Belle II: PS Module firmware
Intended design and work plan

Bonn, Feb. 08, 2011

Agenda

- Introduction

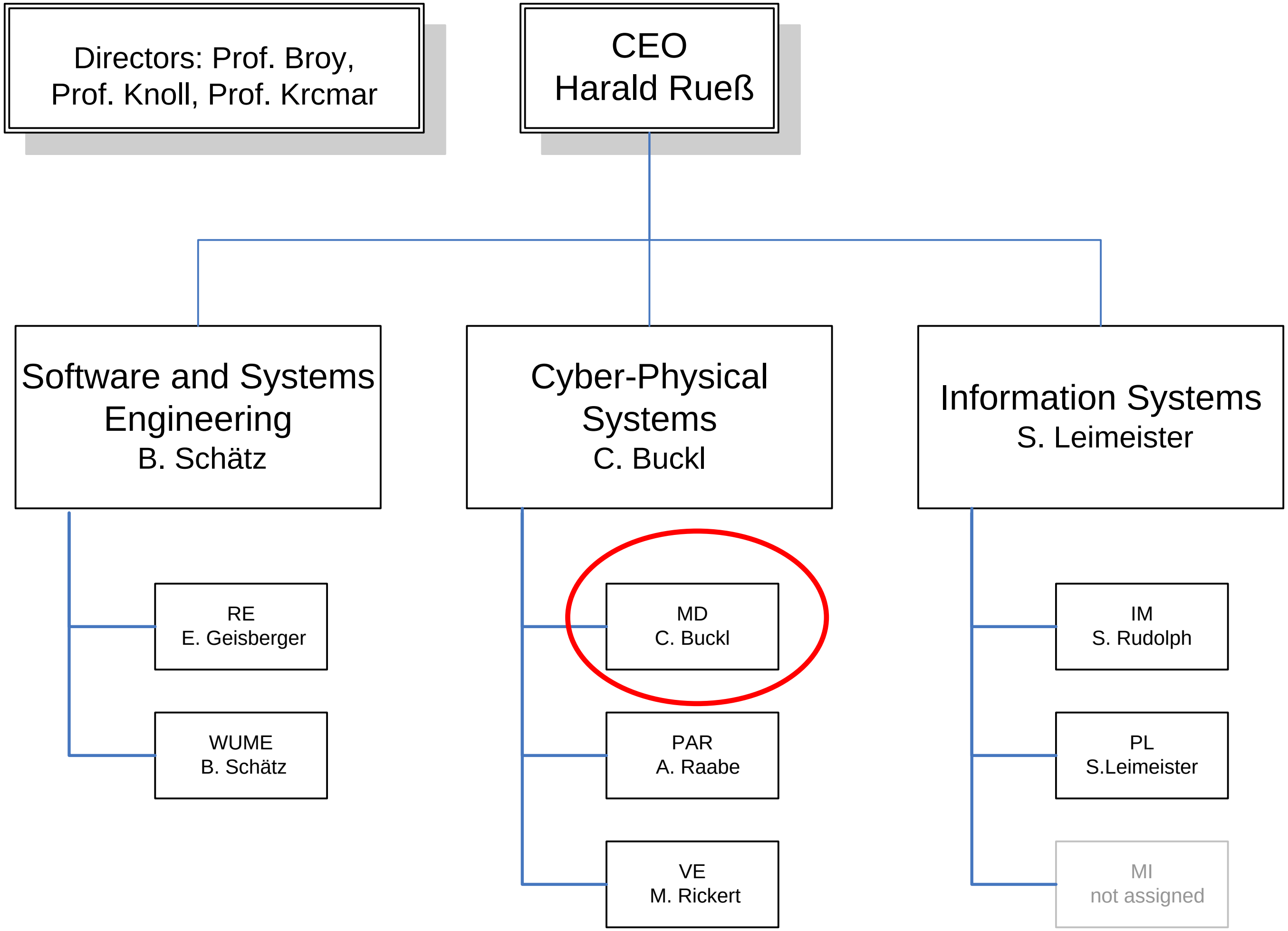
- Contribution of Fortiss to Belle II project
- Planned schedule
- Safety engineering

