Industrial Embedded Systems
- Design for Harsh Environment -

Dr. Alexander Walsch
alexander.walsch@ge.com

Part VII

WS 2011/12

Technical University Munich (TUM)

Agenda

Today:

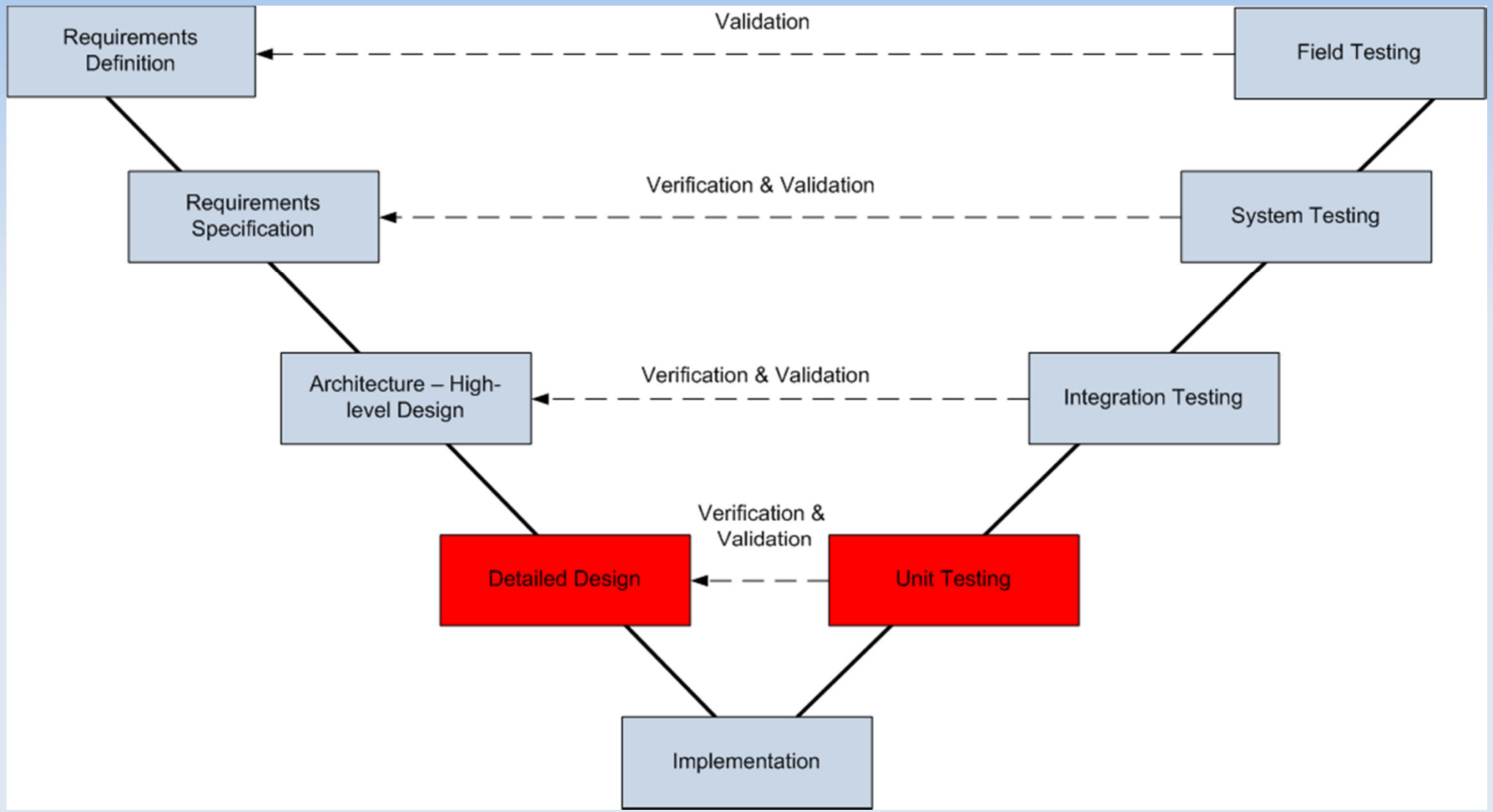
ADD for PMU (Architecture and Detailed Design)

Testing

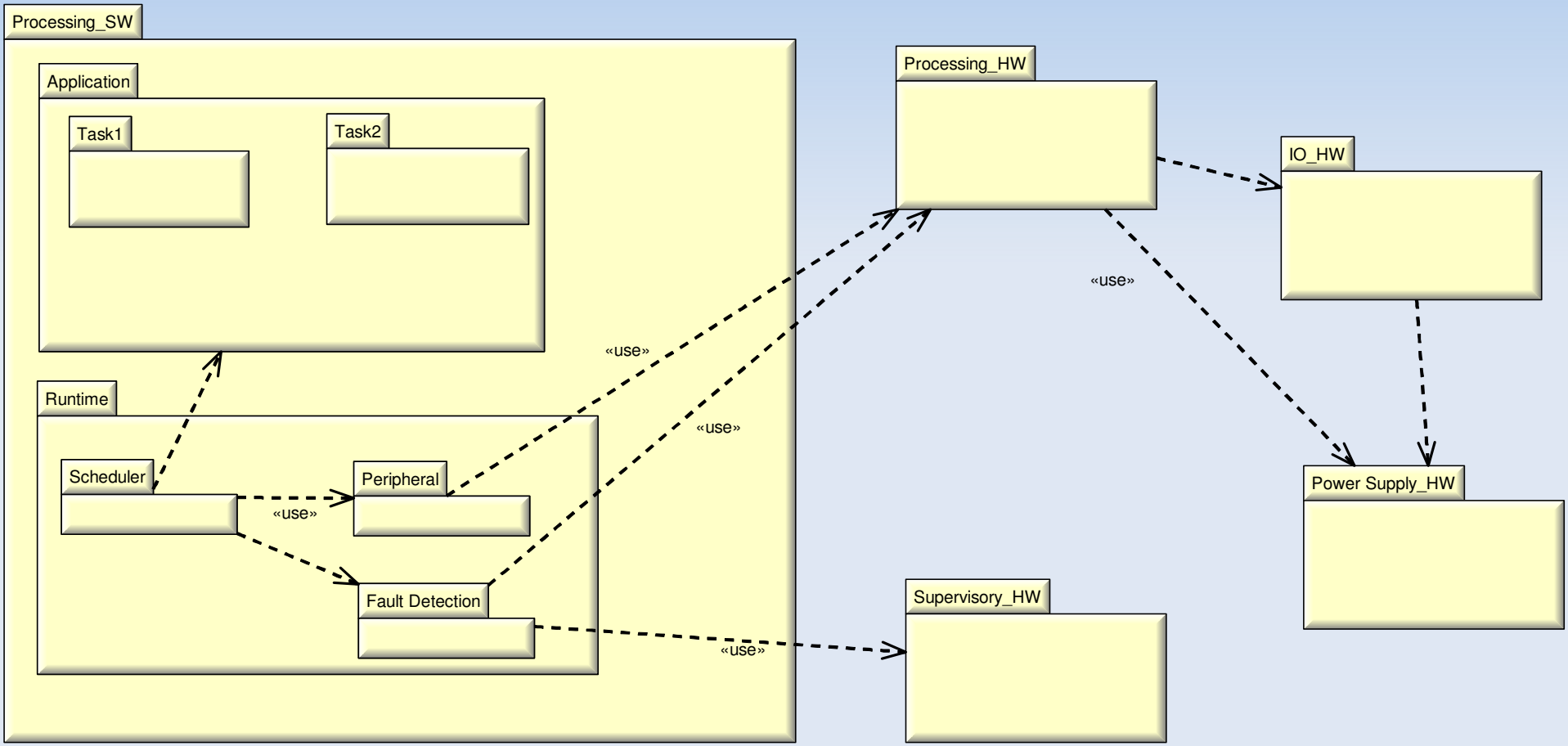
Recap:

