Computerized I&C Modeling in PSA for R1 and R2

NKS/DIGREL SEMINAR 2010-09-14

NKS/DIGREL project on “Guidelines for reliability analysis of digital systems in PSA context"

Agenda

1. **Background**
   - **R1 (Modernization project RPS/SP2 – Ended 2009)**
   - **R2 (Modernization project TWICE – Ended 2009)**
2. **Failure modes - General**
3. **Challenges/Lessons learned**
4. **Conclusion**

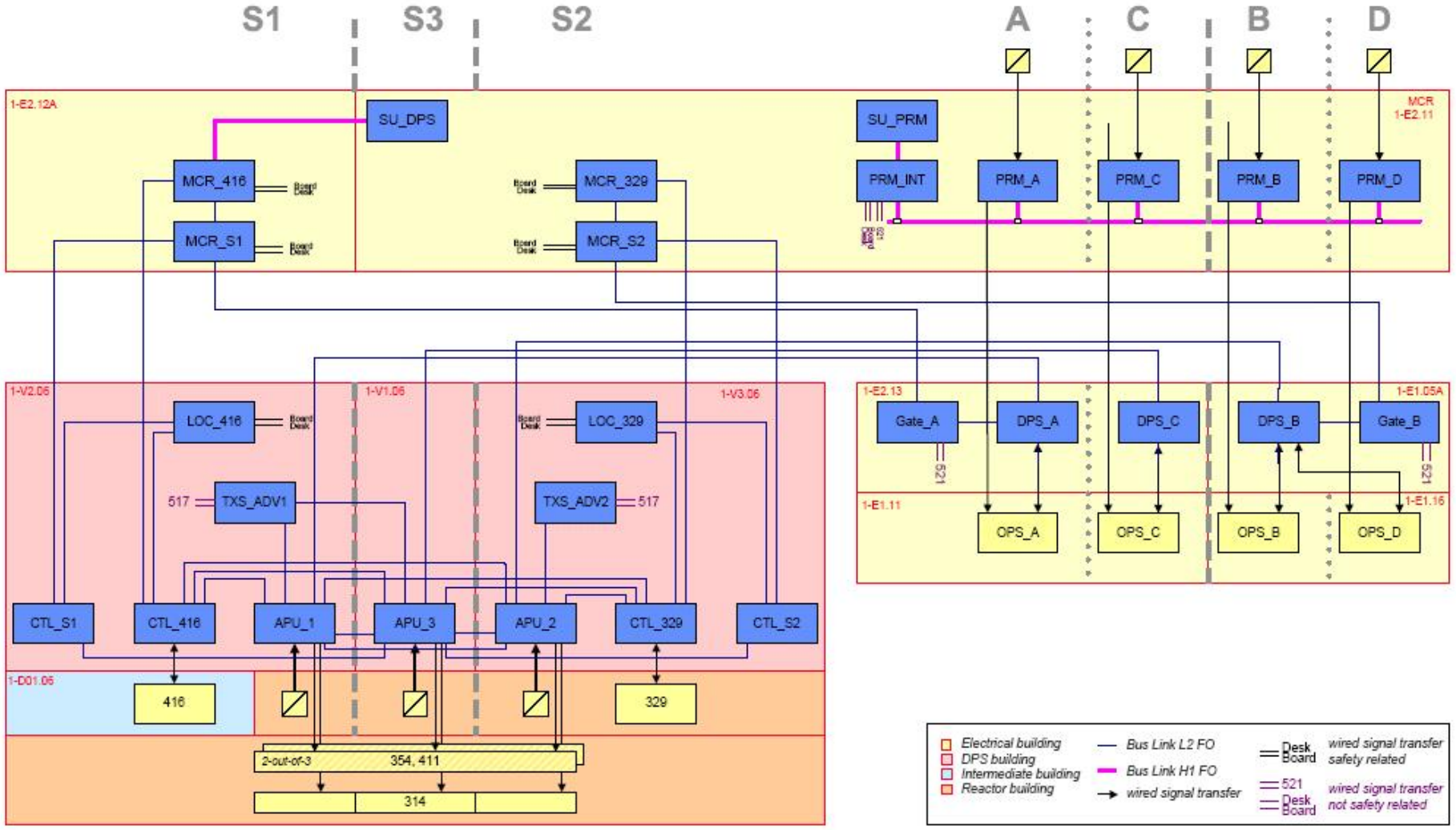
Background – R1

- Modernization of the **Reactor Protection System (RPS)** with certain system improvements, and modernization of the Residual Heat Removal (RHR) function.