- Conclusion

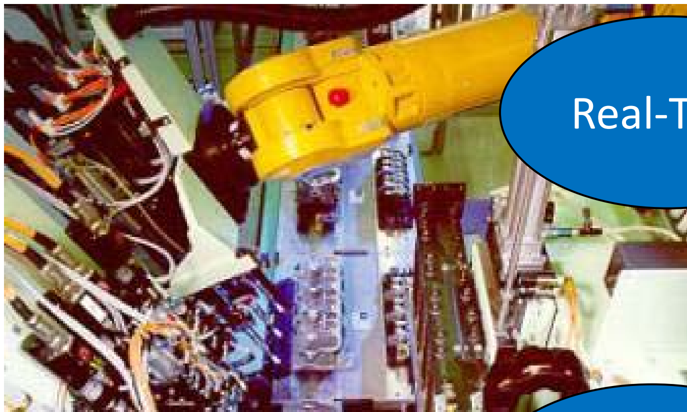
fortiss – Innovation in Software and Systems

- Spin-Off of TU München
- Non-profit research organization
- Proprietors
  - Technische Universität München
  - LfA, Förderbank Bayern
  - Fraunhofer Gesellschaft
- Funded by *Bayerisches Staatsministerium fuer Wirtschaft, Infrastruktur, Verkehr und Technologie* (January 2009)
- Goal
  - Close the gap between industry and academia
    - Transfer of know-how to industry
    - Transfer of research questions to academia
  - Incubator for start ups

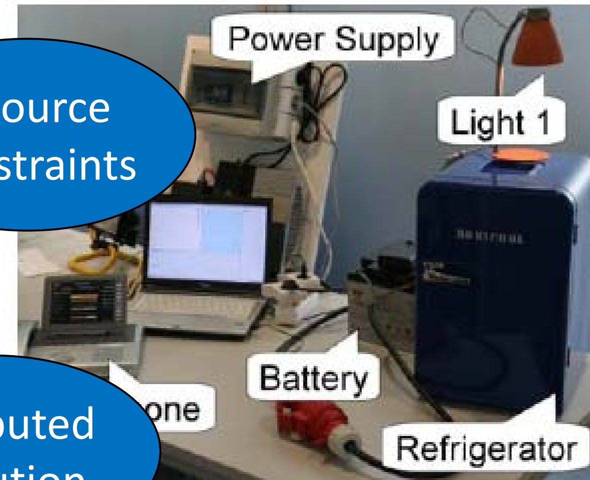
fortiss – Organization



CPS group: Application Area and Focus



Industrial Automa



tion / eEnergy

Real-Time

Resource Constraints

Reliability & Safety

Distributed Execution

Energy Efficiency

Transportation / eCar

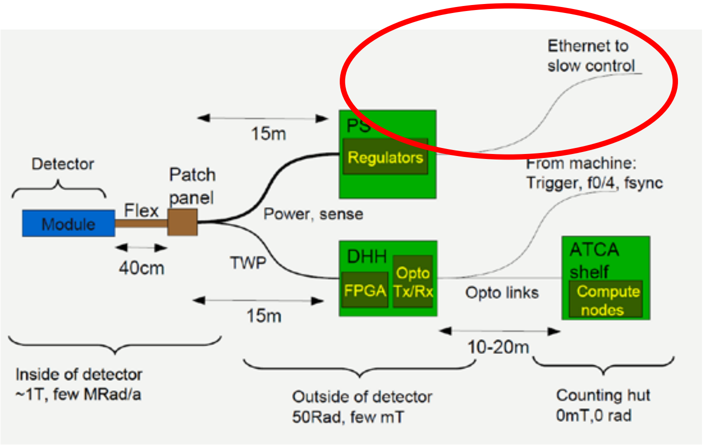
fortiss innovation in software and systems

