Industrial Embedded Systems
- Design for Harsh Environment -

Dr. Alexander Walsch
alexander.walsch@ge.com

WS 2011/12

Technical University Munich (TUM)

Agenda

Today:

Requirements Specification for PMU

Recap:

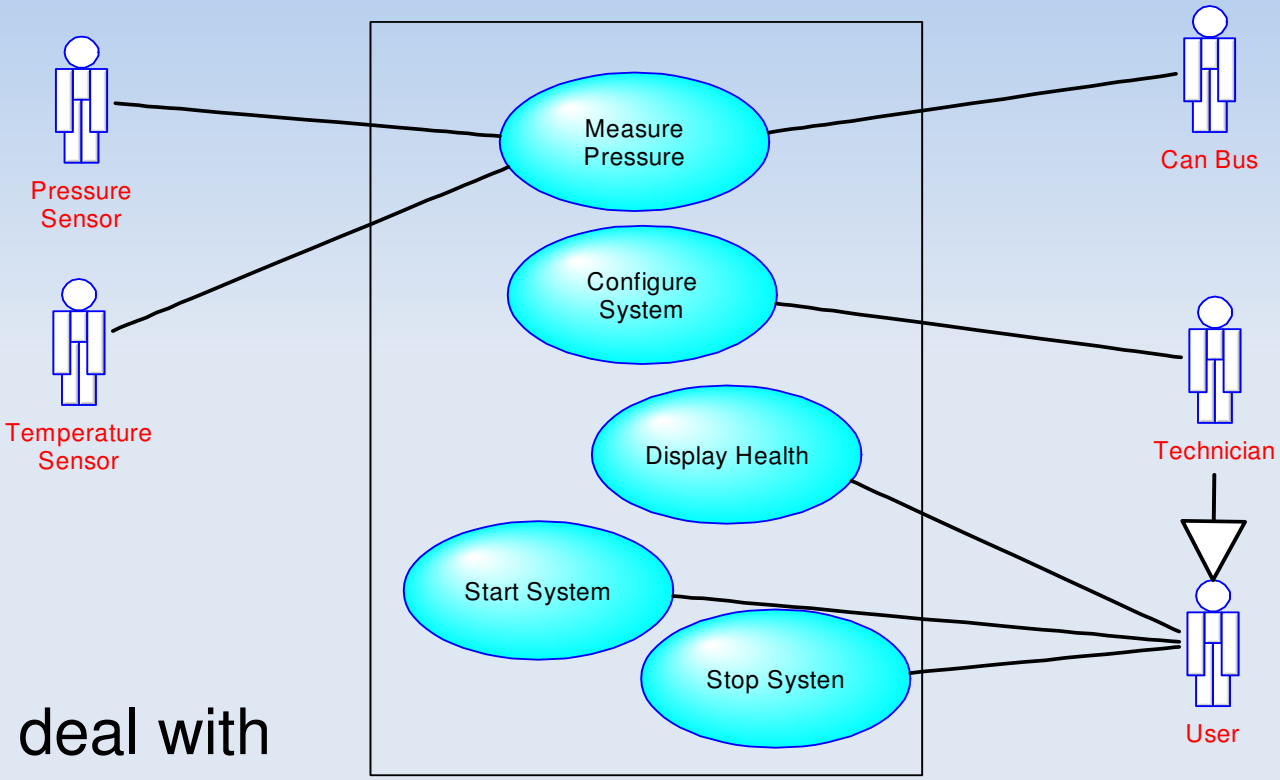
- Safety (risk analysis, safety function, safety integrity)

PMU – Next Steps

- Refine existing UML diagrams – completeness, team approach
- Add global non-functional requirements
- Refine system in terms of reliability and safety (use methods like FMEA and FTA)
- Write a specification document which will conclude the requirements phase
- We will return at a later stage and see how test cases can be developed

PMU – Functions Overview

- 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 – Functions Ctd.

- 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 lecture #2)
- 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 – Functions Ctd.

- 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 – Functions Ctd.

- 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 – Functions Ctd.

