Industrial Embedded Systems
- Design for Harsh Environment -

Dr. Alexander Walsch
alexander.walsch@ge.com

WS 2011/12

Technical University Munich (TUM)

Introduction - Our Backgrounds

- O&G
- Energy
- Sensor systems
- Aviation
- Automation

Source: GE O&G

Outline

Part I: Terms and Definitions

- Small footprint systems
- Design for harsh environments
- Real-time systems
- High-integrity systems

Part II: Development

- Project Acquisition & Planning
- Requirements Analysis - functional and non-functional
- Hardware and Software Architecture
- Special Components (e.g. System on Chips, reconfigurable ICs, operating systems)
- Detailed Design
- Realization

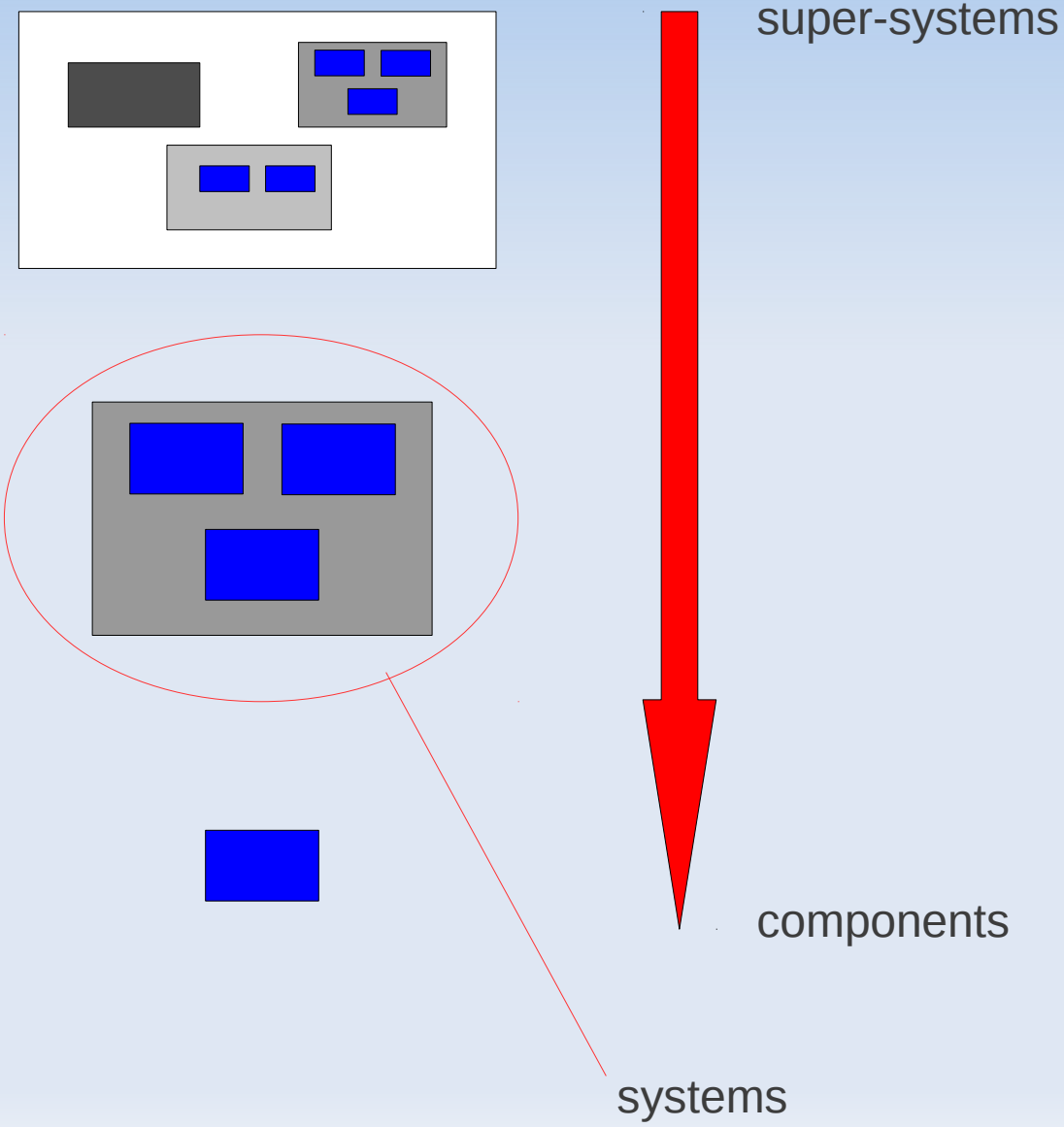
Part III: Verification & Validation

- Tools
- White box and black box testing
- Module, integration, and system testing
- System validation
- Operation and maintenance

Part I: Terms and Definitions

Small Footprint Systems
Design for Harsh Environment

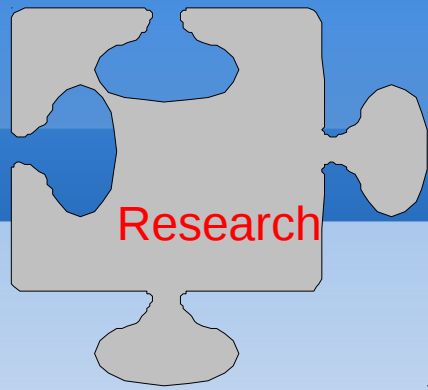
Systems



- Components (boards e.g.)
- Systems (boxes e.g.)
- Super-systems (a bunch of boxes e.g.)