- The chosen technical **RPS concept** is based on the addition of a new diversified and digital protection function (Diversified Plant Section, DPS) while maintaining the existing relay-based RPS.

- For the RHR function chosen technical **SP2 concept** is based on the addition of new independent RHR trains.

R1 - DPS I&C Architecture



Background – R2

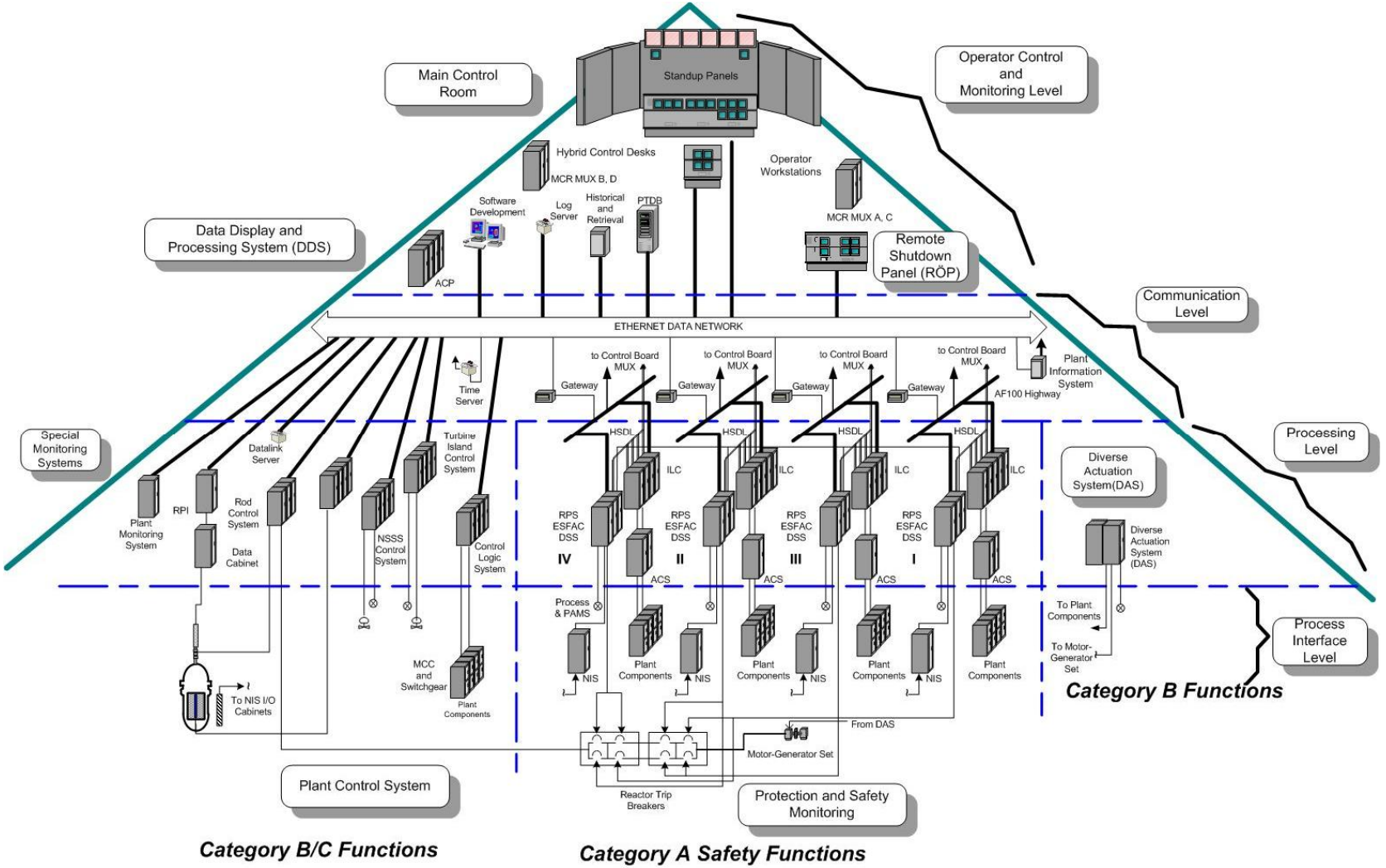
- The **TWICE Project (Ringhals TWo Instrumentation and Control Exchange)** includes the modernization of most of the instrumentation and control functions and associated systems and equipment at Ringhals 2, including the Main Control Room area.

- The **Reactor Safety System (RSS)** consists of two parts:
  - Software based RSS-system - AC160 platforms
  - Diverse actuation system (DAS) - Ovation platforms

- The RSS-system is composed of **four divisions** (A, B, C and D), associated with the **four power trains** (A, B, C, and D).