- Architecture – High Level Design (Software)

V-Model


Requirements Definition
Validation
Field Testing
Requirements Specification
Verification & Validation
System Testing
Architecture – High-level Design
Verification & Validation
Integration Testing
Verification & Validation
Detailed Design
Unit Testing
Implementation

Architecture
- System View (HW and SW)-

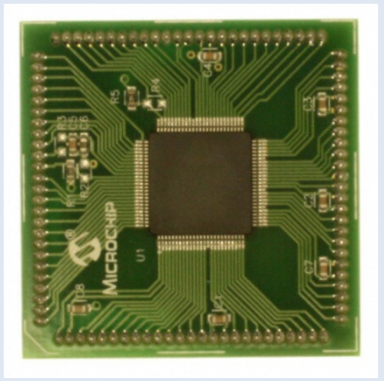


Architecture and Detailed Design
- System View-

- Hardware and software two different disciplines executed in parallel during detailed design, implementation, and unit testing.
- Disciplines get together again at integration testing stage (HW and SW integration).
- HW design:
  - Architectural blocks (see previous slide) transferred into CAD tool.
  - Larger components get selected
  - Detailed circuit design, simulation, reliability calculations
- SW design:
  - Architectural blocks get refined (could happen in same tool – but only makes sense for auto-coding)
  - Detailed object design (function, data)

Hardware
- Bill Of Material (BOM) -

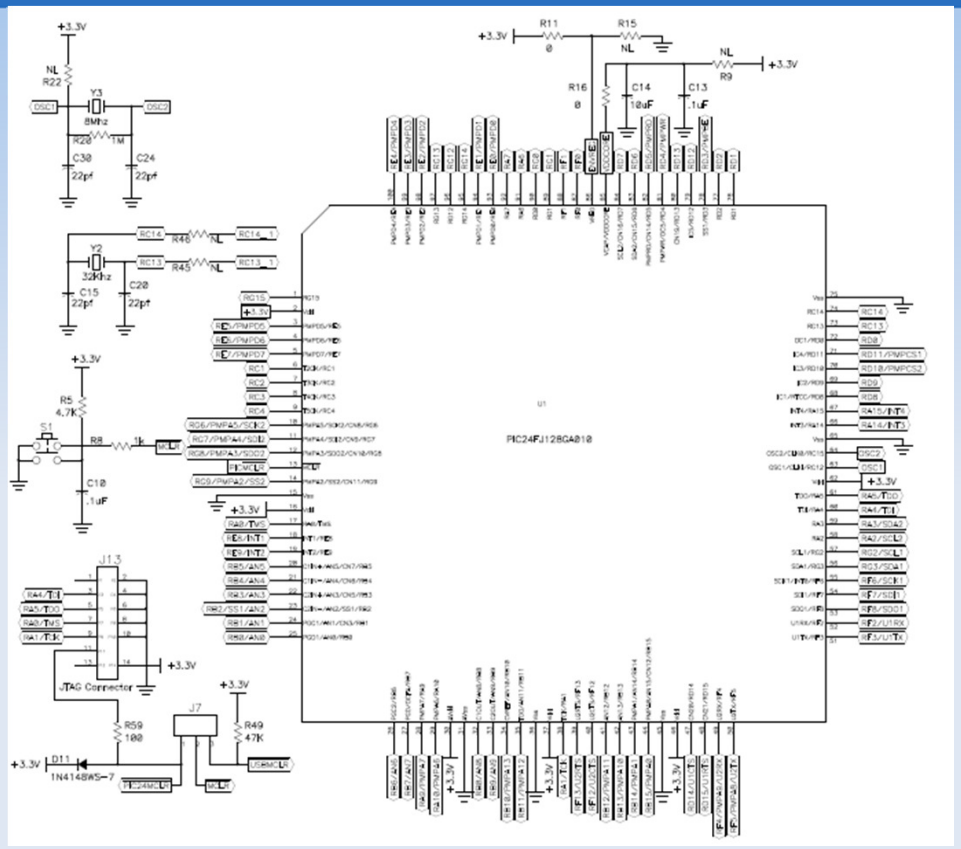
Function	Device	Size	Voltage	Number
PMU control	Microchip dsPIC33FJ128GP710	14x14x1 mm (TQFP-100)	3.3V	1
pressure 4-20mA screw terminal	Phoenix Contact MKDSN 1.5/2-5.08	8.1x10.2x10 mm	NA	1
24V DC power screw terminal	Phoenix Contact MKDSN 1.5/2-5.08	8.1x10.2x10 mm	NA	2
PT100 3 wire screw terminal	Phoenix Contact MKDSN 1.5/3-5.08	8.1x15.3x10 mm	NA	1
RS232 D-sub 9 receptical	Tyco Electronics 747844-5	12.6x30.8x12.5 mm	NA	1
CAN D-sub 9 receptical	Tyco Electronics 747844-5	12.6x30.8x12.5 mm	NA	1
PT100 current source	National Semiconductor LM317	5x6.2x1.8 mm (SO-8)	5V	1
PT100 signal conditioning OpAmp	LT1097	5x6.2x1.8 mm (SO-8)	5V	1
RS232 physical line driver	MAX221	5x6.2x1.5 mm (SSOP-16)	5V	1
CAN transceiver	TI SN65HVD234	5x6.2x1.8 mm (SO-8)	3.3V	1
8.000MHz CRYSTAL 20pf	tbd	11.8x5.5x2.5 mm	3.3V	1
on-board temperature	Microcip TC1047	2.7x3.1x1.2 mm	3.3V	1
Watchdog (windowed) and voltage supervision	MAX6324	3x3.1x1.5 mm (SOT23)	3.3/5V	2
power supply	LT3645	3.5x3.5x0.8 mm	24V	1

