Topics for the Final Exams

Critical Embedded Systems (VIMIMA16) 2018

1. The basic concepts of system and software safety: Introduce the notions of accident, risk, safety, and safety integrity level (SIL). Present the relation of **safety integrity levels** and the development process required by safety standards.
2. Introduce the definitions and measures of reliability and availability: **MTFF, MTTF, MTTR, MTBF,** r(t), a(t), A. Provide an overview on the characteristics of faults and the means to improve dependability.
3. The architecture of safety-critical systems: Present the typical architecture solutions (single-channel architecture, two-channel architectures) used in case of **fail-stop** behaviour.
4. The architecture of safety-critical systems: Present the typical architecture solutions in case of **fail-operational behaviour** (fault tolerance for permanent and transient hardware faults).
5. The architecture of safety-critical systems: Present the typical **fault tolerance techniques** (N-version programming, recovery blocks) used in case of software design faults. Compare the solutions from the point of view of redundancy, execution time, and number of tolerable faults.
6. Hazard analysis techniques: Provide an overview of the typical hazard analysis techniques. Present the **checklists**, **fault tree analysis** (FTA), **event tree analysis** (ETA) techniques and the **cause-consequence analysis** (CCA).
7. Safety requirement specification: Present the concept of Functional Safety Concept (Risk, risk reduction). Specify what are risk bands and how they are reléated to the tolerability of hazards.
8. Formal modelling of time-dependent behaviour: Introduce the **timed automaton** formalism. Present the extensions of timed automata to support the modelling of distributed systems.
9. Formal verification: Show how to formalise safety requirements using **temporal logics** (LTL and CTL). Introduce the concept of formal verification with model checking.
10. **Basics of nuclear power generation**, inherent security, feedback (coefficients). Comparison of Functional Safety (61508) and Nuclear Safety. Postulated initial events (PIE), design basis. Nuclear incidents, accidents - INES scale. **Important reactor accidents and malfunctions**: Three Mile Island, Chernobyl, Fukushima (Serious incident at Paks in 2003). Regarding each nuclear accident: What causes and events led to the accident? How did the accident proceed and what were the consequences?

    What and how could/should have been done differently to avoid the accident / reduce the consequences? **What lessons were learned** from the accident and how did nuclear safety change, with particular regard to control systems?

11. **Characteristics of nuclear power plants**.Safety objectives and basic defense strategies. Major protection systems and their functions. Important Generation III + reactor types and their main characteristics.
12. **Essential functions of the control systems** of nuclear power plants. **Hierarchical and functional grouping** of nuclear control systems. (Normal operation) Control systems, Limiters (limiting controls), Interlocks, Protection systems: what role do fulfill, how do they influence the process? Protection systems in the Paks NPP. **Unit power control strategies, their characteristics**: Power Control with Pre-Turbine Intervention, Power Control with Reactor-side Intervention, Integrated. I&C functions in reactivity control, heat removal from the core, and confinement of radioactive materials. **Typical architecture** of the I&C systems of nuclear power plants.
13. **Legal and regulatory background** (Atomic Act, NSC (Govt. Decree 118/2011), Govt. Decree 190/2011). OAH's (Hungarian Atomic Energy Authority) role and responsibilities. IAEA's role and responsibilities, IAEA standards and guides. IEC (International Electrotechnical Commission): IEC standards for nuclear I&C systems. **Safety categorization** of functions, **safety classification** of equipment (IAEA, IEC and Hungarian). Main principles of nuclear I&C design. **Design for reliability** of I&C systems important to safety: defense in depth concept, single failure tolerance; common cause failure (the means of avoiding it); independence, separation, diversity. Fail-safe design, safety orientation concept.