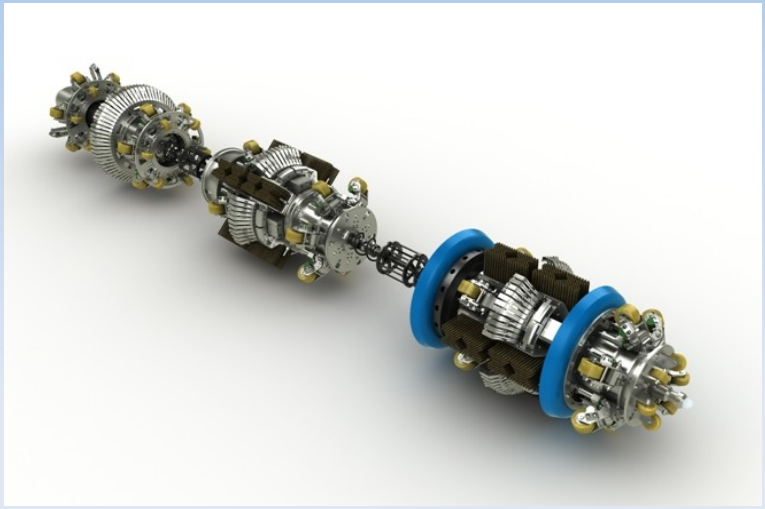
  What is the system border?
  What is the functionality?
  What are the quality considerations?

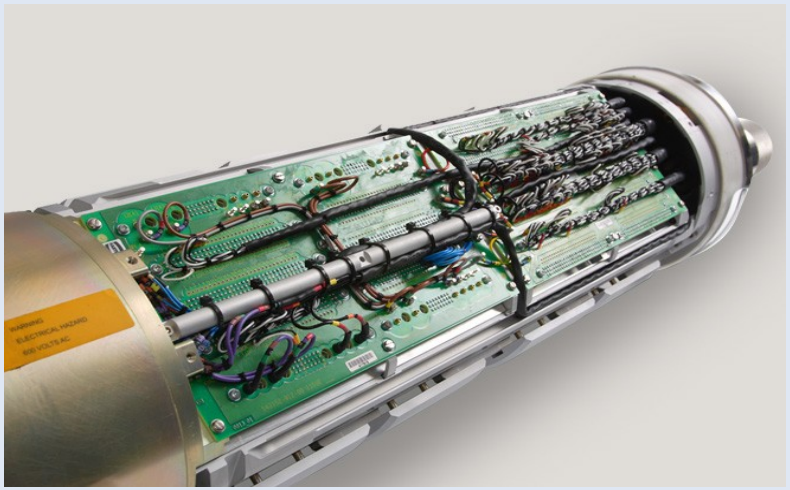
System Modeling



- Embedded systems are part of more and more complex electrical systems – team members with very different background.
- Need for Modeling at system level (requirements, interoperability, team communication).
- SysML, UML widely used as notation but disadvantages: timing, no formality, non-functional requirements hard to describe
- Hot topics: Model-based design, automated design flows

Small Footprint System





- Limited resource (size, power, memory, CPU)
- A hidden technology (no-one cares if it works everyone screams if it fails)

Source: GE O&G

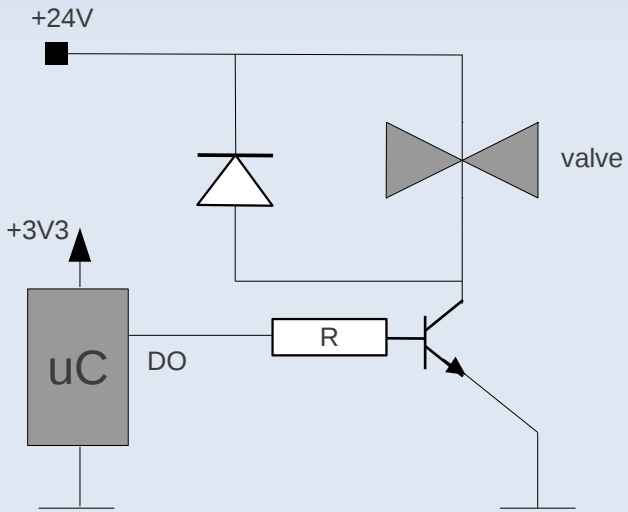
System Classification

- Control systems – open loop/closed loop
- Monitoring systems – monitoring and diagnostics
- Protection systems – safety functions
- Combination of the above