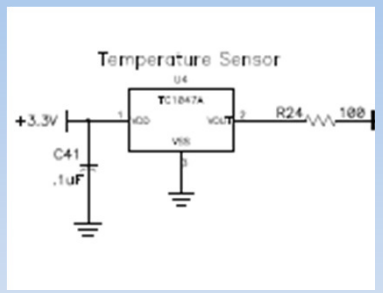


Hardware Ctd.

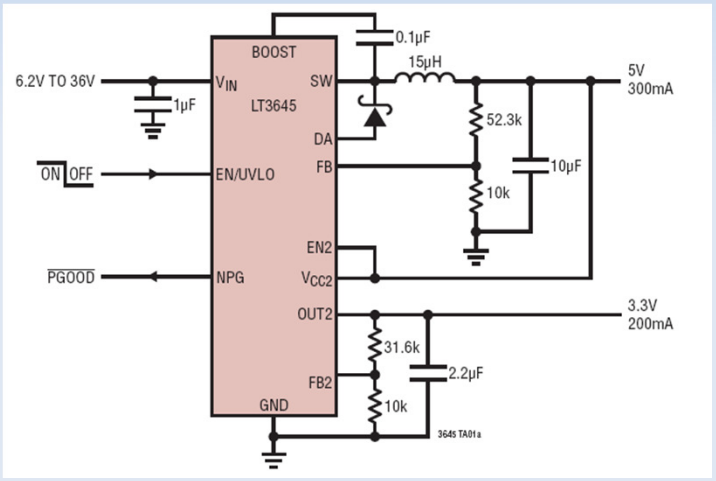
- BOM of big parts see previous slide. Small parts (resistors, capacitors, diodes, etc.) missing.
  - Calculated area: 1481 mm^2
  - Target area: 1250 mm^2 physical PCB size (PMUSysRQ 20)
- We could stay with selected components or try to minimize area of connectors (especially D-sub)
- Hardware designer figures out right components (requirements defined) and their interconnection:
  - Data sheets
  - White papers and application notes
  - Documents that come with eval boards (schematics, BOM)
  - Test setups and/or simulation

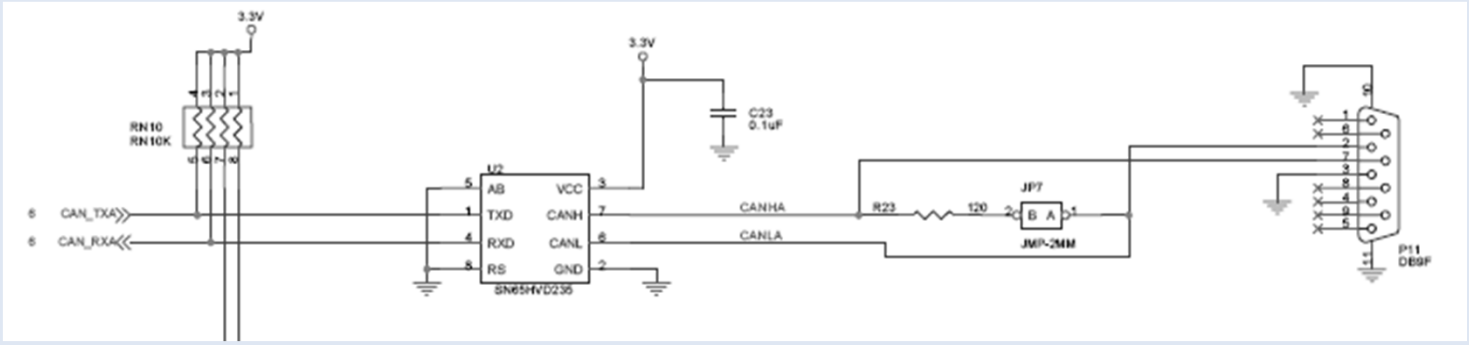
Hardware Ctd.





Source: microchip.com, ti.com and linear.com





Design Reliability

- Reliability is generally related to a function. Therefore, we can either calculate a reliability for our main function („measure pressure“) or the safety function („communicate pressure limit violation“)
  - Reliabilty looks at all failure modes (λ)
  - Safety looks at dangerous failure modes (λ_d)
- IEC61508 requires a safety-related system either to be high-demand or low-demand. The demand mode determines if a PFD or PFH metric is used to show quantitative safety integrity
  - High-demand: in general safety integrity is associated with the failure rate of the safety function (a failure always results in a hazardous system state)
  - Low-demand: integrity is associated with the failure rate and the MDT (unavailability) caused by the failure (a failure not necessarily results in a hazardous system state since the failure might be dormant)

Determination of λ_d

- FMEDA (Failure Mode Effects and Diagnostic Analysis)
  - Take one block (a collection of electronics components)
  - Input: λ values taken from literature (see lecture #2 - literature) or IC vendors
  - Each failure mode (λ) can be safe or dangerous from a safety perspective (λ_d and λ_s)
  - A dangerous component failure can be transferred to a safe failure by the concept of DC (see lecture #VI – fault detection)
  - Output: λ_d, λ_s, λ_{du}, $\lambda_{dd,}$,SFF (qualification of architecture)
- Use λ_d in RBD or FTA to combine different blocks to system
- λ_d used to calculate PFH(PMU is a high-demand system)
- SFF used to qualify architecture (SFF and HW fault tolerance) for a SIL

