October 16, 2015

NKS-R MODIG and PLANS
Joint workshop on reliability analysis and safety demonstration of digital I&C

29-30 September 2015, Espoo, Finland

Location: VTT, Vuorimiehentie 3, Espoo

Notes drawn by: Ola-Bäckström, Jan-Erik Holmberg, Vikash Katta and Tero Tyrväinen

Background

MODIG (Modelling Of DIGital I&C) project aims at developing a consensus approach for a reliability analysis of a plant design with digital I&C, including improved integration of probabilistic and deterministic approaches in the licensing of digital I&C.

PLANS (Planning Safety Demonstration) project aims at providing detailed guidance on selected topics of safety demonstration and planning for digital I&C systems in NPPs by building upon existing guidance and models for safety justification.

The Finnish research activities within MODIG and PLANS are part of a larger research project SAUNA "Integrated safety assessment and justification of nuclear power plant automation", which is included in the Finnish nuclear research programme SAFIR2018, see http://virtual.vtt.fi/virtual/safir2018/index.htm

The aim of the workshop was to discuss topics related to the safety assessment of digital I&C at nuclear power plants, software reliability, requirements on digital I&C, safety demonstration and safety case.

Agenda and participants

Workshop agenda is given in Appendix 1 and the list of participants are given in Appendix 2. Workshop presentations were submitted to workshop participants separately.

Summary: Day 1

Janne Valkonen and Antti Pakonen (VTT), Introduction of VTT, SAFIR2018 and SAUNA project

SAUNA is an integrated approach and toolset for safety demonstration of nuclear power plant automation, and is the project embracing both MODIG and PLANS (the projects the workshop is covering).

Jan-Erik Holmberg (Risk Pilot), project leader for MODIG, introduces the MODIG project and gives a history of the DIGREL project

Objective of MODIG is:

- Get a consensus in the approach for reliability assessment
- Get improved integration of DSA and PSA with regard to digital I&C
- Improve failure data collection including SW

- To perform practical application of PSA to compare design alternatives

For this year:

- Assessment of Defense in Depth (DiD) with PSA with emphasis on I&C
- Framework for analysis of spurious actuation
- SW reliability analysis
- Collection of data within WGRisk

Jan-Erik Holmberg (Risk Pilot), Defense in depth (DID)

Jan-Erik continues with a presentation of DiD from an I&C perspective. The concept of DiD is applied also in other industries but then referred to as Layer or Lines Of Protection. The concept of DiD has evolved over time. DiD is understood in the same way, but the applied regulatory requirements may differ (e.g. Swedish and Finnish requirements). The presentation also covers discussion about what an I&C system is. Then the presentation discusses the challenges regarding DiD for I&C systems. It is in practice not possible to have full diversified DiD levels and I&C systems. The diversification shall be reasonable, as specified in the YVL. Some questions are formulated with regard to DSA, for example;

- how to classify initiating event categories
- what is the level of abstraction with regard to applying failures
- how to assess diversification

A question that is raised, and is important for the evaluation of DiD is how *reasonable* is defined. Jan Erik raises the question if PSA be used as part of this evaluation?

There are several research topics with regard to PSA and DiD raised, e.g.;

- More detailed analysis of DiD level 1-2
- Numerical risk criteria for DiD level 3-5 (PSA level 1-3)
- Assessment of independence between barriers (diversity)
- Assessment of impact of complexity
- How are DiD levels understood

Discussion:

Challenges with regard to DiD estimation were discussed.

Petteri Suikkanen (STUK), Failure tolerance analysis

Petteri presents how failure tolerance analysis requested by STUK shall be understood.

“Old” relay technology tends to be independent by nature. Modern I&C are not. How to consider failure propagation? You have to demonstrate independence between barriers.

What if an active failure happens? You should assume this and a simultaneous initiating event. Then you need to demonstrate that you are still within acceptance criteria. One entity shall assume to go to worst possible scenario. If it is more than one redundancy and they are the same and interconnected, then “one entity” can actually be CCF between redundant entities.

The STUK YVL requirements with regard to I&C systems safety were introduced. Then some comments on “how to make it real life” were made. You should note that also multiple spurious actuations of one entity shall be assumed.

You should not screen out failure combinations based on low frequency, you should study the consequences first.

Discussion:

Discussion about independence and interconnection. When is an entity independent?

