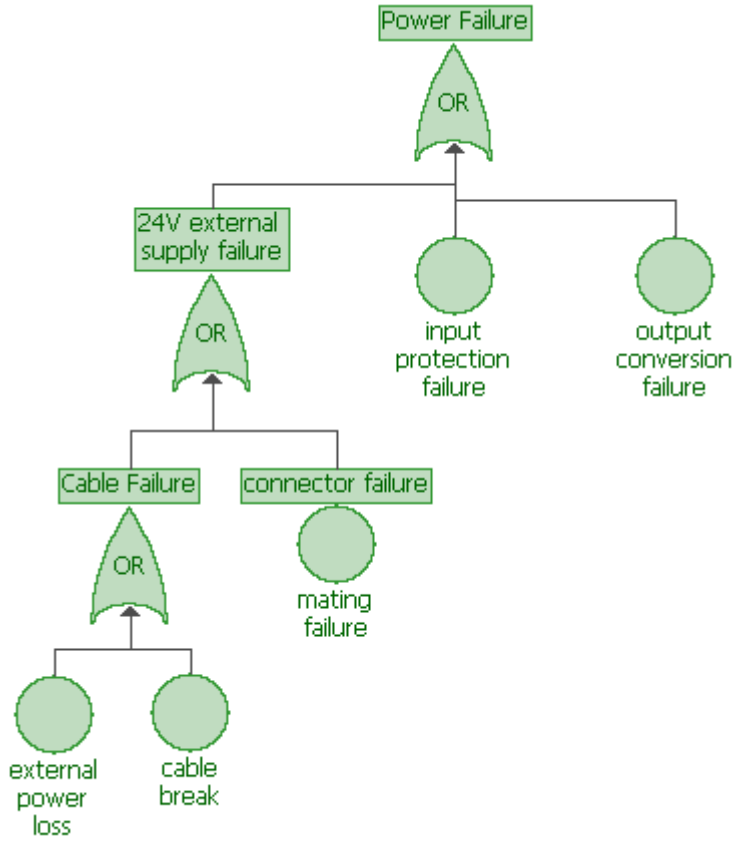
PMU Reliability III

Function	Failure	Effekt	Si	Cause	Oi	Di	RPN
power	external 24V power connection	Total power loss	8	cable breaks	7	5	280
				insufficient mating	5	5	200
	input protection	Total power loss	8	faulty passive components	3	5	120
		power quality loss	7	faulty passive components	2	5	70
	output conversion	partial power loss	8	faulty power conversion electronics	3	5	120

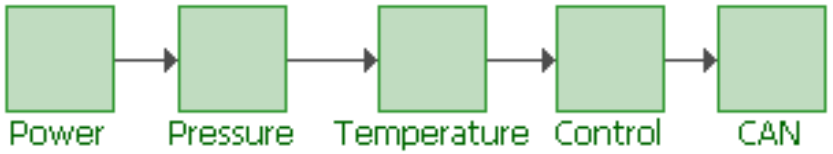
- Function, failure, effect, Si (severity), cause, Oi (occurrence), Di (detectability) to be filled in -> Risk Priority Number
- Now we think about how we can mitigate the effects with respect to the system level
- An obvious approach here would be to use a second independently routed power cable.

PMU Reliability IV

- FTA is another way of analyzing the systems.
- Gives us the root cause of a failure.
- Cable failure is further analyzed asking “Why?”.
- FTA more powerful when analysis of combinations are necessary.

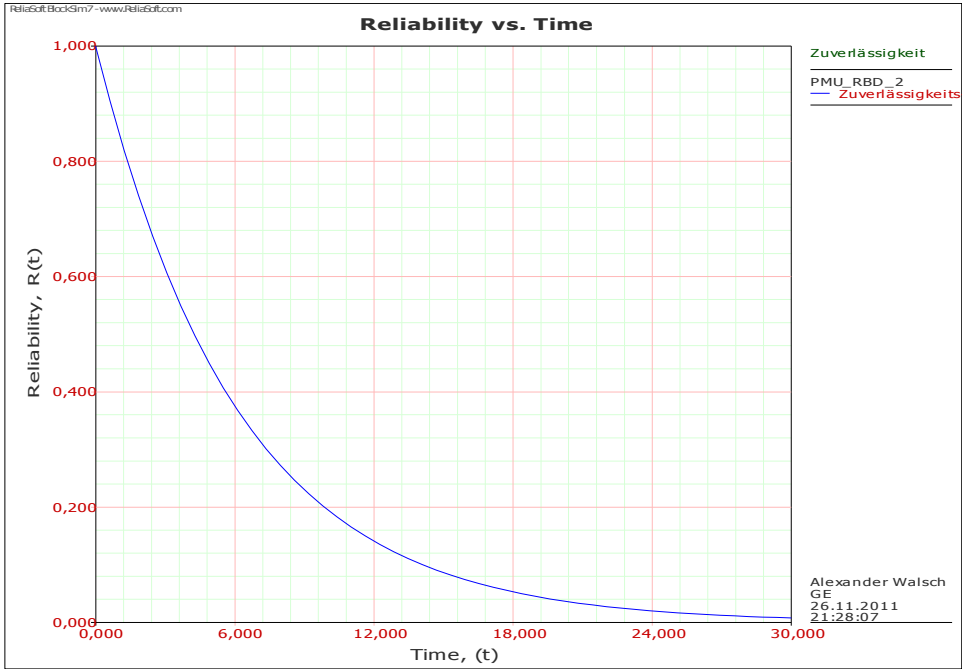


PMU Reliability V



MTBF_Power = 15a
MTBF_Pressure = 50a
MTBF_Temp=50a
MTBF_Control=150a
MTBF_CAN=20a

$$\Theta = 6{,}1195\, a$$



A second power connector is added. It increases the MTBF (details are not clear at this point).