Dept. of Informatics, TU München VI – Robotics and Embedded Systems

- Informatik VI – Robotics and Embedded Systems :
  - » **A. Knoll** Professor
  - » **D. Burschka** Associate Professor „Service Robotics“, with DLR
  - » **G. Hirzinger** Honorary Professor
  - » **G. Schrott** Academic Director
- Main research directions
  - » **Sensor based service and medical robotics**
  - » **Cognitive robotics & man-machine-dialogue-systems**
  - » **Embedded real time systems**
- Teaching
  - » Undergraduate: Informatik I & II (Introduction to computer science)
  - » Graduate: robotics, sensor systems, real-time systems, digital signal processing, machine learning I & II, autonomous systems

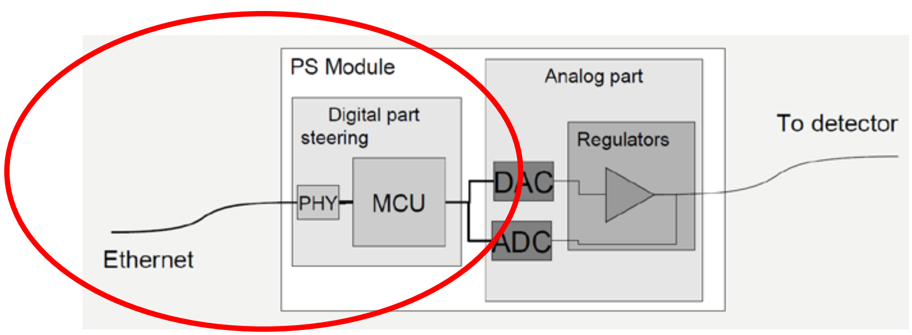
Contribution of Fortiss to Belle II project

- Sub-contractor of LMU, Excellence Cluster Universe
  - Phase 1: Design and implementation of software for power supply modules
  - Phase 2: Support