How can this type of analysis be performed early in the process, to avoid heavy re-design of the I&C system? Can PRA be part of the design choice? There are references where this has been done.

The EPRI report 3002002953 “Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments” is including some basic rules when designing an I&C system to avoid finding significant design problems at a late stage.

It was stressed that a digital I&C system could implement a system that is exactly mimicking the relay system, but that makes no sense – you do not consider the positive effects of this type of system.

The approach presented could potentially also be used to support cyber security analysis, but that is not the target of this presentation.

The approach is similar to NRC approach, but the definition of entities is not necessarily the same.

Discussion session, How can PSA be part of the safety justification

How can PSA be part of the safety justification?

- The Minimal Cut Sets (MCS) can be used to identify relevant scenarios and complex failure combinations
- If something cannot be fully excluded, then that could be relevant for PSA.
- Use the MCS as qualitative information.

The question was raised if digital I&C need its own definition of independence. The consensus however seemed to be that this is not the case.

What are the hardest questions for DSA/PSA?

- Capability to define entities is probably one of the main issues. Level of abstraction.
- How is independence defined
- Unplanned dependencies

Should PSA and DSA use the same level of abstraction? Is there any reason that we should not use that?

Tero Tyrväinen (VTT), Ola Bäckström (LRC), Software failure probability

Tero and Ola presented the method for analysis of software reliability. The software is split in different types of software. For system failures only fatal failures are considered, but for application software both fatal and non-fatal failures are considered.

System failure modes, communication failure modes and failure modes of application software leading to fatal failures are proposed to be estimated based on operational experience. Non-fatal failures are estimated based on a metric of level of V&V and Complexity. A method for complexity estimation was also presented (SICA).

Discussion

- Are active and passive failures considered? Yes, see definitions for fatal/non-fatal failures
- Entities are defined hierarchically following the I&C architecture
- Meaning of demand is same as in PSA
- System SW is one entity. Claim "only fatal failure needs to be considered"
- Atte H: "earlier VTT experience from the analysis motor-protection relays, opposite way of quantifying SyS and AS as proposed in DIGREL/MODIG
- Two-stage Bayesian may be used when analysing OE (Jan Stiller's proposal)

Unintended software failures was discussed and it was discussed if the method could study failure propagation. It should be possible to study the failure propagation through the FT logic. It was suggested that this should be addressed further in the report.

Mariana Jockenhövel-Barttfeldt (Areva), Analysis of spurious signals

Mariana presented that in the traditional approach spurious signals are considered to have very low probability. The challenge is to model spurious signals in a reasonable way. The focus of the presentation is on hardware failures.

Classification of spurious signal

- Single spurious signal
- Multiple spurious signals

Important boundary conditions in the analysis are (which are backed by deterministic analyses)

- Failure of HW modules are single failures
    - Active failures are not correlated
    - Accumulation of random failures are excluded
- Progression of IE is not aggravated/worsened by the emission of single/multiple spurious signals

- Higher class systems are not affected by lower class systems

Detection is very important. The focus is on delayed detection.

Steps:

- Scoping, identify potential signals
- Effects of spurious signals (analysis of dependencies)
    - It was found that all effects were actually covered by the PSA (e.g. CCF between I&C units, CCF between components etc)
- Identify process components, whose actuation could lead to unavailability of the system
- For each component, list all possible I&C functions that could affect the component and then identify which could lead to the spurious failure of interest.

The analysis has been performed on large scale PSA. The screening analysis covered approx. 300 pages listing of I&C signals. The conclusion was that spurious actuations are not significant for PSA results.

Discussion

The analysis is performed on hardware module level.

The analysis has not been performed for software, and the essential difference would be that we can no longer talk about single spurious signals.

Markus Porthin (VTT)/Jan Stiller (GRS), WGRisk I&C diversity assessment and data collection activity

The presentation is about an initiative on data collection, which is put forward to the OECD/NEA working group on risk assessment. The activity may be approved by the end of 2015 and if approved, it can commence from 2016.

Objectives were presented as defining taxonomy and a guidance on I&C diversity assessment and how to collect data. The scope covers both hardware and software. The outline of activities for the coming 3 years was presented. The co-operation with ICDE is a natural part of the activity.

The plan is to have the guidance on data collection and the taxonomy ready and accepted by CSNI in June 2019.