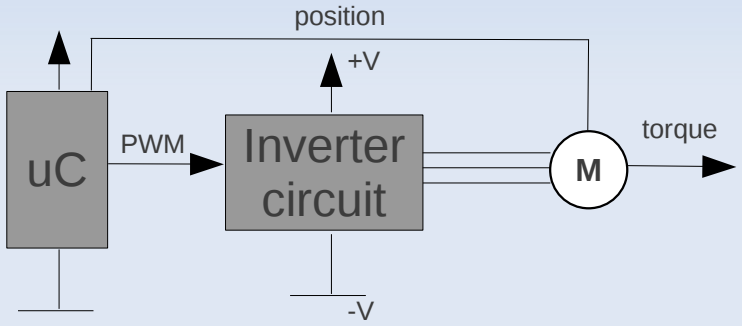
Control Systems

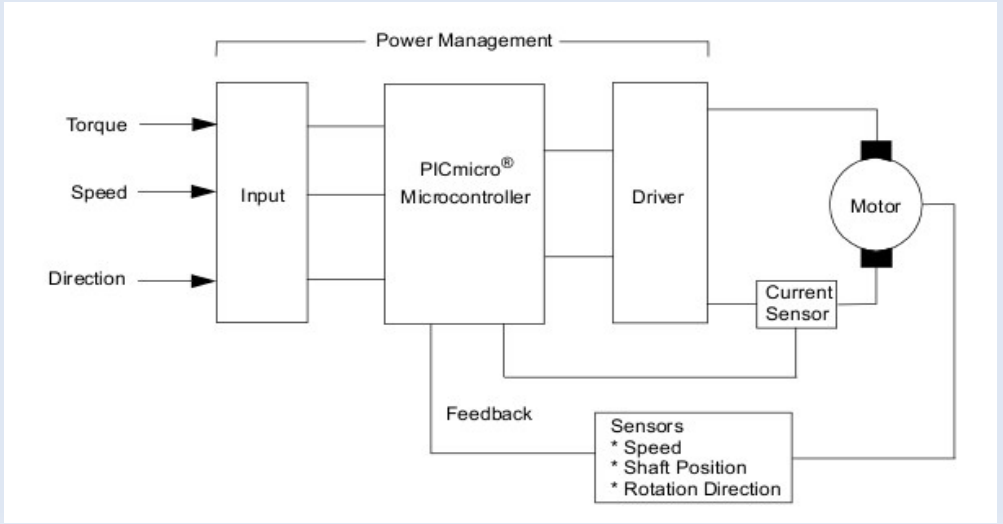
Control systems – open loop and closed loop

open loop: solenoid valve



closed loop: BLDC motor

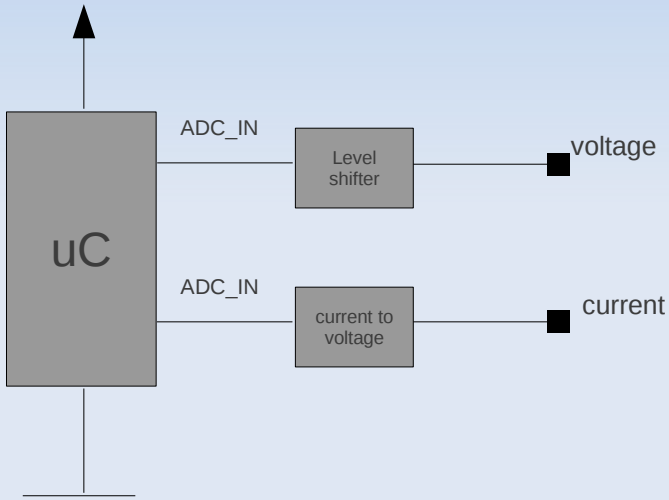




Source: Microchip AN894

Monitoring Systems

Monitoring systems – monitoring and diagnostics

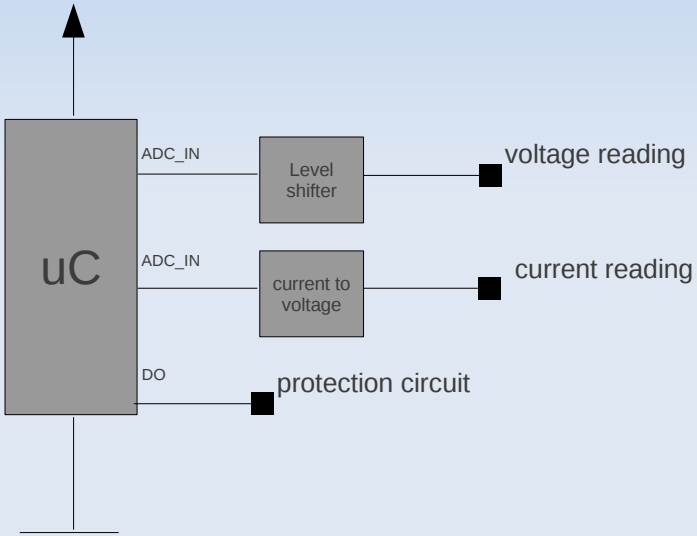


- Temperature
- Humidity
- Pressure
- Currents
- Voltages

Monitoring systems are used to collect system data (on-board, off-board) for online or offline diagnostics (RM&D, CBM). System data might be stored for later analysis in case of remote systems (”flight recorder”).