- 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

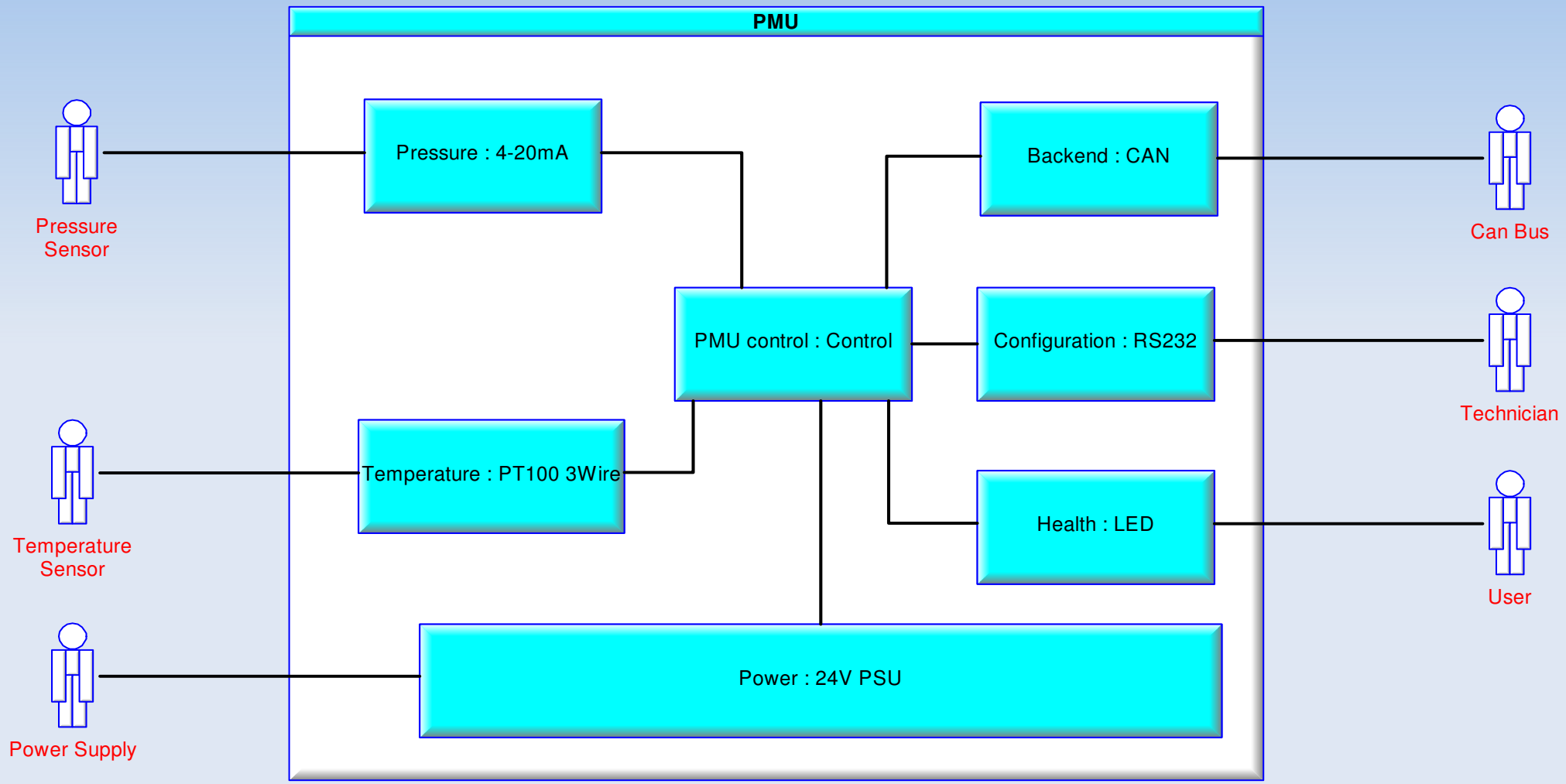
PMU – Functions Ctd.

- 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 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 – Functions Ctd.

- 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. I^2C 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