Everyone is encouraged to participate!

Discussion

- The application of the information is not intended for PSA only.
- What type of equipment should be included. Not fully defined, but software based is a good attribute.
- There is a trial on ICDE going on with regard to software failure collection.

- Is the purpose to be able to quantify the diversity? This is one objective!
- In ICDE the raw data is available for contributing countries.
- WGRisk reports are public.
- Will NRC join the WGRisk project. Not clear at this point, but there is a significant probability they will.
- US.NRC has prepared a D3-guidance
- IAEA report on I&C CCF

Final discussion

The final discussions did span over all of the topics during the day. Below are the main topics being discussed.

- Have you looked into the failure mechanisms of the occurred failures? Yes, but very few failures have occurred.
- What types of errors are occurring in software design? Information could help the process of software development to improve. Most (of the few) failures that have been discovered (by Siemens) are in the operating system and not in the application software. Hence there is not much learning for the application software developers. The question was raised if Siemens can share their experience of found errors? (It should be noticed that systems are different and the above discussion was based on the Siemens system).
- Operating experience should be analysed to find types of design errors – what are difficult issues for designers
- Wrong human actions/maintenance is most common reason, deviation from procedures
- Will the requirement on operating experience be a show-stopper for designing new systems? If new systems are requested to demonstrate operating experience, then there will be a catch 22 (paradoxical situation where the escape is impossible). It was however discussed that we are rather seeing evolution of existing systems, so maybe this should be ok.
- Definition of entities is important
- The proposed level of detail looks quite ok
- The definition of an entity is system specific. Definition of which entities to study and the SyS are dependent on the system. Based on the discussion the entities presented regarding software failures seemed reasonable to the audience. There was also support from the audience regarding the Fatal failure assumption for SyS software.
- Numbers are less important, uncertain. It was discussed that sensitivity analysis should be performed for all types of failures and should be an important way to demonstrate robustness.
- Meaning of "independence" is ambiguous
- Safety demonstration example using PSA could be interesting. Demonstrate how PSA could be used
- Further development of failure tolerance analysis method

- Guidance on failure modes which can be screened out. residual shall be quantified
- How to make FMEA for SW
- Comparison of designs could be interesting

During the discussion about focus areas for coming years following issues were discussed:

- Safety justification using the methods. How to include in failure tolerant analysis?
- Failure modes for CCF
- Quantification of relevant data
- Experience from different styles of modelling, to get any feeling for fractions of what is really contributing
    - Should be tested on real models
- Look at also other systems, e.g. aviation. Can we get information?
- Configuration management is very important for software. Failures are often due to maintenance.
- Comparison of different architectures combined with sensitivity analysis would be interesting.

Summary: Day 2

Day 2 of the joint workshop was conducted by the NKS-R PLANS (Planning Safety Demonstration) project. The objective of the 2nd day of the workshop was to bring together experts from NPP domain to actively seek their expertise in safety demonstration of systems as well as to disseminate the up-to-date results of the PLANS project.

The PLANS project aims at providing detailed guidance on selected topics of safety demonstration and planning for digital I&C systems in NPPs by building upon existing guidance and models for safety justification.

Agenda

The workshop started with an introduction to the PLANS project. PLANS project partners gave presentations on the ongoing work on improving guidance on safety demonstration planning, especially on safety demonstration plan guide. These presentations focused around the following topics, which were the suggested future directions/activities by the participants of an earlier PLANS workshop conducted in May 2015.

1. Define how safety demonstration fits with systems engineering.
2. Define terminology for the concepts of safety demonstration.
3. Examples describing how to apply safety demonstration plan guide.
4. Multidisciplinary safety demonstration approach covering the overall plant.
5. Increase the awareness on safety demonstration within the NPP community.

In addition to presentations from PLANS project partners, the workshop had six presentations on practical experiences, research and standardisation activities in safety demonstration. The workshop also had a brainstorming session on safety demonstration and future activities for PLANS.

Overview of the PLANS project, Vikash Katta (IFE)

A brief introduction to PLANS laying out its background and objectives was given. The future directions/activities which were elicited during earlier PLANS workshop were also introduced to the participants.

