Critical Embedded Systems

Horváth Ákos, Majzik István, Bartha Tamás, Farkas Rebeka

ahorvath@mit.bme.hu

bartha@mail.bme.hu

Fault Tolerant Systems Research Group

- Department of Measurement and Information Systems
  - Approx. 70 employees, 35 PhD students
  - Embedded Systems
  - Intelligent Systems
  - **Fault Tolerant Systems (FTSRG) – 24 person**
- Software engineer, electrical engineer, medical engineer
- Basic courses (software engineering)
  - Digital systems
  - Operating systems
  - Artificial intelligence
  - Embedded systems
  - Formal methods
  - Measurement laboratory
- Specialization (software engineering)
  - Integrated intelligent systems (BSc)
  - Systems design (BSc)

Fault Tolerant Systems Research Group

- Lectures
  - Ákos Horváth
  - Tamás Bartha
  - Rebeka Farkas
  - + invited speaker
  - (István Majzik)
- Labs:
  - Rebeka Farkas

Course structure

- Basics of Safety
  - Definitions
  - Requirements
- Techniques for verification and validation of safety
  - Formal methods
  - Hazard analysis
- Nuclear I&C safety and its requirements
  - Techniques, requirements and architectures
- Case studies
  - Avionics
  - Railway
  - Nuclear

Planned course schedule

Semester week	Lecture date	Topic
1	2020.09.09.	Course requirements, schedule, short overview
2	2020.09.16.	Safety-critical systems: introduction, basics
3	2020.09.23.	Sports day
4	2020.09.30.	
5	2020.10.07.	Safety-critical systems: 1st consultation
6	2020.10.14.	Reliability analysis (fault-tree analysis) practice
7	2020.10.21.	
8	2020.10.28.	Safety-critical systems: 2nd consultation
9	2020.11.04.	Nuclear I&C safety: introduction, basic terms, overview
10	2020.11.11.	Formal methods (UPPAAL) practice
11	2020.11.18.	
12	2020.11.25.	
13	2020.12.02.	Nuclear I&C safety: consultation
14	2020.12.09.	Student presentations (homework final step)

Requirements

- „Self-processing of a relevant topic”
  - Reading, understanding, and summarizing a scientific paper on safety
    - Presentation in 12+3 minutes
  - Guidelines
    - Relevant to the course
    - You can provide your own selected publications or select from our list
    - **(handout** ~8. week, **submission:** 11. week)
- Homework
  - Application of formal methods for safety critical design
  - Handout: ~6th week, submission: 11 week.
- Oral exam
  - HW has a significant impact on the final grade (50%)
  - Extra assignments can be done during the semester for extra points
  - Materials: mainly the slides

Contact

- Homepage
  - Course material
  - https://inf.mit.bme.hu/edu/courses/kbr
    - May try out the Teams group for sharing the materials
- Class:
  - We will have consultation sessions related to the hand-out topics
    - Wednesday, ~~I.L. 405~~, 10:15-12:00
    - Check the Teams Calendar

First group of topics: Safety in Design

- Safety Basics, Architectures and Hazard Analysis
  - Safety-critical systems: Basic definitions
    - Hazard, risk and safety
    - Safety integrity, Safety requirements
    - Dependability attributes, Threats to dependability
    - Means to improve dependability
  - Design of the architecture of safety-critical systems
    - Typical architectures for fault-tolerant systems
  - Hazard Analysis
    - Evaluation and estimation of reliability attributes

Second group of topics: Nuclear I&C Safety

- Nuclear Safety Basics
  - Introduction to Nuclear Safety
    - Nuclear power generation, inherent security, feedback
    - Comparison of Functional Safety (61508) and Nuclear Safety
    - Postulated initial events (PIE), design basis
    - Nuclear incidents, accidents - INES scale
- Nuclear Power Plant Safety Basics
  - Construction Principles and Safety Features NPPs
    - Characteristics of nuclear power plants
    - Security objectives and basic defense strategies

Nuclear I&C Safety (cont.)

- Nuclear I&C Systems Basics
  - The role and characteristics of ICS in NPPs
    - Essential functions of the control systems of NPPs
    - Protection systems (in the Paks nuclear power plant)
    - Unit power control strategies, their characteristics
    - Typical architecture of the I&C systems of NPPs
- Nuclear I&C Systems Safety
  - The Principles of Nuclear Safety for I&C
    - Legal and regulatory background
    - Security categorization, security classification
    - Main principles of nuclear I&C design
    - Design for reliability of I&C systems important to safety