- All Safety System divisions are **physically**, **functionally**, and **electrically separated** from each other and from non-Category A systems.

R2 - DPS I&C Architecture



Failure modes – General

- The modeling of computerized I&C for R1 a R2 is based on a FMEA.

- Failure data from AREVA (R1) respectively from Westinghouse (R2) is used.

- Only hardware failures is regarded, software failure is only regarded or modeled as an CCF event.

Cont. Failure modes – General

- The main components modeled in the fault trees are:
  - Communication devices, (high speed links, cables etc)
  - Component Interface Modules (R2)
  - Processor Modules
  - I/O-modules
  - Power supply

Cont. Failure modes – General

- The general failure modes for R2 are:
  - No activation signals
  - Open, close or start signals

- For R1 is also detected (self-revealing) failures part of the scope due to the fail-safe concept:
  - Spurious activation (only detected failures)
  - No activation signals (latent and detected)

Cont. Failure modes – General

- Hardware CCF for latent and/or detected (self-revealing failures) failure modes:
  - R1 hardware CCF is modeled for latent and detected (self-revealing failures) failure modes and the consequence is depending on failsafe concept (“no activation on demand” or “spurious activation”).
  - R2 hardware CCF is modeled for latent failure and the consequence “on activation on demand”.
- Software CCF is analyzed for R1 and R2, but only part of the PSA model for R1 (no activation on demand).

Challenges/Lessons learned

1. **Achieving a realistic model of software based RPSs with traditional fault tree technique and the integration into existing PSA-models is a big challenge, for example:**
   - The complex design of a Digital RPS in many ways puts the task of systems analysis on untouched ground and requires that previously well established methodologies are revised.
   - Modelling of a Digital RPS significantly increases the effort of failure mode analysis, dependency analysis and fault tree modelling.
   - The amount of resource involved in the task should not be underestimated, neither should the task of quality assurance.

Cont. Challenges/Lessons learned

2. **Documentation and transparency must be improved**

3. **Large expert need:**
   - **Electrical software experts for mapping of electrical dependencies**
   - **PSA software experts for modeling and review**
   - **Plant operation and construction expertise for handling design questions**

Cont. Challenges/Lessons learned

4. **Use of results in the construction phase for R1 and R2 was weak, possible areas for improvement:**
   - **Single failure analyses**
   - **Comparing different solutions**
   - **V&V**

Cont. Challenges/Lessons learned

5. **R2 CDF-contribution, not as-built results (TWICE BL 6.0):**
   - **The modeling of the new RPS [539] is more detailed than the modeling of the previous solid-state protection system.**
   - **The importance of the new reactor protection system (RPS) to the overall CDF is 6%.**
   - **If the direct actuation system (DAS) also is included is the importance 7%.**

Cont. Challenges/Lessons learned

5. **Cont. R2 CDF-contribution, not as-built results (TWICE BL 6.0):**
   - **The importance of RPS is strongly dependant on the failure rate for the ILCs, which has an importance of 4%.**
   - **The importance of the solid-state reactor protection system before TWICE was less than 1%.**

Cont. Challenges/Lessons learned

6. **R1 CDF-contribution, not as-built results (RPS/SP2 BL 2.3):**
   - **The modeling of the new RPS [505] is more detailed than the modeling of the previous RPS system.**
   - **The importance of the new reactor protection system (RPS) to the CDF (loss of core cooling) is 26%.**
   - **The importance of the previous reactor protection system before RPS/SP2 was less than 6%.**

Cont. Challenges/Lessons learned

6. **Cont. R1 CDF-contribution, not as-built results (RPS/SP2 BL 2.3):**
   - **Software CCF system 505:**
     - **The contribution from software CCF is very low, <<1%, and even if the probability of software CCF is increased from the applied value of 10-6 to a conservative value of 10-4 the total CDF only increases with approximately 1.5%.**
   - **Hardware CCF system 505:**
     - **Analog input, latent failures modules, highest FC (3,4E-02)**

Conclusion

- **The task of incorporating a model of a Digital RPS realistic into a PSA is a challenge!**
- **The importance of the new digital RPS is large!**
- **The impact on the CDF from the software CCF can be neglected for R1 (design related and not based on as-built results)!?**
- **Software failures is considered one of the most prioritized areas of future development!**

Cont. Conclusion

- **Digital I&C modeling in PSA is an issue for every utility OR will be!**
- **Benchmark studies and Guidelines on the use of taxonomy in modeling, data collection and quantification of digital I&C reliability in PSA are strongly needed!**
- **Ringhals intention and objective is to actively contribute as far as possible to reach useful results!**