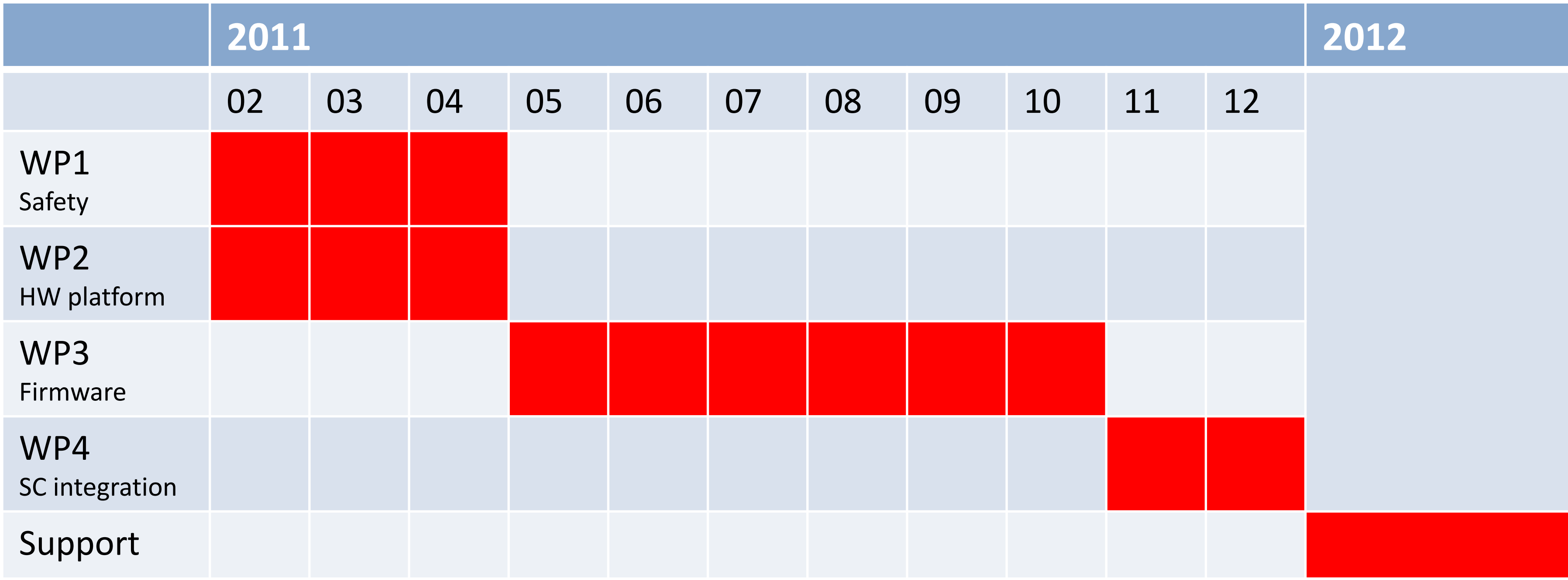


- Phase 1: Work packages
  - WP1: Development of safety concept
  - WP2: Consulting services to LMU w.r.t. hardware platform
  - WP3: Firmware development
  - WP4: Integration to slow-control

- Phase 2:
  - Bug fixes
  - Minor adaptations



Planned schedule



- Next steps
  - Consulting services
    - Selection of hardware platform (Feb. 2011)
    - Definition of fault hypothesis (Feb. 2011)
  - Specification of firmware and interface to slow control (Mar. 2011)

Safety Engineering

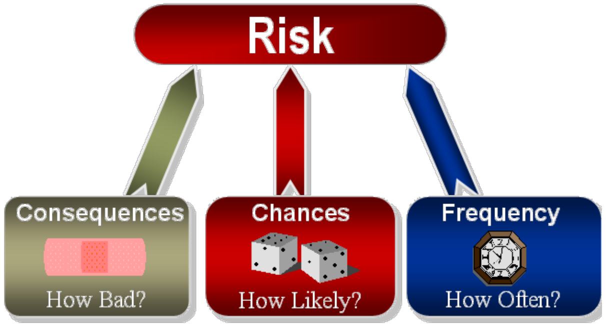
1. Identification of safety requirements:
   - Typically not: „*the system must output always a correct value*“, but „*erroneous outputs must be corrected within 1 ms*“
2. Identification of faults:
   - What can go wrong in the system → *fault hypothesis*
3. Which hazards can lead to a violation of safety requirements:
   - Analysis using Fault-Tree Analysis (FTA) and/or Failure Mode and Effect Analysis (FMEA)
4. Selection of appropriate system design including fault-tolerance mechanisms
   - Identification of minimal cut sets leading to violation of safety requirements (*top-level undesired event*)
   - Check whether minimal cut sets are within fault hypothesis
   - Yes: introduction of fault-tolerance mechanisms
   - No: design is okay

Safety Engineering – Important terms

- „*An **error** is a manifestation of a **fault** in a system, which could lead to system **failure**.*“ [Singhal/Shivaratri]
  - Fault – undesired state which can lead to an error
  - Error – system state which is not part of the specification
  - Failure – System can no longer provide its service(s)

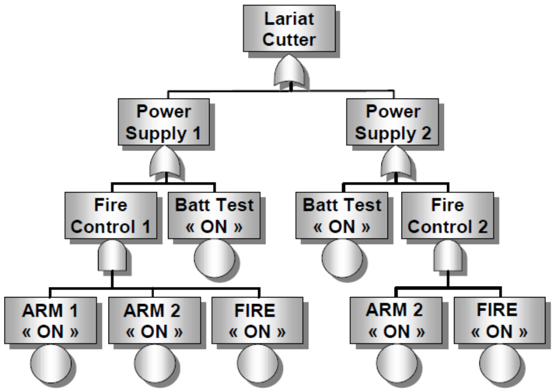
- Risk management
  - Hazard: Situation, that poses a level of thread to life, health, property, or environment
  - Risk = Likelihood of occurrence x seriousness if incident occurred

- Three key techniques
  - Hazard and Operability Study (HAZOP)
  - Fault Tree Analysis (FTA)
  - Failure Modes and Effects Analysis (FMEA)



Fault-tree analysis (FTA)