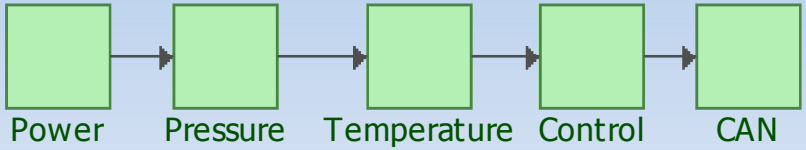
FMEDA Example

Component Reference	Description	safety relevant	λtotal (FIT)	Failure mode	Failure kind	Failure distribution (%)	λs (FIT)	λd (FIT)	DC	λdd (FIT)	λdu (FIT)
R1	resistor	yes	5	short	dangerous	50	NA	2,5	0	0	2,5
				open	safe	50	2,5	NA	0	NA	NA
U2	ADC	yes	1000	stuck-at	dangerous	50	NA	500	90	450	50
				drift	dangerous	50	NA	500	60	300	200
sum								1002,5		750	252,5

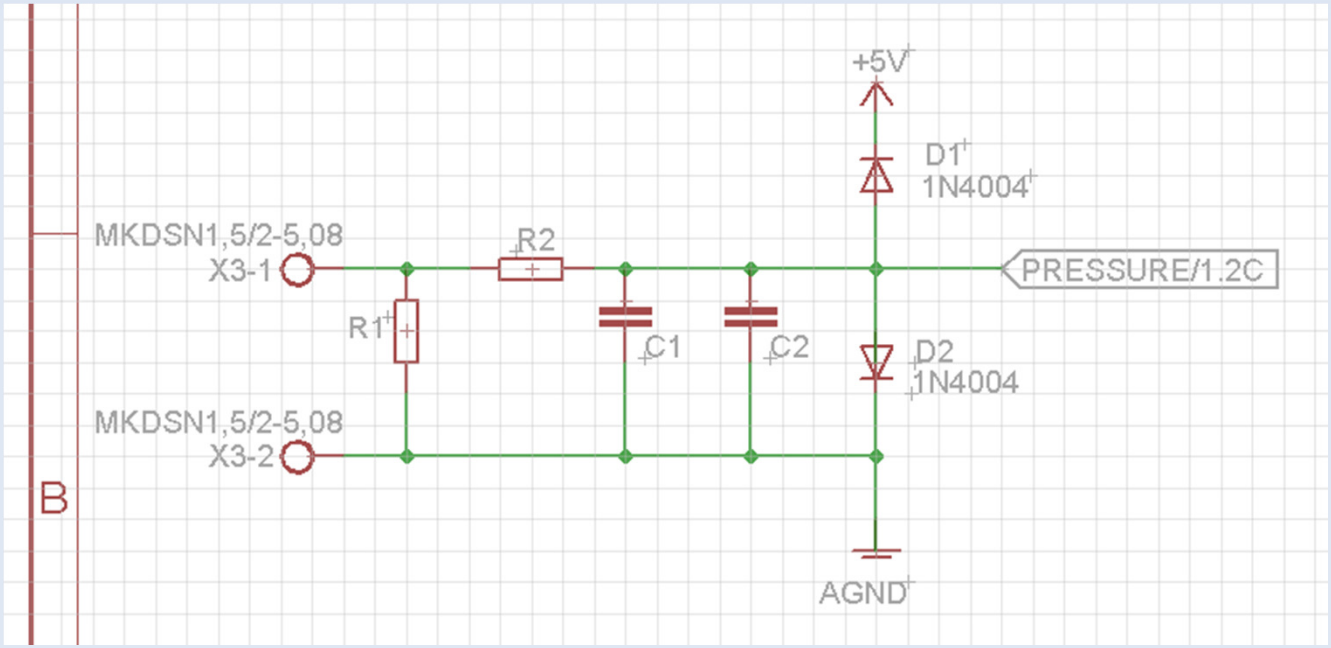
- We use simple spreadsheet – there are some tools out there (TUV, exida)
- $\lambda_{total} = \lambda_{du} + \lambda_{dd} + \lambda_{sd} + \lambda_{su}$
- $DC = \sum \lambda_{dd} / \sum \lambda_{d}$ (see lecture#6 - fault detection)
- $\lambda_{dd} = \lambda_{d} \times DC/100$ (see lecture#6 - fault detection)
- $\lambda_{du} = \lambda_{d} \times (1 - DC/100)$
- $SFF = 1 - \sum \lambda_{du} / \sum \lambda_{total}$

PMU Example

- From requirements analysis:



- We focus on one block (pressure) or a part of it:



PMU Example Ctd.

Component Reference	Description	safety relevant	λtotal (FIT)	Failure mode	Failure kind	Failure distribution (%)	λs (FIT)	λd (FIT)	DC	λdd (FIT)	λdu (FIT)
R1	resistor	yes	0,05	short	dangerous	10					
				open	dangerous	90					
R2	resistor	yes	0,05	short	dangerous	10					
				open	dangerous	90					
C1	capacitor	yes	2	short	dangerous	30					
				open	dangerous	30					
				drift	dangerous	40					
C2	capacitor	yes	2	short	dangerous	30					
				open	dangerous	30					
				drift	dangerous	40					
D1	diode	yes	10	short	dangerous	50					
				open	dangerous	50					
D2	diode	yes	10	short	dangerous	50					
				open	dangerous	50					

- Now: determination of λ_d and λ_s

PMU Example Ctd.

Component Reference	Description	safety relevant	λtotal (FIT)	Failure mode	Failure kind	Failure distribution (%)	λs (FIT)	λd (FIT)	DC	λdd (FIT)	λdu (FIT)
R1	resistor	yes	0,05	short	dangerous	10	NA	0,005			
				open	dangerous	90	NA	0,045			
R2	resistor	yes	0,05	short	dangerous	10	NA	0,005			
				open	dangerous	90	NA	0,045			
C1	capacitor	yes	2	short	dangerous	30	NA	0,6			
				open	dangerous	30	NA	0,6			
				drift	dangerous	40	NA	0,8			
C2	capacitor	yes	2	short	dangerous	30	NA	0,6			
				open	dangerous	30	NA	0,6			
				drift	dangerous	40	NA	0,8			
D1	diode	yes	10	short	dangerous	50	NA	5			
				open	dangerous	50	NA	5			
D2	diode	yes	10	short	dangerous	50	NA	5			
				open	dangerous	50	NA	5			

- Now: determination of λ_{dd} and λ_{du} given a DC

PMU Example Ctd.