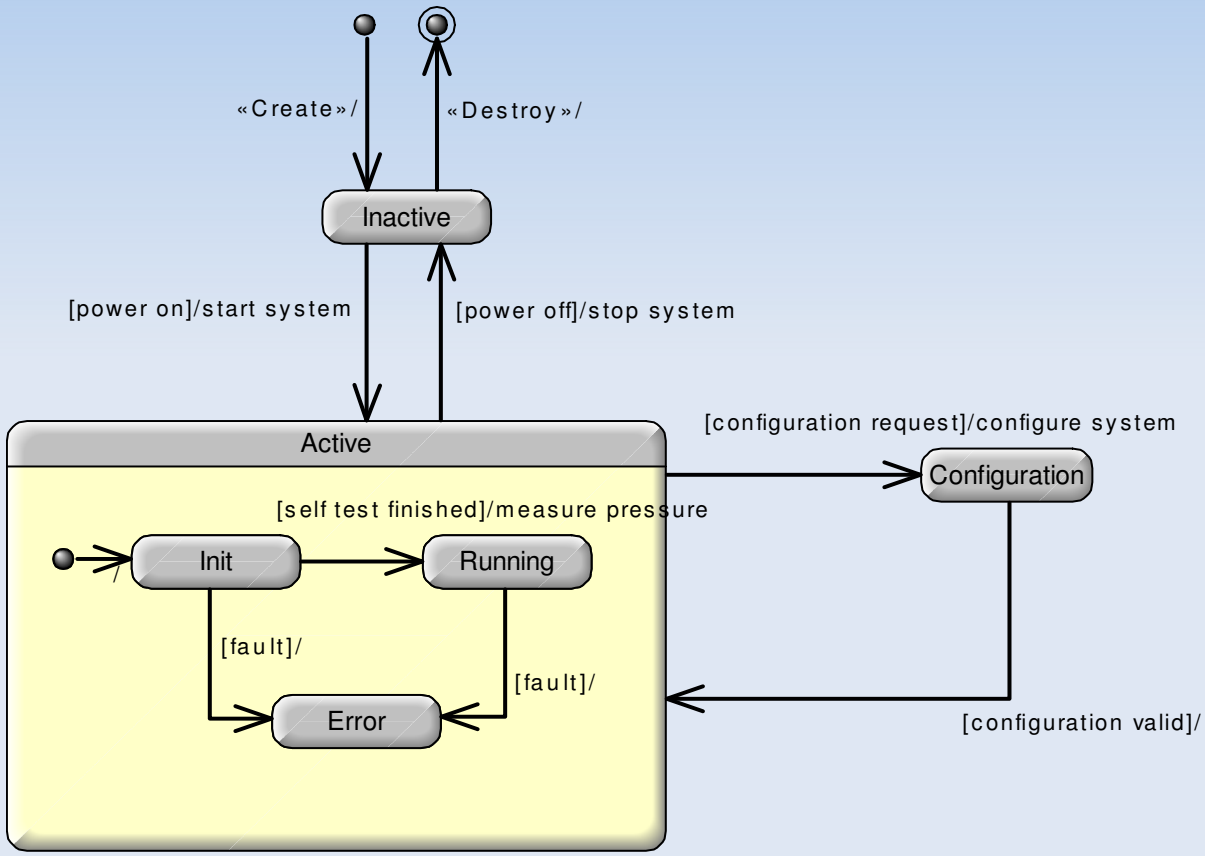
PMU – Scope


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 Ctd.

- 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

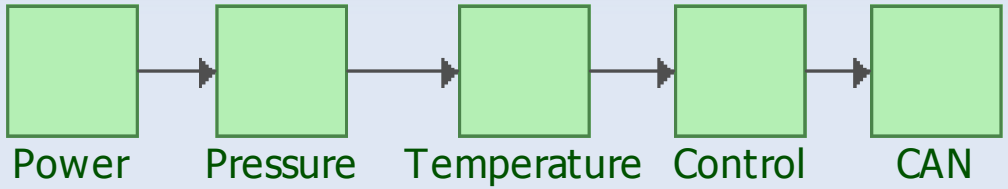
- System states: states of the system when viewed as a black box
  - States of the PMU control object
  - States allow or disallow certain use cases
  - State transitions often triggered by actor interaction (see scope in previous slides)
  - Where use cases are shown as actions, it is important to recognize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

PMU – Non-functional Requirements

- Material cost < $50
- Power consumption < 2 W
- Physical PCB size 50 x 25 x 10 mm
- Ambient operating temperature -40 degree C to +85 degree C
- PIC uC as compute resource
- Industrial connectors for communication and power
- Performance will not be modeled (difficult in UML anyways)

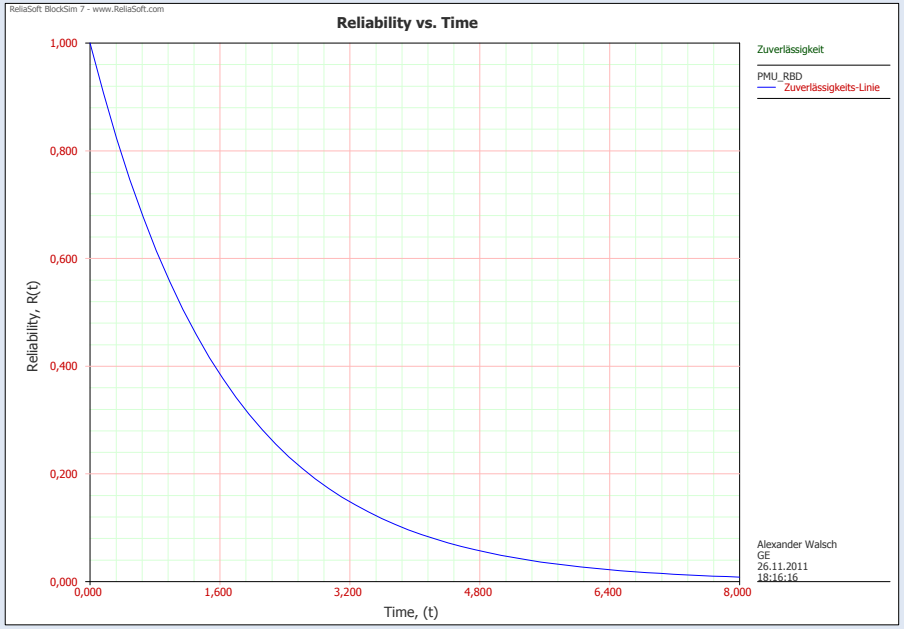
PMU Reliability

- First we look into a simplex system according to the composite structure diagram.
- 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 Ctd.