Protection Systems

Protection systems – safety functions



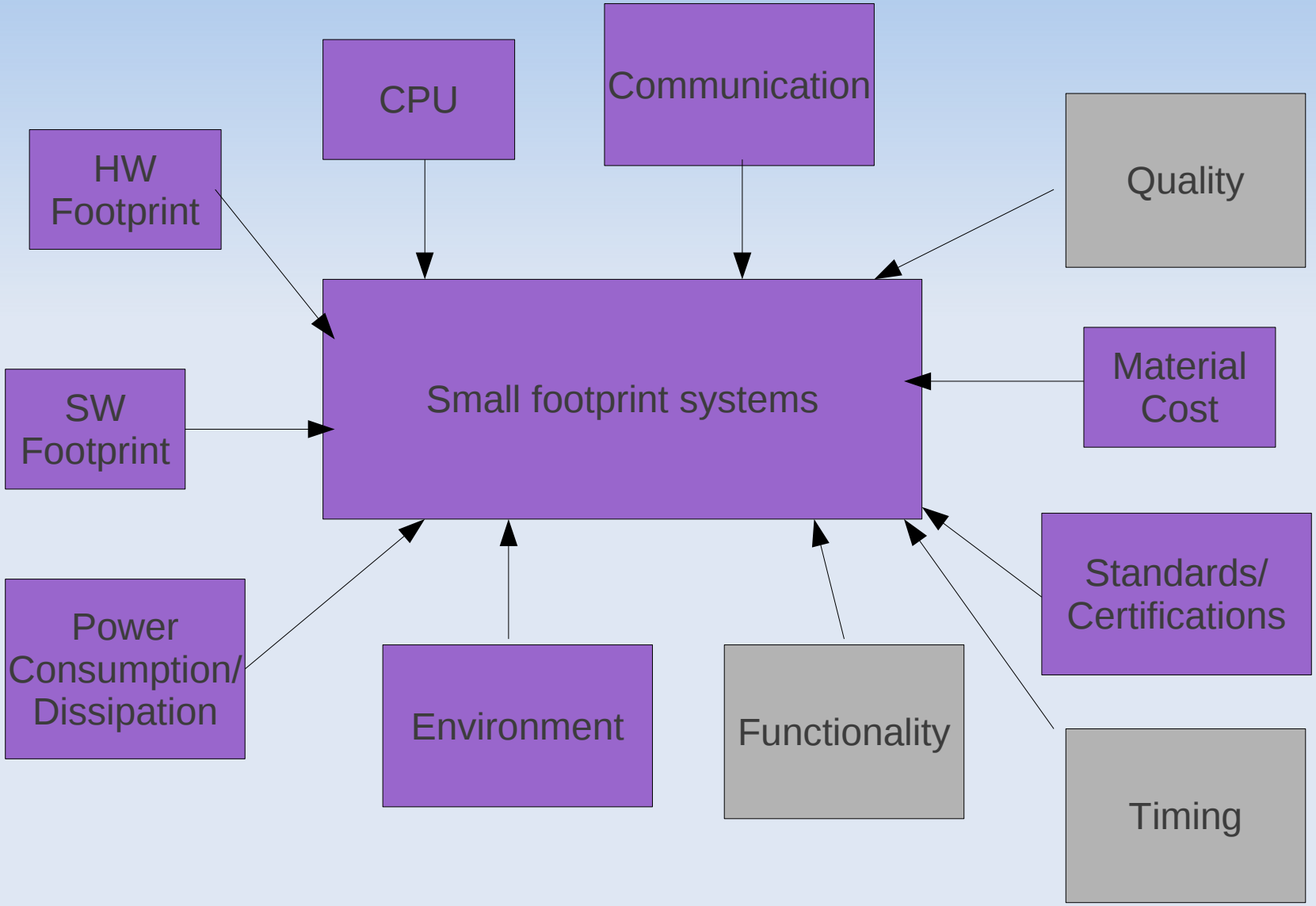
Source: VW

Protection systems have the sole purpose to put the system into a safe state upon fault detection. The safe state needs to be maintained until a clearance operation has been carried out (e.g. safety chains).

System Requirements

- Functionality – what is the system doing?
- Timing – timely execution, scalability?
- Cost – material cost (HW/SW partitioning)?
- How much power is consumed?
- Hardware size – form factor?
- Software size?
- Are there regulations?
- Where is it used – extreme conditions?
- Quality/Standards?

System Requirements - Putting it all together



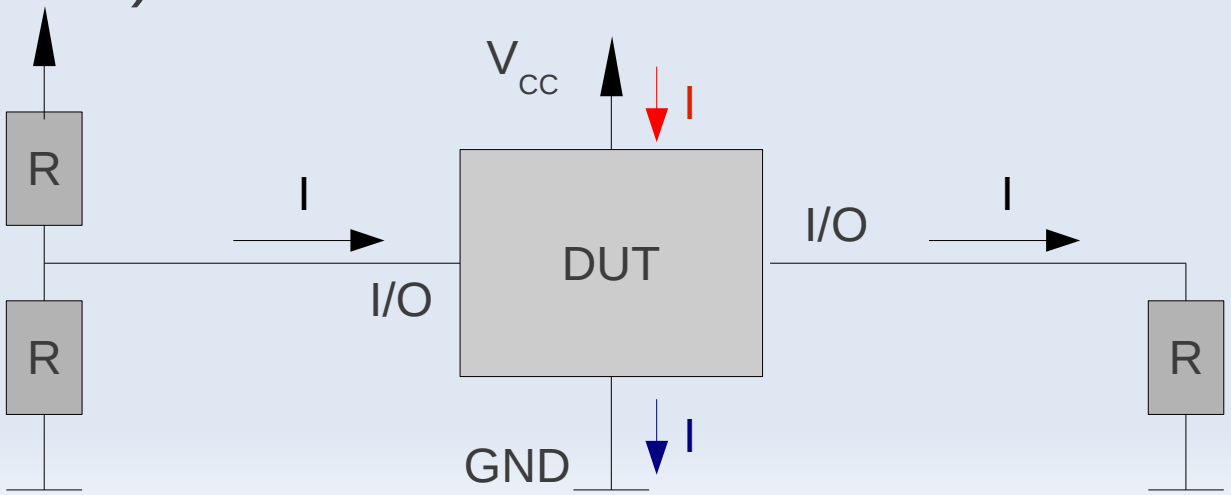
Material Cost

- Hardware cost:
  - Bill of material (BOM)
  - Board manufacturing, population
- Software cost
  - Royalties (e.g. for an OS)

Power Consumption and Dissipation

Model for power consumption

- Logic consumption – DUT (analog, digital)
  - Power dissipated by electronics (static, dynamic).
- I/O consumption (discrete I/O, data transmission)
  - Power to drive external loads (DUT and remote power consumption, DUT and remote power dissipation).
  - Power that is sunk (DUT power consumption and dissipation).