Component Reference	Description	safety relevant	λtotal (FIT)	Failure mode	Failure kind	Failure distribution (%)	λs (FIT)	λd (FIT)	DC	λdd (FIT)	λdu (FIT)
R1	resistor	yes	0,05	short	dangerous	10	NA	0,005	0	0	0,005
				open	dangerous	90	NA	0,045	0	0	0,045
R2	resistor	yes	0,05	short	dangerous	10	NA	0,005	0	0	0,005
				open	dangerous	90	NA	0,045	0	0	0,045
C1	capacitor	yes	2	short	dangerous	30	NA	0,6	0	0	0,6
				open	dangerous	30	NA	0,6	0	0	0,6
				drift	dangerous	40	NA	0,8	0	0	0,8
C2	capacitor	yes	2	short	dangerous	30	NA	0,6	0	0	0,6
				open	dangerous	30	NA	0,6	0	0	0,6
				drift	dangerous	40	NA	0,8	0	0	0,8
D1	diode	yes	10	short	dangerous	50	NA	5	0	0	5
				open	dangerous	50	NA	5	0	0	5
D2	diode	yes	10	short	dangerous	50	NA	5	0	0	5
				open	dangerous	50	NA	5	0	0	5

- This was a simple example using passive electronics components only
- Every component has been labeled relevant to safety and the total FIT ratings have been made up – in reality they depend on the mission profile

Complex Components

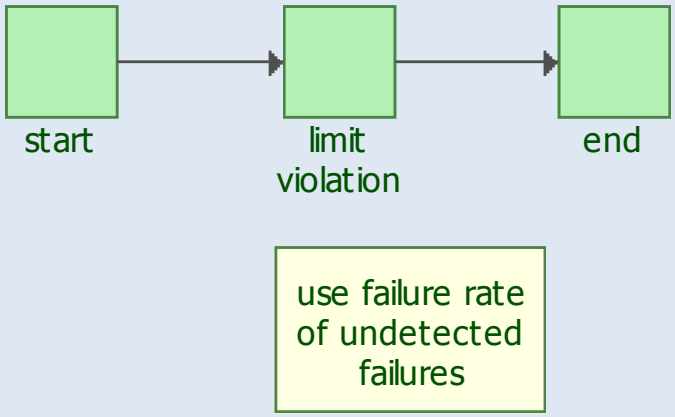
- Complex components (e.g. embedded processors) failure rates are not publically available
- Failure rates need to be determined based on IC vendor information
- If a total failure rate is know the failure rate for a specific functionality can be determined using a transistor count method:

Base FIT	component	% of transistors	component FIT
10000	Flash	50,9	5090
	RAM	30	3000
	ADC	3	300

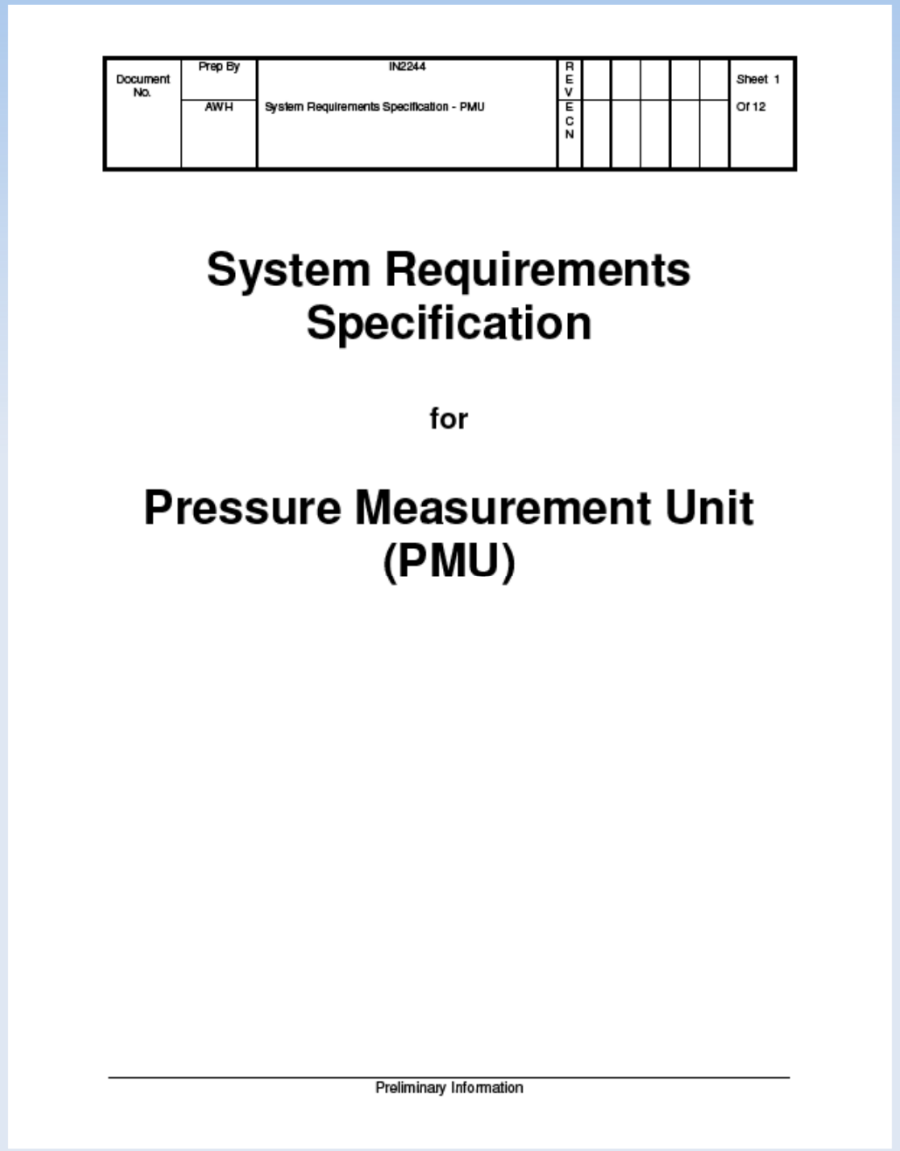
- Not used components do not contribute

Calculating PFD/PFH

- Calculation of PFD/PFH depends on the system architecture (# channels)
- In general this is a complex exercise (depending on the system architecture) which needs the system dangerous failure rates as calculated in the FMEDA (needs to be done for all components)
- PMU (a 1oo1D architecture): PFH = λ_{du}



