Project's full name:	Guidelines for reliability analysis of digital systems in PSA context
Project's short name:	CHARISMA / NKS-DIGREL
Project's number:	41265-1.5
Drawn up by:	Jan-Erik Holmberg, VTT and Stefan Authén & Josefin Larsson, Risk Pilot
Date:	September 14, 2010
Place:	Espoo, VTT, Digitalo, Vuorimiehentie 3, meeting room AP314

Persons present

1. Jan-Erik Holmberg, VTT
2. Kim Bjorkman, VTT
3. Ilkka Karanta, VTT
4. Juho Matikainen, VTT
5. Stefan Authén, Risk Pilot
6. Josefin Larsson, Risk Pilot
7. Stefan Eriksson, Ringhals AB
8. Jan Nirmark, Vattenfall Power Consultant
9. Bo Liwång, SSM
10. Kalle Jänkälä, Fortum
11. Ilkka Paavola, Fortum
12. Jari Pesonen, TVO
13. Lennart Wallin, OKG
14. Michael Landelius, OKG
15. Ola Bäckström, Scandpower
16. Gennady Loskutov, Scandpower

1 Opening of the meeting

Jan-Erik Holmberg opened the meeting and welcomed everybody to the workshop. Participants presented themselves.

2 Project aim, scope and basic concepts

Jan-Erik Holmberg presented the project aim and scope (attachment 1) and Stefan Authén presented basic concepts (attachment 2).

Discussion
- Project scope is large compared to the size of the project
- Is it possible to model the reliability of software? Is it meaningful to model the reliability of software? Software failures are not random by nature. The hard thing is to find data which is applicable for reliability modelling.

3 International literature survey

Kim Björkman presented a summary of the international literature survey (attachment 3).

Discussion

- Are we interested in exact numbers? The difficulty is to find data to the model. There can be a method to estimate software reliability, but it is not necessarily the reliability in PSA context. In PSA, software reliability related to type II interactions[1] of digital I&C systems are of interest.
- The digital feedwater control system example of NUREG/CR-6962 is not a good example from PSA point of view.
- One position is that the aim is to verify that the plant fulfils reliability targets. Exact numbers are not needed. The question is what numbers should be used in PSA and how to justify them.
- EDF modelling approach is one alternative[2]

4 Situation in Finland and Sweden, practices, needs and problems

Stefan Eriksson presented modelling of I&C system in Ringhals 1 and Ringhals 2 PSAs (attachment 4).

Discussion

- Software CCF was screened out in the vendor's analysis in R2.
- Reference documents used in the analysis were spread out.
- Use of PSA model during the modernisation projects was weak. There was a CDF criterion for the I&C system, but this was not actually applied in the licensing process.
- ILC (integrated logic circuit) components have quite high failure rate and quite high risk importance
- The vendor wants to use "calculated" failure rates instead of directly empirically estimated failure rates. Empirical failure rates are lower than calculated failure rates.

[1] [NUREG/CR-6901] "*From a reliability modeling perspective, this conclusion implies that there is a need to account for the dynamic interactions between the reactor protection and control systems and controlled plant physical processes (e.g., heatup, pressurization) and also between the components of the reactor protection and control systems itself (e.g., communication between different components, multi-tasking, multiplexing). These interactions will be referred to as Type I and Type II interactions, respectively.*"

[2] [NEA/CSNI/R(2009)18] "*...the goal of this model* [EDF compact model] *is to represent simply the contribution to the failure of the protective action of the components implemented in the control channels. The model divides an I&C channel into four parts: sensors part, logic part specific to a given protection channel and its processing logic, logic part common to all channels and specific to a programmable controller, and actuation part. The final value of the unavailability assigned to the I&C automatic devices is considered to essentially come from systematic failures (mainly residual errors), and their importance can only be evaluated from a qualitative judgment based on the devices' quality. This judgment is independent of the modeling options. Standard unavailability values for a single protection channel are assigned according to the channel's classification level.*"