HW Footprint

- Requirement on hardware components.
  - Functionality must be mapped on available space.
  - Especially conduction cooled systems put strict requirements on component size and its physical integration.
- Standardized form factors available – highly depends on industry

SW Footprint

- Parameter memory (non volatile)
  - EEPROM – byte wise read and write – holds e.g. configuration parameters, run-time parameters (hour meter, status)
- Program memory (non volatile)
  - Flash (NOR)– word wise read, write requires a block erase - holds executable (XIP – execute in place)
- Data memory (volatile)
  - RAM (SRAM) – word wise read and write addressable - holds data and stack

Standards and Certifications

Important domain specific standards:

- Automotive: ISO CD 26262 – Automotive Safety Integrity Level (ASIL)
- Aviation: DO178/DO254 – Design Assurance Level (DAL)
- Healthcare: IEC 62304
- Rail: EN 50126/50128/50129 – Safety Integrity Level (SIL)
- General/Industrial: IEC61508 – Safety Integrity Level (SIL)

Environmental

- Important environmental constraints:
  - Temperature (e.g. -40 to +85 °C)
  - Electromagnetic compatibility – EMC (conductive, inductive, capacitive, radiative coupling)
  - Shock (e.g. 2000 g)
  - Vibration (displacement, velocity, acceleration)
  - More exotic once (rad hard etc.)

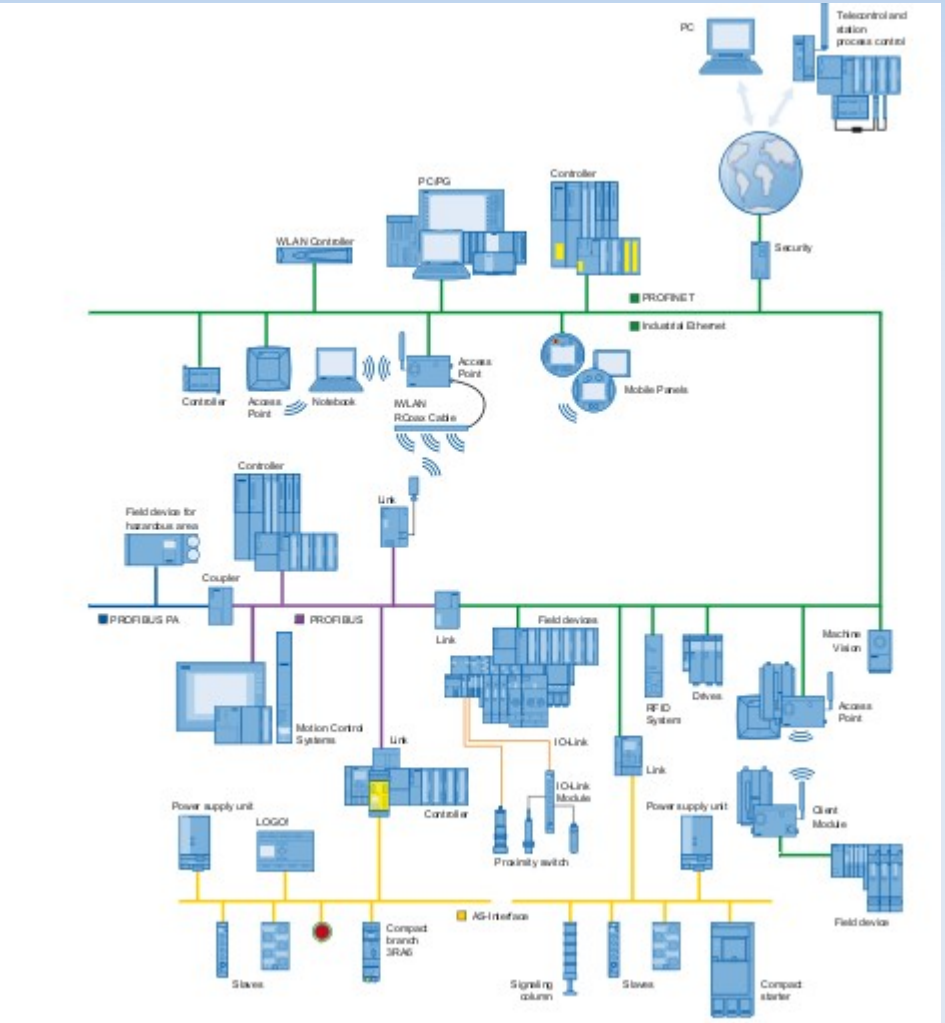
CPU

- Often the CPU is not a free choice:
  - Prior usage
  - Tools already available
  - Long term availability or scalability (CPU roadmap)
  - Communication interfaces in package
  - Multiple suppliers (e.g. IP cores like ARM/MIPS)
  - Legacy code