- 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?

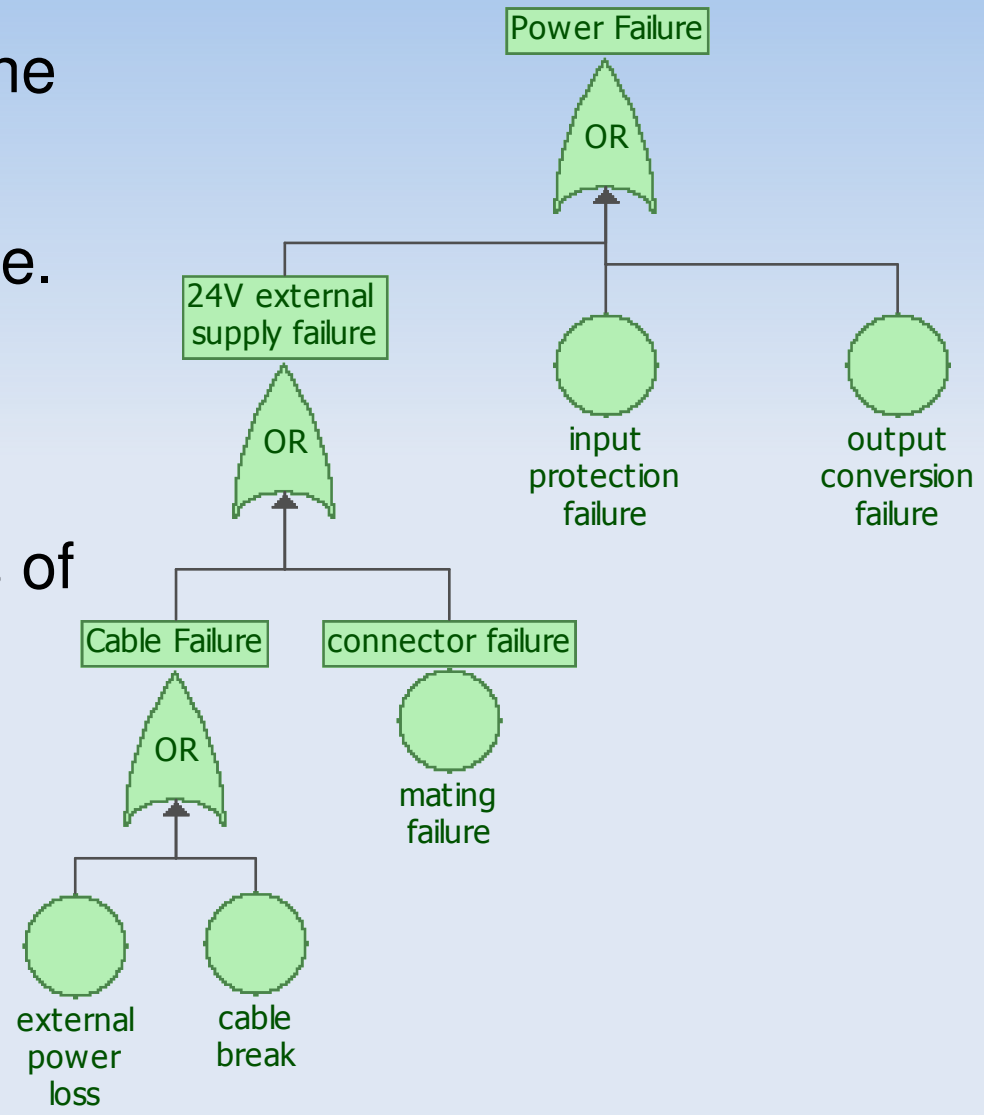
PMU Reliability Ctd.