- In R1, conservative treatment of corrective maintenance contributes to the results. The problem is the lack of data to estimate repair times, and therefore Tech.Spec. AOTs are assumed.
- 10^{-4} is typical probability value assumed for CCF, and it is considered conservative number, but is it conservative?
- The development of software modelling should be to address the software failures in the analysis.
- Detected failures can have importance to CDF (R1 experience)
- Utilities are dependent on data provided by vendor. Vendor’s analysis must be accepted.
- There is a large uncertainty how large part of the failure rate is detectable and how large part is latent. The amount of detected failures are more important than the failure rate it self.
- Undetected failures are assumed to be detectable in periodic tests.
- Diversification of RPS is needed to reach the reliability goals.
- In O1 modernisation, Siemens was responsible for the safety concept and Westinghouse Atom for I&C equipment

Jari Pesonen presented modelling of I&C system in Olkiluoto 1/2 PSA (attachment 5).

Discussion

- In the turbine automation project, probabilistic analysis was made to be verify the compliance of the deterministic requirement with regard to the frequency of spurious turbine trip with dump blocking (TS x D)
- SIL-judgements were applied to PLC-software
- Functional failure matrix is an extension of FMEA and can be used to analyse consequences of I&C component failures
- Olkiluoto 3 has hardwired back-up, which has some computerised features

Kalle Jänkälä presented modelling of I&C system in Loviisa automation renewal PSA (attachment 6).

Discussion

- At this stage, preventive protection system has been implemented. RPS will be replaced later in future.
- No data available to judge CCF and software failure probabilities. Only single failure data from the supplier.
- CCF has been postulated with diversified components
- In the estimation of CCF between transmitters, ICDE data has been used.
- The approach can be called super basic event modelling
- This is a design phase PSA. Detailed modelling has been done for some parts, but not yet for RPS
- FT-models provided by the vendor are detailed, in module level, but they are not as such applicable for PSA. Vendor’s FT-models seem to be similar to Ringhals 1 model. It is unsure how detailed FT-models

will be finally made in PSA. A big difference between Loviisa and Ringhals 1 is the fail safe concept.

Stefan Authén made a summary of the modelling approaches in the Ringhals 1, Ringhals 2 and Olkiluoto 1/2 PSAs (attachment 7).

Discussion

- The scope of OL1/OL2 modernisations is different from Ringhals. OL1/OL2 modernisations do not include RPS.
- Oskarshamn 1 modelling approach is more like Ringhals 1 than Ringhals 2.
- Need to model spurious actuations depends on the plant design
- Super-component modelling approach is usual. Group components in super-components as far as possible to get a small model but not more than you can motivate.
- There is experience from analog I/O module failures in Ringhals 2

5 OECD/NEA WGRISK activity on "Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA"

Jan-Erik Holmberg presented OECD/NEA WGRISK activity on "Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA" (attachment 8).

Bo Liwång, who is the member of the OECD/NEA COMPSIS project, explained the COMPSIS activities. COMPSIS is a operating experience exchange project on computerised system failures, see http://www.compsis.org/Compsis

6 Information about other related activities

Jan-Erik Holmberg informed about other related activities at VTT (attachment 9).

Discussion

- The EURATOM Framework Programme 7 project proposal HARMONICS is partly based on work done in EURATOM FP6 projects CEMSIS and BE-SECBS. CEMSIS results can be found in http://www.cemsis.org/

7 Discussion

Jan-Erik Holmberg introduced the discussion items (attachment 10). Jari Pesonen presented issues based on TVO’s experience (attachment 11).