Communication

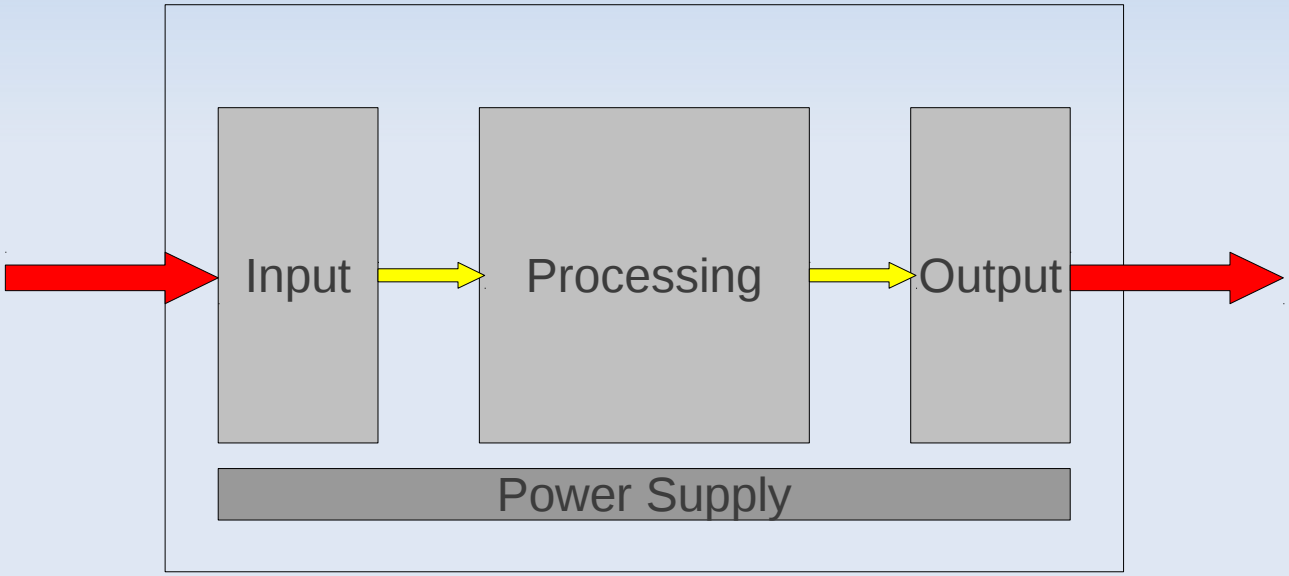
Communication depends on:

- Integration, a requirement which results from system level requirements



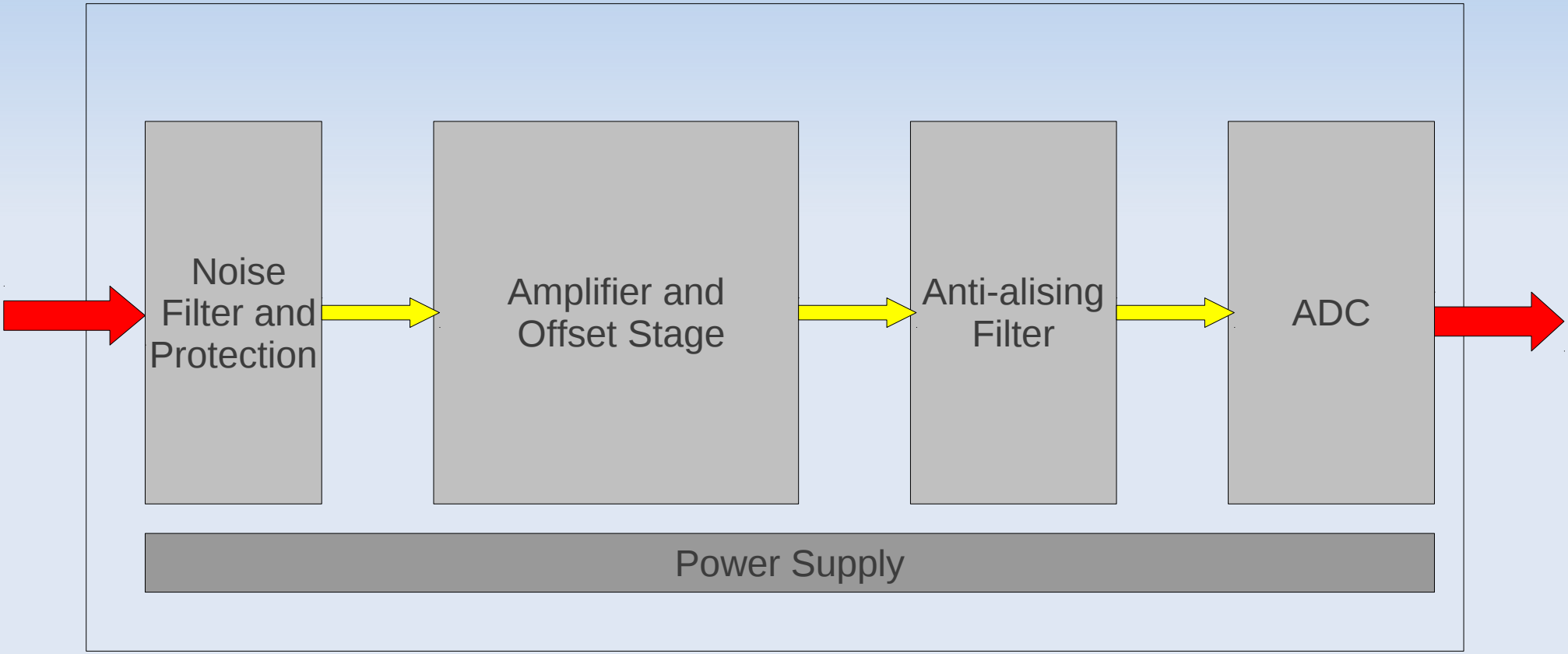
Source: Siemens
Simatic Net
Profibus Network Manual