Meeting the Requirements again
- Watch out for HW Requirements -



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

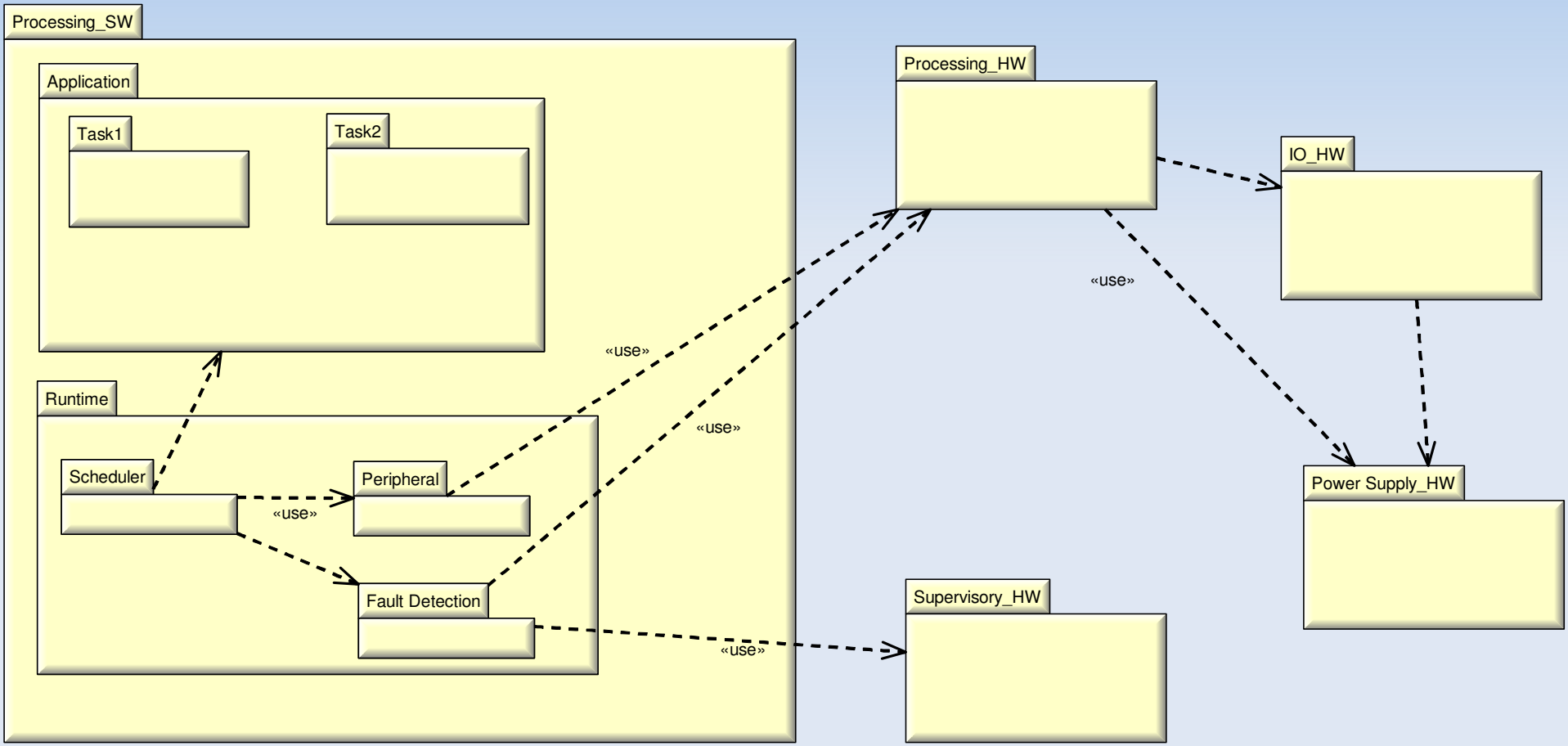
System Requirements Specification

for

Pressure Measurement Unit (PMU)

Preliminary Information

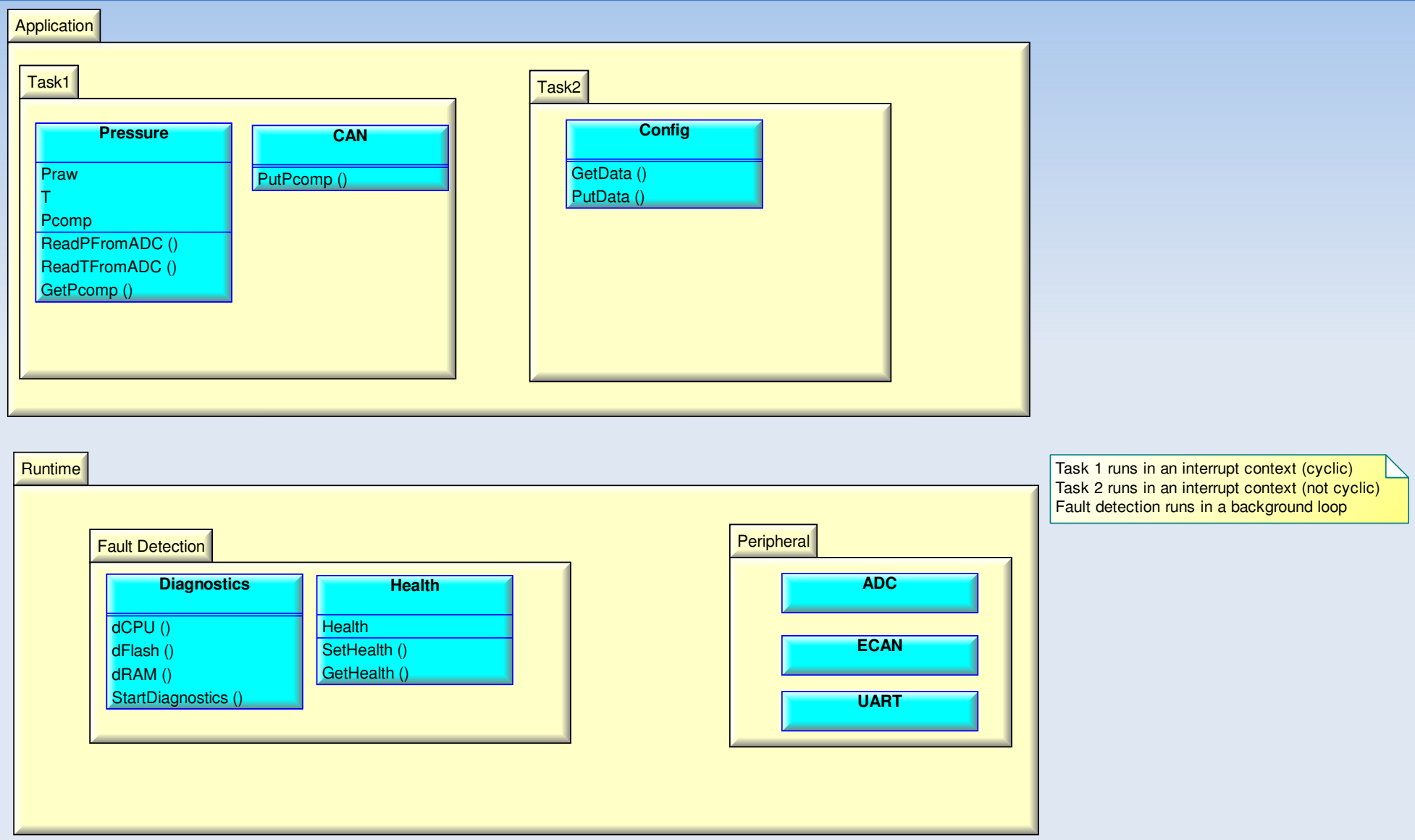
Architecture
- System View (once again)-