Fennovoima's strategy to demonstrate and justify safety in Hanhikivi 1 project, Janne Peltonen (Fennovoima)

This presentation outlined Mr. Peltonen’s views on Fennovoima’s strategy to demonstrate safety, including the development of management systems. Mr. Peltonen discussed the important aspects of demonstration of I&C including the importance of requirements management, architecture design and clearly defined interfaces between different systems. He also illustrated the different roles/personnel involved in development and demonstration activity, highlighting the importance of having a good information flow between personnel from different disciplines and organisations. The discussions after the presentation were on, but not limited to, how knowledge transfer is achieved between I&C supplier and Fennovoima.

Extracting the assurance argument from an interim safety demonstration – A case study from the nuclear field, Peter Karpati (IFE)

Dr. Karpati’s presentation was on an ongoing case study in the Safety Demonstration Framework Project carried out as part of the OECD Halden Reactor Project. The presentation focused on applying a structured review approach for extracting safety arguments in an existing NPP submittal. Observations with respect to the comprehension of the argument (which was implicit in the submittal) were presented. Dr. Karpati also gave an overview of a notation for categorising different types of claims, where the notation is being developed to support the extraction of safety argument.

Current I&C status at SSM, Niclas Larsson (SSM)

An overview of the SSM with its organisational structure and I&C activities were briefly presented. Due to ongoing renewal of the Swedish nuclear safety regulations, SSM could not much comment the safety demonstration topics.

Introduction to Safety Demonstration Plan Guide (SDPG), Pontus Ryd (Solvina)

Mr. Ryd gave a thorough presentation on the Safety Demonstration Plan Guide (SDPG), which was developed by Solvina for ELFORSK. The main contents of the guide, including the overall safety demonstration lifecycle and its phases, and safety subject areas were explained. Mr. Ryd also pointed out the importance of accurately defining the product scope and I&C requirements, and how vital it is to demonstrate that the product scope and I&C requirements are complete, consistent and correct.

Applying SDPG – Initial results from a case study, Vikash Katta (IFE) & Pontus Ryd (Solvina)

The ongoing work on extending SDPG by detailing the guidance on safety subject areas (SSAs) and by preparing examples on application of the guide was presented. With the help of an example of an existing submittal, it was being described how three SSAs of SDPG (namely *Product Design*, *Product Design Qualification Status*, *QA and Plans Compliance Including Organization and Competence Assessment*) can be detailed into claim-evidence structures. Observations on how to use the guide to put forward the approach for reasoning on safety was discussed.

Characterization of safety evidence for assessment and certification of critical systems, Sunil Nair (IFE)

Dr. Nair's presentation started with giving clarifications on the difference between assurance and demonstration, and provided overview of the concepts (claim, evidence and reasoning) underlying certification/demonstration. He presented his research on safety evidence categorisation, and highlighted the importance of evidence structuring and management especially while developing large systems which involves large amount of documentation. He also presented his work on an evidential reasoning approach for assessing confidence in safety evidence.

Safety case tool review, Joonas Linnosmaa (VTT)

Mr. Linnosmaa presented his ongoing Master Thesis work on investigating existing tools for safety case development. Different tools available in the market, their functionalities, and notations (e.g. GSN, CAE) they support were presented.

Common position on licensing of safety critical software for nuclear reactors, Mika Johansson (STUK)

Mr. Johansson's presentation outlined the contents of the common position on licensing of safety critical software for nuclear reactors. Participants, history, and scope of the document were introduced. Weak points and topics that might be considered in the next revisions of the document include cybersecurity, third party qualification. failure analysis that should be done, and HFE issues. Level of awareness of the document is high because it is used a lot as a reference. However, its actual usage is not known.

Related work (Harmonics, RIL 1101, etc.), Janne Valkonen (VTT) & Pontus Ryd (Solvina)

A brief overview to relevant work such as Harmonics project and RIL 1101 guidance was given to the participants.

Brainstroming, Teemu Tommila (VTT), Janne Valkonen (VTT), Pontus Ryd (Solvina)

A brainstorming session was conducted in the last session of the workshop. First Teemu Tommila and Janne Valkonen moderated discussion on clarifying the concepts of safety demonstration, difference between safety demonstration case and safety analysis report, relation between safety demonstration and other processes/activities such as systems engineering, requirements engineering and PSA.