System Components



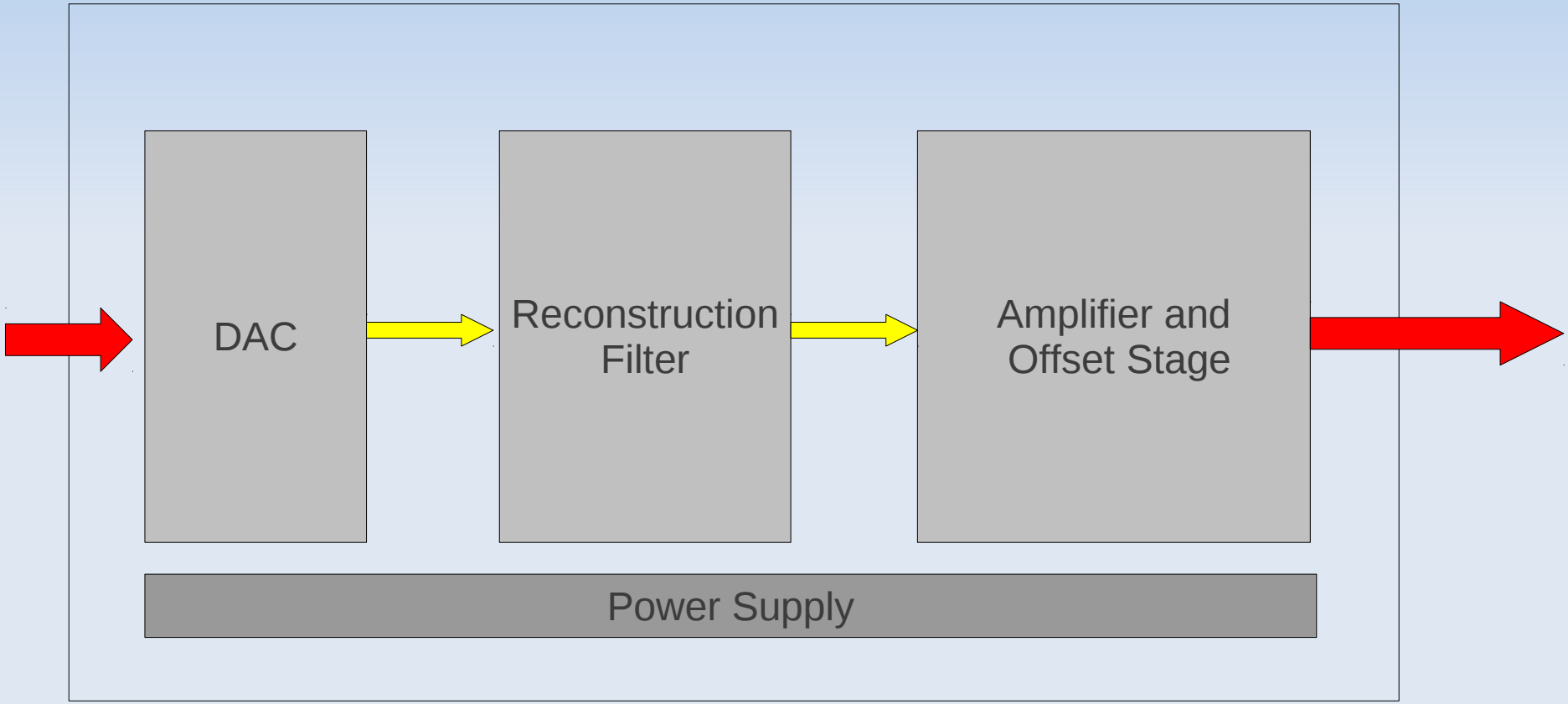
- Electro-mechanical view
- Input
- Processing
- Output
- Power Supply