Function	Failure	Effekt	Si	Cause	Oi	Di	RPNi
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

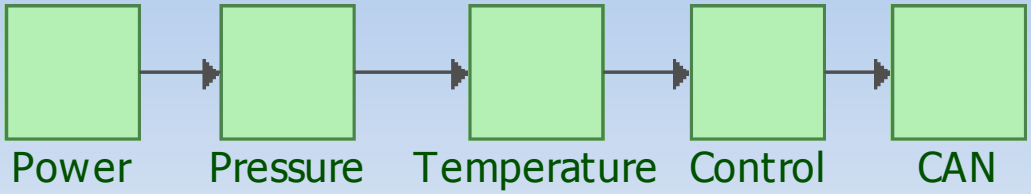
- Function, failure, effect, Si (severity), cause, Oi (occurrence), Di (detectability) to be filled in -> Risk Priority Number (lecture #3)
- Now we think about how we can mitigate the effects with respect to the system level
- An obvious approach here would be to use a second independently routed power cable.

PMU Reliability Ctd.

- 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 Ctd.



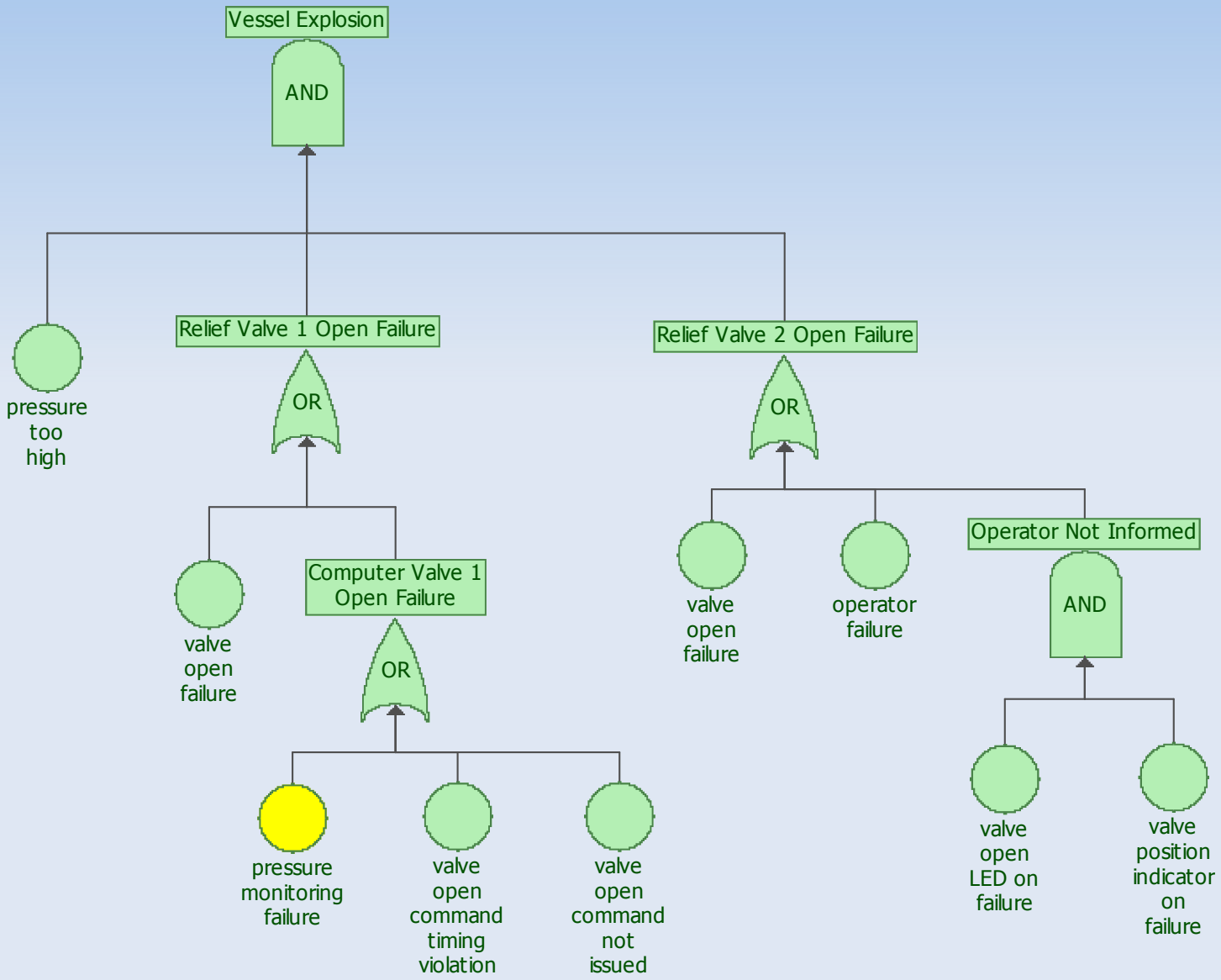
MTBF_Power = 15a
MTBF_Pressure = 50a
MTBF_Temp=50a
MTBF_Control=150a
MTBF_CAN=20a

$\Theta_S = 6{,}1195a$ in new configuration -> a second power connector is added. It increases the MTBF (details are not clear at this point).