Software
- Object List-

- Pressure interface – interface to peripheral ADC
- CAN interface – external request via ECAN peripheral
- Temperature compensation – interface to peripheral ADC
- LED interface for health status – GPIO
- Configuration – RS232
- On-board temperature – peripheral ADC
- Start-up diagnostics – CPU, RAM, Flash, ADC, CAN
- Background diagnostics – CPU, RAM, Flash
- Scheduling

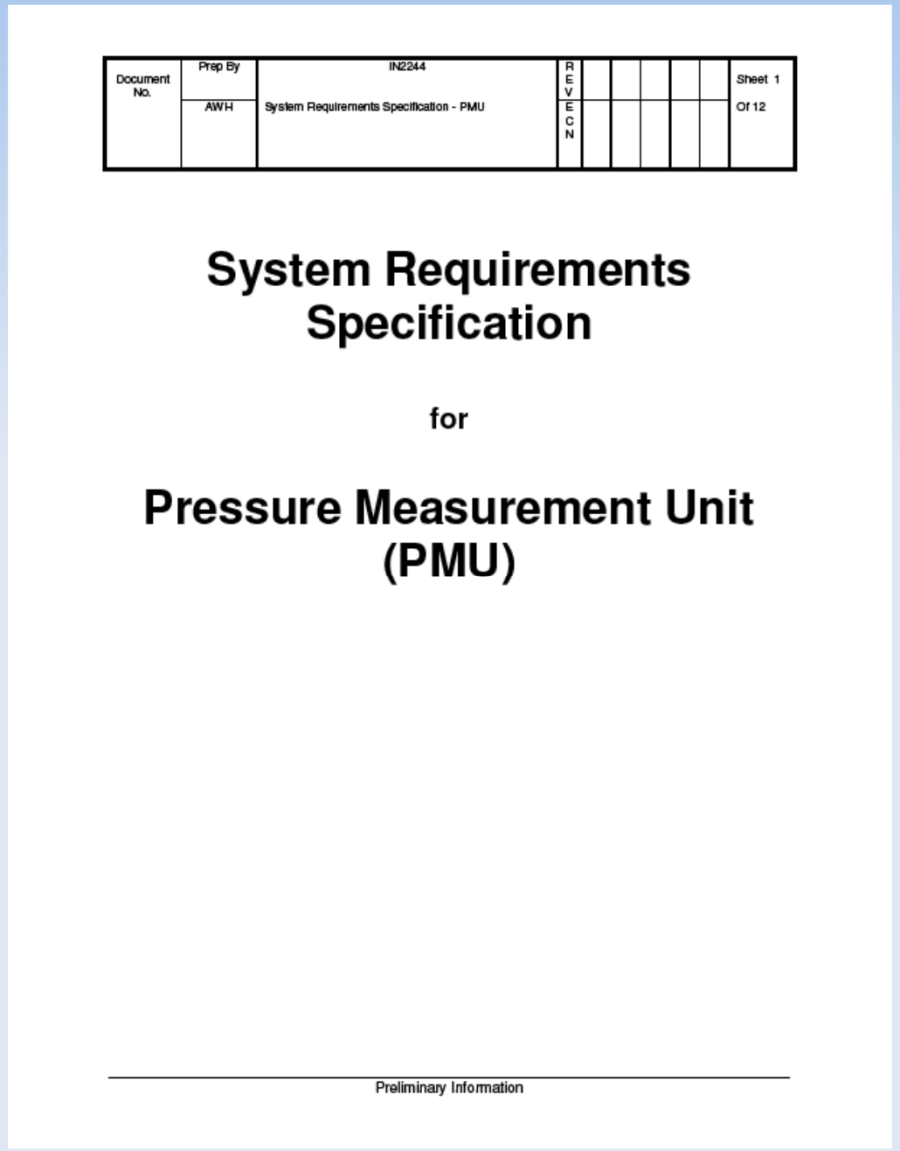
Software Ctd.



Schedulability

- 3 tasks:
  - Interrupt context – no cycle time (C1), response time < 100ns (R1)
  - Interrupt context – 100ms cycle time (C2), response time 10ms (R2)
  - Background context – 3s cycle time (C3), response time 900ms (R3)
  - Independent, static priorities (high, low)
  - Rate Monotonic Scheduling (RMS) – assign priority depending on cycle times (we have done that already without too much thinking)
- Worst case schedulability: $W_n = n \times (2^{1/n} - 1)$
- Always confirm: $\sum_i \frac{R_i}{C_i} \leq n \times (2^{1/n} - 1)$
- Here we get: $0.4 \leq 0.83$