Components – Analog Input

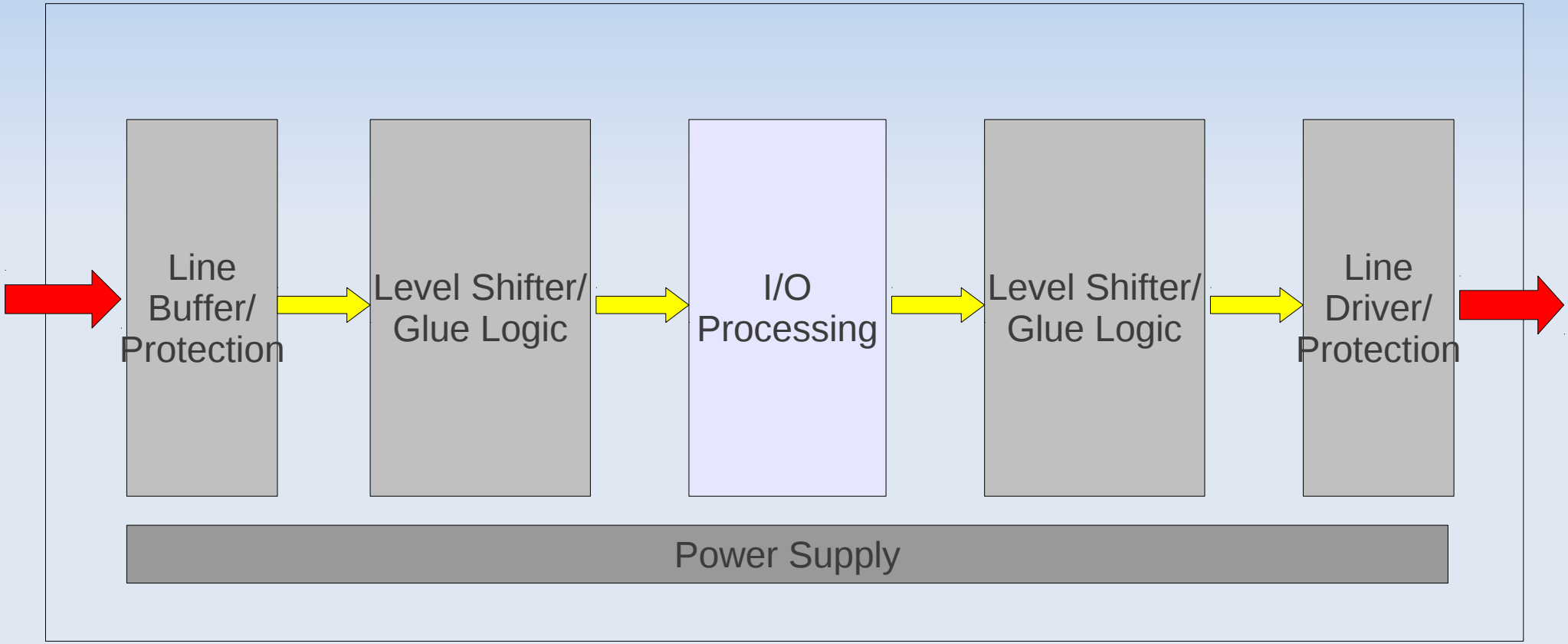


Nyquist frequency $f_N = 0.5 \times f_S$; f_N is the highest frequency component that must be present at the ADC input → proper reconstruction

Components – Analog Output

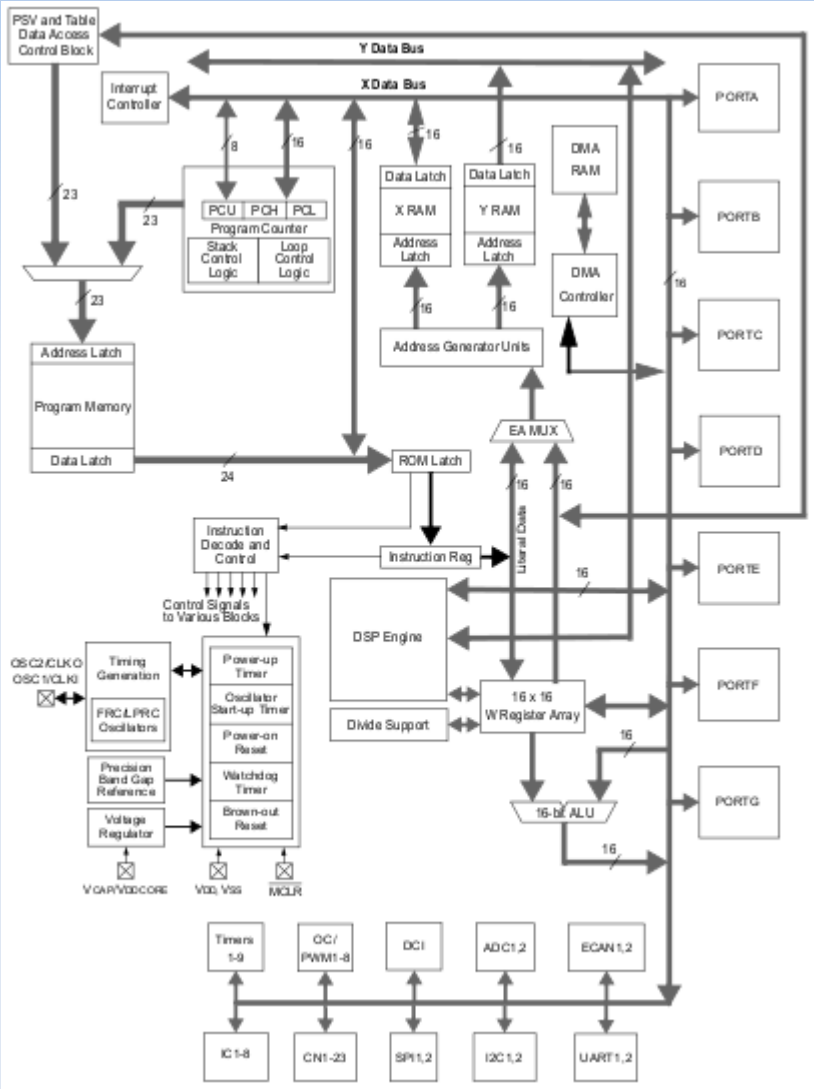


Components – Digital Input/Output



Protective circuits can contain both transient, over/under-voltage protection and galvanic isolation.

Components – Processing



- Example: dsPIC33FJXXXGPX06
- Digital Signal Controller (DSC)
- Modified Harvard architecture
- Flash and SRAM
- On-die peripherals

Source: Microchip DS70286C

Example System - PMU

- PMU: Pressure Measurement Unit
- Will be used as an example virtual technology development
- Measures pressure, temperature compensation, inexpensive, CAN interface

- COTS single board small form factor
- I/O interfaces
- Networking
- Limited memory
- Vendor specific design tools

PMU - Requirements

- Material cost < $50
- Power consumption < 2 W
- Physical size 50 x 25 x 10 mm
- Standard/Certification: IEC61508
- Operating temperature -40 °C to +85 °C
- PIC uC
- Communication: temperature sensor, pressure sensor, CAN backend

PMU – Requirements on Software

- Timely monitoring of pressure and temperature – soft real-time
- Sense faults with a very high confidence (external, board level, processor) – hard real-time

Outlook

- Real-time systems
- High integrity systems