Safety

- Safety is a system approach. The safety function and the safety integrity has to be met on the system level (last lecture).
- 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 the marketing organization communicated:
  - SIL3 in a 1oo2 configuration (duplex)
  - SIL2 for simplex
- Requirements specification needs to hold the safety function.
- Also additional project planning activities need to be known (not part of this class) at the requirements stage.

System Safety FTA

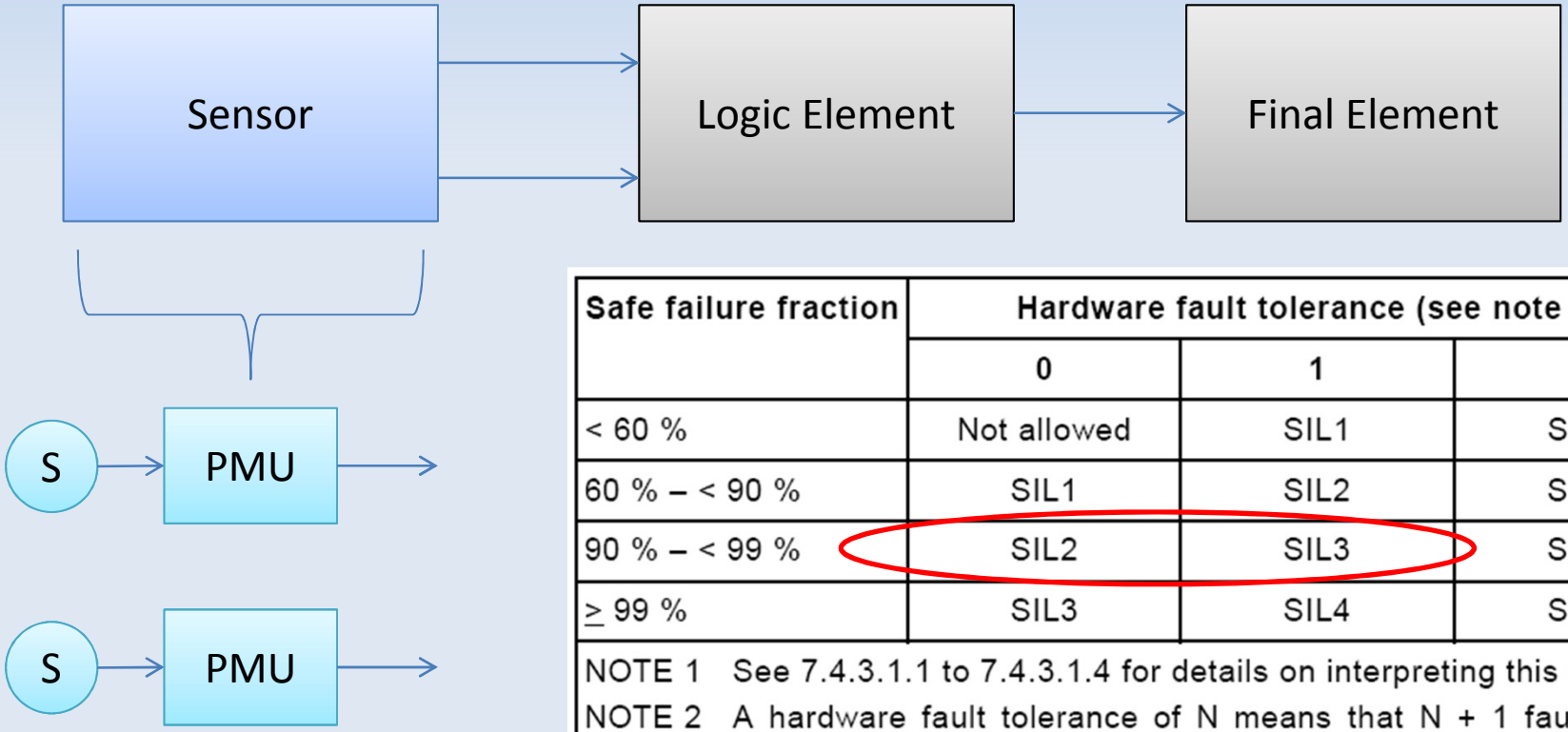


Safety Function

- Wrong pressure readings can lead to hazardous states and possibly to harm at the 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) and limit violations need to be detected and communicated.
- Therefore, the safety function can simply be phrased like:
  "*The PMU shall communicate a pressure limit violation*".
  The message indicating the limit violation is the "safe state".
- The safety function comes with non-functional requirement – the SIL (last lecture), limit settings, etc.