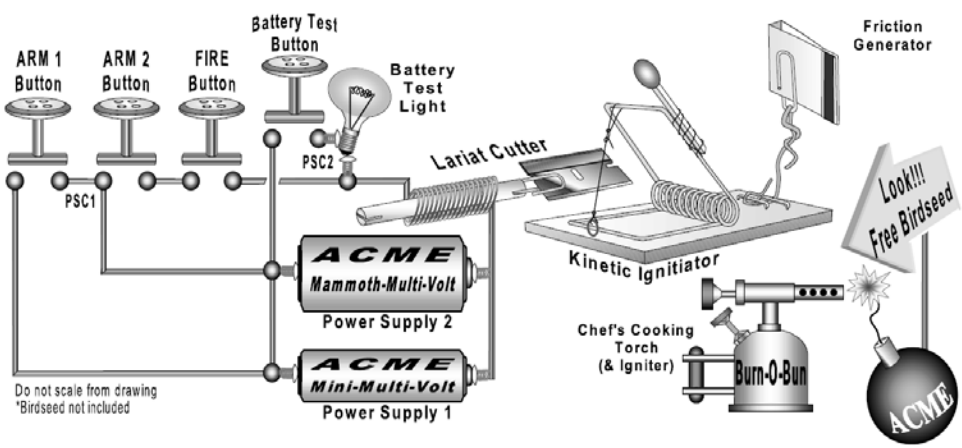
- FTA
  - Deductive, **top-down** method
  - Analyze effects of initiating faults and events on a complex system
  - **„User perspective“**



- Origin
  - 1962: Developed in by U.S. Airforce (H.A. Watson)
  - Later adopted by other domains (civil aircraft, nuclear power industry, NASA, military)

- Standards
  - NUREG-0492: NRC Fault Tree Handbook
  - SAE ARP4761
  - MIL–HDBK–338
  - IEC / EN 61025

- Approach
  1. Define the undesired event to study
  2. Obtain an understanding of the system
  3. Construct the fault tree
  4. Evaluate the fault tree
  5. Control the hazards identified



[A. Long 2003]

Failure Mode and Effects Analysis (FMEA)

- FMEA
  - Supplement FTA: "*Bottom-up*" use of FMEA to identify many more causes and failure modes resulting in top-level undesired events.
  - Restriction: Not able to discover complex failure modes involving multiple failures within a subsystem.
  - **"Platform perspective"**
- Origin
  - 1940ies: by US Armed forces
  - 1960ies: Apollo program
  - 1970ies: Introduced to automotive industry

Function	Failure mode	Effects	S (severity rating)	Cause(s)	O (occurrence rating)	Current controls	D (detection rating)	CRIT (critical characteristic	RPN (risk priority number)	Recommended actions	Responsibility and target completion date	Action taken
Fill tub	High level sensor never trips	Liquid spills on customer floor	8	level sensor failed level sensor disconnected	2	Fill timeout based on time to fill to low level sensor	5	N	80	Perform cost analysis of adding additional sensor halfway between low and high level sensors	Jane Doe 10-Oct-2010	

Source: Wikipedia

- Preparation
  - Analyze robustness of system integration
  - Describe system and its function
  - Create block diagram of system → logical relation of system components
  - Create worksheet collecting important information of system → List system functions (based on block diagram)
- Approach
  - Severity
    - Determine failure modes based on functional requirements and their effects
    - Failure modes can propagate
    - Failure effect: Result of failure mode as perceived by user
    - Assign severity number (SN, 1 = no danger, 10 = critical)
  - Occurrence:
    - Look at cause of failure mode and rate its frequency (occurrence ranking: 1-10)
    - Failure cause is considered as design weakness
    - High occurrence (> 4 for non-safety failure modes, >1, if SN >= 9): Determine action
  - Detection: Test efficiency of actions

Conclusion

- Design and implementation of
  - PS module firmware
  - Interface to slow-control

- Safety engineering for PS system
  - All relevant parts of the system must be considered (HW, SW)
  - FTA
  - FMEA

- Next steps
  - Requirements analysis
  - Consulting services for selection of hardware platform
  - System specification

Contact

Dipl.-Inf. Simon Barner
barner@fortiss.org

Dr. Christian Buckl
buckl@fortiss.org

Prof. Alois Knoll
knoll@in.tum.de

fortiss GmbH
Guerickestr. 25
80805 München