Discussion

- Guidance is needed to define input needed for the analysis
- Guidance is needed for how to use PSA during design
- Present PSA guidance documents provide very little support to the reliability analysis of I&C systems

- There are different requirements for I&C in different safety classes
- One question is whether software failure can be screened out, how this could be justified and what evidence is used
- There can be software failures in different levels: compiler, base, operating system, application software
- Software errors are CCFs per definition. Hardware failures are more like single component failures.
- PSA is an approximation of what can happen
- Hardware failures are more probable than software failures
- It would be good to have a check list of software failures to be considered in the reliability analysis.
- Software failures are often dependent on the environment and influence the whole system.
- How can we identify consequences of software failures? We need a method to identify dependencies. Quantification is the next step. Some consequences are modelled, but it can be difficult to say which consequence is worst.
- Justification of numbers used for software reliability is an open issue. The vendors or the vendors' competitors are the only ones that could confirm the numbers.
- V&V is intended to achieve a high reliability for these systems, but it does not provide numbers.
- Analysis of "fail-safe-state" is important. "Fail-safe-state" is not necessarily safe state with respect to all consequences. Computerised voting logic can be degraded in several ways. These considerations can lead to the need of a detailed system reliability model.
- We need a strategy on how to handle the open issues.
- Plant design should be such that it tolerates the behaviour of degraded systems. Should the design be simpler than present concepts? Modern technology provides too many features, which may then cause problems in safety critical applications. One solution is to implement manual possibilities to recover from automation system failures.
- We need a description of problems areas, list of issues to be considered in the reliability analysis.
- Primary thing is the demonstration of safety. We need a common understanding what is needed for the demonstration and what is the role of PSA in the demonstration.
- Guidance is needed to define the right level of details, use of failure data and modelling approach to get better confidence on PSA.
- RPS is the main issue, not PSA.
- Guidance is needed to define the contents and level of details of the documentation.
- It is important that the utility, vendor and authority discuss in the early phase of the project and agree on the licensing process
- One problem is that vendor does not have the necessary understanding of the PSA needs which is required to get more exact information to the PSA.
- The question of estimation of software failure rates remains. V&V provides some evidence. Principally, we could assume that the

triggering events follow a random process, but the rate of triggering events is unknown. We do not have data to estimate CCF.
- Could SIL numbers be used?
- In 1980’s the status and use of PSA was discussed. Focus was on quantification, but qualitative insights from results should be used too.
- The idea of having generic I&C system as reference for the definition of failure modes taxonomy is regarded as good. Maybe several variants are needed to cover features of different present I&C solutions.
- It was supported that the WGRISK working meeting in Spring 2011 would be arranged in Finland or Sweden. It would be a good idea to invite the vendors.
- We need a list of important issues to be considered in the reliability analysis. This should reduce the burden of vendor, too.
- Human factors and control room issues could be important to address, too. I&C failures can have unpleasant consequences in the control room.
- This is a large area to be discussed. It can be expected that not much can be solved within next few years.
- How does fire affect these systems?
- PSA has up to present been a fix state analysis, but not any more. How to address dynamic features in the PSA?

8 Summary

- Early discussion between the utility, vendor and authority is necessary.
- Develop a guideline: Discuss the failures, the common problems and the level of details. Generic I&C system example is OK.

9 Closing of the meeting

Jan-Erik Holmberg closed the meeting at 15:40.

ENCLOSURES

1. Jan-Erik Holmberg, Introduction
2. Stefan Authén, Basic concepts
3. Kim Björkman, Literature survey
4. Stefan Eriksson, Computerized I&C Modeling in PSA for R1 and R2
5. Jari Pesonen, Modelling of I&C system in Olkiluoto 1/2 PSA
6. Kalle Jänkälä, Reliability of New Plant Automation of Loviisa NPP
7. Stefan Authén, Investigation of state-of-the art in Nordic PSA-studies
8. Jan-Erik Holmberg, OECD/NEA WGRISK task
9. Jan-Erik Holmberg, Related activities at VTT
10. Jan-Erik Holmberg, Discussion items
11. Jari Pesonen, Discussion

DISTRIBUTION Participants, SAFIR TR8, NPSAG, NKS/Patrik Isaksson