Safety Function

- From marketing we know that the SIL of the PMU shall be 3 in a 1oo2 configuration. A system configuration might look like this:



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

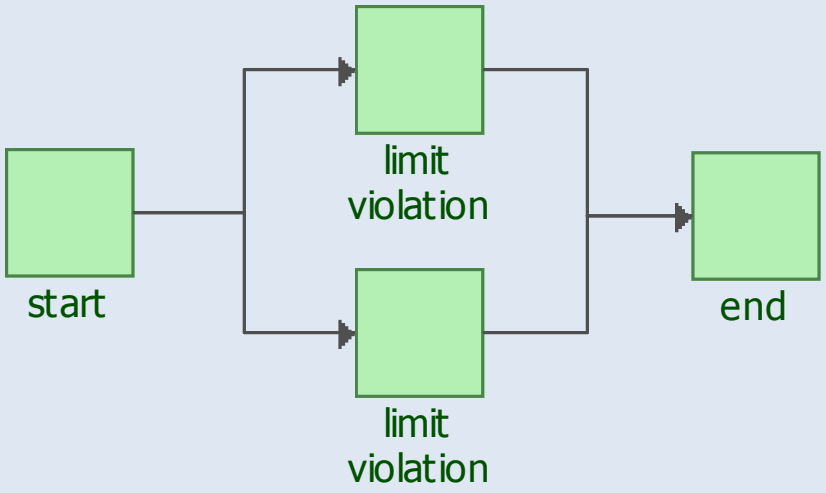
NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.

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.

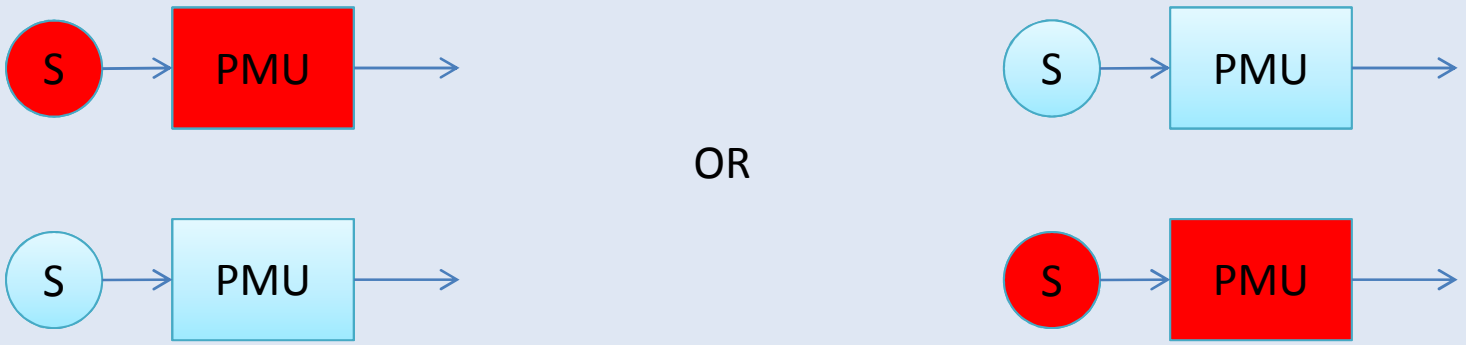
Safety Function

- Reliability of 1oo2 (lecture #2):
  $R_{1oo2} = 2R - R^2 > R_{simplex}$; $R_{simplex}$ being the reliability of the safety function in a simplex configuration
  this is the “random failure” portion of the reliability aspect. More to come.



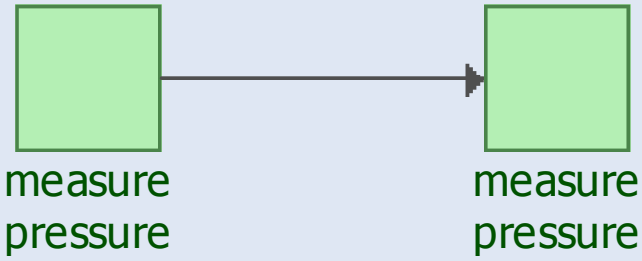
PMU Availability

- Availability of 1oo2 (lecture #2):
  In normal operation a precise and accurate pressure measurement is required
  (measure pressure = functional requirement)
  (precise, accurate = non-functional requirement)
- If a fault of any kind is detected on either channel of the PMUs the safe state is signalled and the channel is repaired (or rebooted after physical inspection)
- During that time the output of the 1oo2 system is “safe state”:



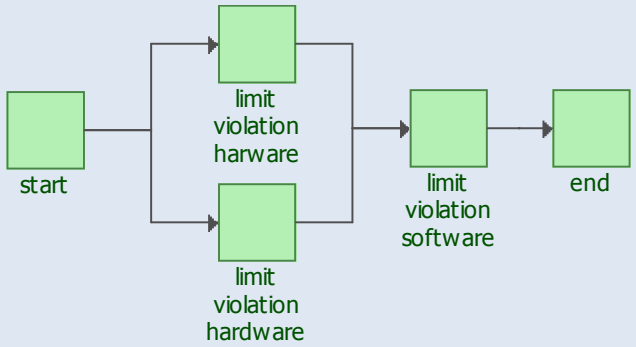
PMU Availability Ctd.