Meeting the Requirements again
- Watch out for SW Requirements -



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

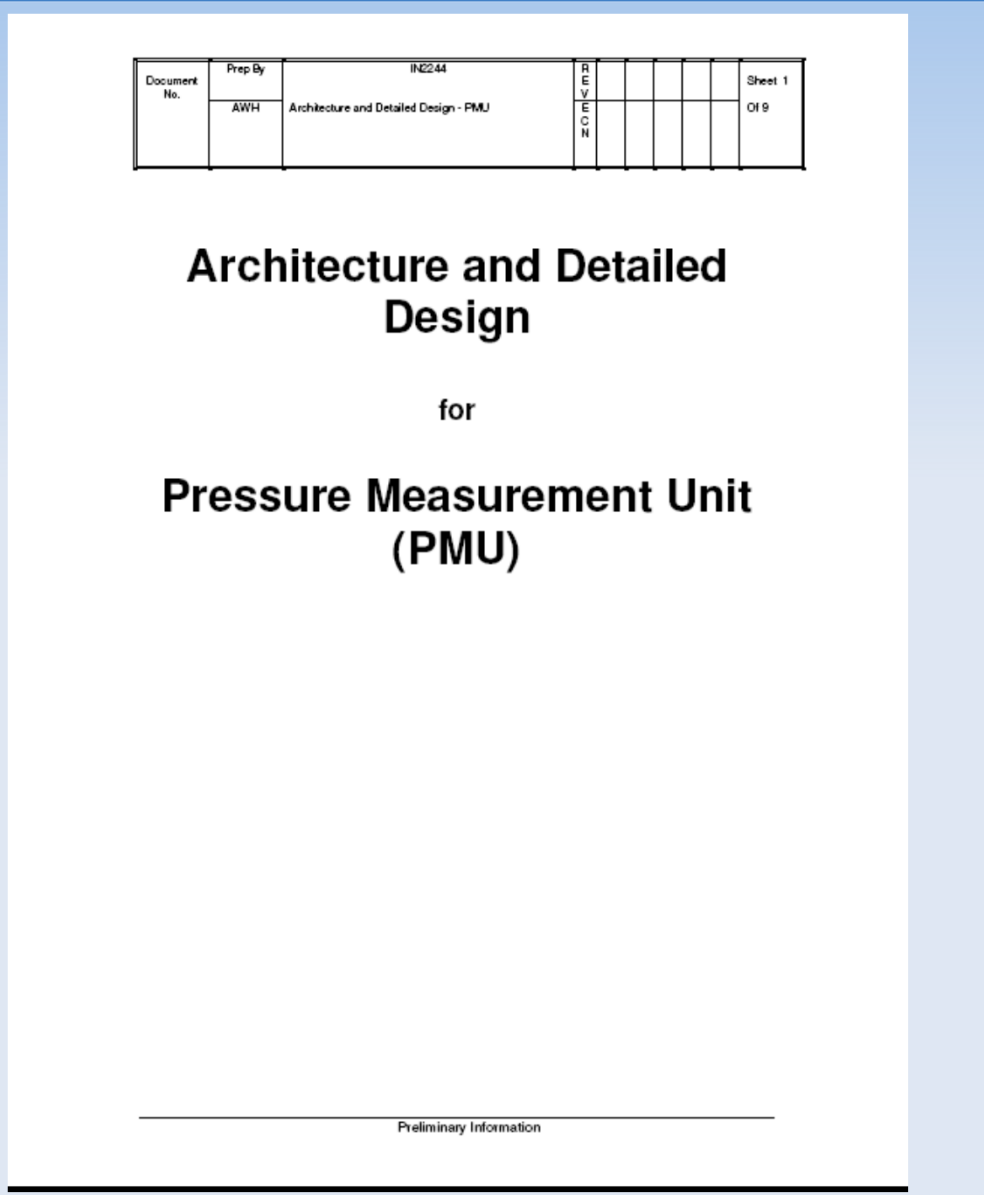
System Requirements Specification

for

Pressure Measurement Unit (PMU)

Preliminary Information

PMU Architecture and Design Description



Document No.	Prep By	IN2244	REVECN	Sheet 1
	AWH	Architecture and Detailed Design - PMU		Of 9

Architecture and Detailed Design

for

Pressure Measurement Unit (PMU)

Preliminary Information

Software Unit (Module) Testing (based on IEC61508-3)

Technique/Measure	Ref	SIL3	Interpretation for PMU
Static analysis	B.6.4 (IEC61508-7) Table B.8 (IEC61508-3)	HR	- automated coding standard compliance tests - design reviews - program not executed
Functional analysis (dynamic/black-box)	B.5.1 (IEC61508-7) B.5.2 (IEC61508-7) Table B.3 (IEC61508-3)	HR	- test against design document - program is executed - boundary value analysis, equivalence classes and input partitioning **Test Environment:** - PMU + test harness (I/O)+ PC software (analysis)
Structural analysis (dynamic/white box)	B.6.5 (IEC61508-7) Table B.2 IEC61508-3)	HR	- Test against design document and code - Boundary value analysis, performance testing equivalence classes and input partitioning (100% branch coverage). **Test Environment:** - Same as functional analysis
Data recording and analysis	C.5.2 (IEC61508-7)	HR	- All testing needs to be documented. Pass/fail criteria need to be in place.

HW/SW Integration (based on IEC61508-3)

Technique/Measure	Ref	SIL3	Interpretation for PMU
Functional analysis (task level + framework)	B.5.1 (IEC61508-7) B.5.2 (IEC61508-7) Table B.3 (IEC61508-3)	HR	**Tests against architecture and design:** - boundary value analysis, equivalence classes and input partitioning (at least one per equivalence class) - Test cases need to cover input, output boundaries and extreme values. Test cases which drive the output to exceed the specification need to be considered **Test Environment:** - PMU + test harness (I/O)+ PC software (analysis)
Data recording and analysis	C.5.2 (IEC61508-7)	HR	- All testing needs to be documented. Pass/fail criteria need to be in place.
Performance testing	C.5.20 (IEC61508-7) Table B.6 (IEC61508-3)	HR	• Avalanche/stress testing - high CAN request load, highest sampling rate • Response timings and memory constraints – analysis of the resource usage and elspsed time for every PMU functionality. • Fault insertion testing

System Testing

Technique/Measure	Ref	SIL3	Interpretation for PMU
Simulation/modelling	Table B.5 (IEC61508-3)	HR	Comparison of simulated and real readings.
Functional and non-function testing against requiremnents (real IO, real environment)	B.5.1 (IEC61508-7) B.5.2 (IEC61508-7) Table B.3 (IEC61508-3)	HR	**Test against requirements:** - boundary value analysis, equivalence classes and input partitioning **Test Environment:** - PMU + pressure sensor + PC software (CAN master)