- Both channels have to deliver a valid result (no detected faults, within limits) in normal operation.
  $R_{1oo2} = R^2$ (lecture#2: the reliability is always referring to a function)
  availability decreases

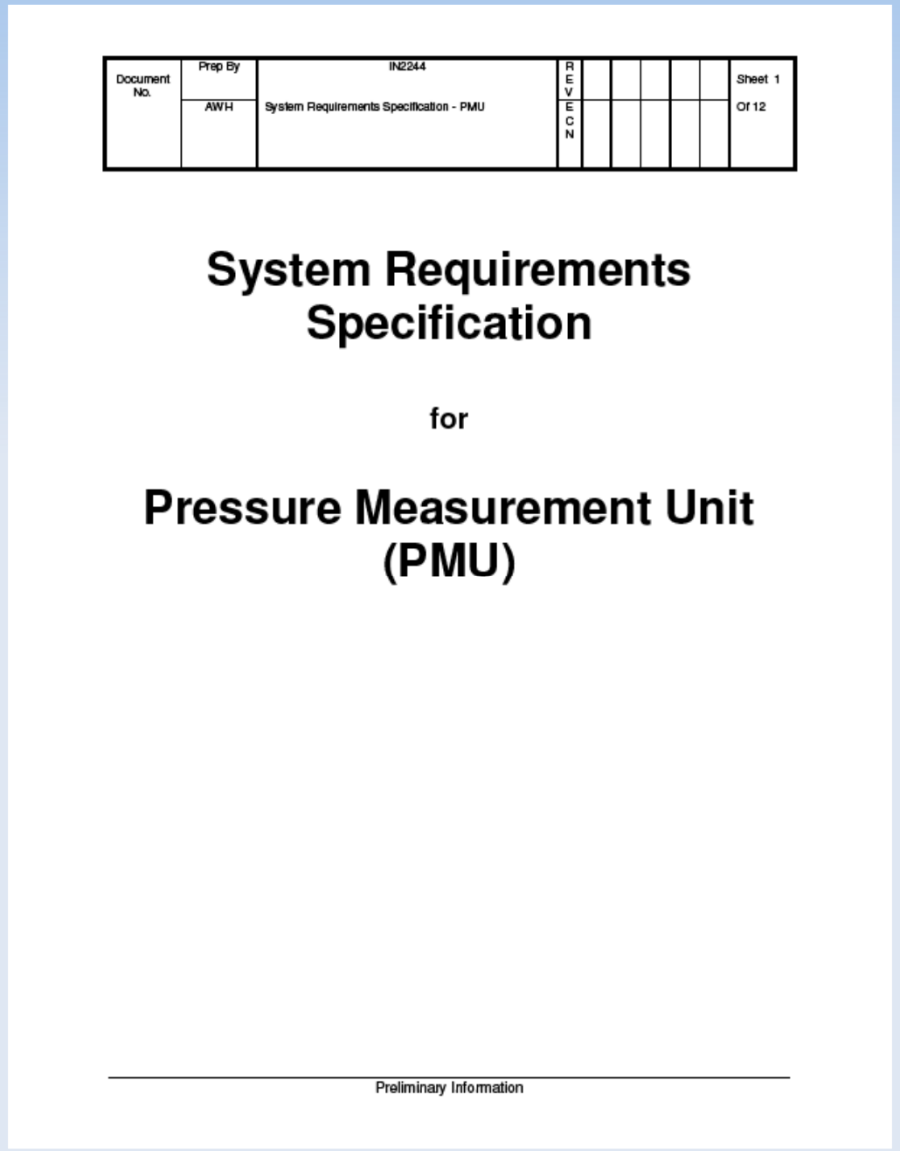


Systematic Failures

- So far only random hardware failures (see bathtub curve) have been considered.
- Systematic failures, especially software, has not been considered.
- We have seen that reliability of the safety function can be increased by adding redundancy (from SIL2 to SIL3).
- What about software? Software is considered to show systematic failures which can not be modeled in reliability diagrams as shown before. Systematic failures are somehow similar to common mode failures (failures which affect each channel the same way). Therefore:



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