Secondly Pontus Ryd moderated discussion on the possible topics on which the further work of the PLANS project should focus on. It was pointed out that SDPG’s approach of demonstration planning covering entire life cycle and organising safety reasoning as safety subject areas is interesting. Some participants pointed out that SDPG provides a good starting point for projects to plan for safety demonstration. The future directions on improving SDPG such that it supports multidisciplinary approach for safety demonstration got the most attention from the participants.

Appendix 1 Programme

Day 1: Tuesday, September 29, 2015

Session	**Topic**	**Speaker**
09:00-09:15	Opening of the workshop - Welcome, introduction of participants - Introduction to the joint workshop	Jan-Erik Holmberg, Risk Pilot Janne Valkonen, VTT Vikash Katta, IFE
09:15-09:30	Short overview of the Finnish nuclear research programme SAFIR2018 and the SAUNA (Integrated safety assessment and justification of nuclear power plant automation) project	Antti Pakonen, VTT
09:30-09:45	Short overview of the MODIG project	Jan-Erik Holmberg, Risk Pilot
09:45-10:30	Defence-in-depth and I&C	Jan-Erik Holmberg, Risk Pilot
10:30-10:45	Coffee break	
10:45-11:15	Failure tolerance analysis of I&C	Petteri Suikkanen, STUK
11:15-12:00	Discussion – How can PSA be part of the safety justification?	Jan-Erik Holmberg, Risk Pilot
12:00-13:00	Lunch	
13:00-14:00	Software reliability	Ola Bäckström, LRC Tero Tyrväinen, VTT
14:00-14:30	Modelling spurious signals in probabilistic safety assessment	Mariana Jockenhövel-Barttfeld, AREVA
14:30-14:45	Coffee break	
14:45-15:05	OECD/NEA Working Group RISK initiative on diversity assessment and failure data collection	Markus Porthin, VTT
15:05-16:00	Discussion – Future planning, conclusions	Markus Porthin, VTT
16:00	End of Day 1	

Day 2: Wednesday, September 30, 2015

Session	Topic	Speaker
09:00 – 09:20	Overview of the PLANS project	Vikash Katta, IFE
09:20 – 09:50	Fennovoima's strategy to demonstrate and justify safety in Hanhikivi 1 project	Janne Peltonen, Fennovoima
09:50 – 10:15	Extracting the assurance argument from an interim safety demonstration – A case study from the nuclear field	Peter Karpati, IFE
10:15 – 10:30	Current I&C status at SSM	Niclas Larsson, SSM
10:30 – 10:50	Coffee break	
10:50 – 11:20	Introduction to Safety Demonstration Plan Guide (SDPG)	Pontus Ryd, Solvina
11:20 – 11:50	Applying SDPG – Initial results from a case study	Vikash Katta, IFE Pontus Ryd, Solvina
11:50 – 12:45	Lunch	
12:45 – 13:15	Characterization of safety evidence	Sunil Nair, IFE
13:15 – 13:35	Safety case tool review	Joonas Linnosmaa, VTT
13:35 – 14:00	Common position on licensing of safety critical software for nuclear reactors	Mika Johansson, STUK
14:00 – 14:20	Coffee break	
14:20 – 14:30	Related work (Harmonics, RIL 1101, etc.)	Janne Valkonen, VTT Pontus Ryd, Solvina
14:30 – 15:55	Discussion - Future directions for safety demonstration - Essence of safety demonstration - Relation to design and licensing of I&C	Teemu Tommila, VTT Janne Valkonen, VTT Pontus Ryd, Solvina

	- Role of PSA in safety demonstration - Practises: Proposals for improving SDPG	
15:55 – 16:00	Conclude, End of workshop	Vikash Katta, IFE

Appendix 2. Participants

Country	Organisation	Name
Finland	Risk Pilot	Jan-Erik Holmberg
Germany	AREVA	Mariana Jockenhövel-Barttfeld
Sweden	Lloyd’s Register Consulting - Energy AB	Ola Bäckström
Finland	VTT	Markus Porthin
Finland	Fennovoima	Janne Peltonen
Finland	VTT	Tero Tyrväinen
Sweden	ÅF	Gunnar Johanson
Finland	VTT	Antti Pakonen
Finland	VTT	Janne Valkonen
Finland	Bewas	Björn Wahlström
Netherlands	NRG	Wietske Postma
Finland	STUK	Ilkka Niemelä
Finland	STUK	Petteri Suikkanen
France	EDF R&D	Gilles Deleuze
Finland	VTT	Nikolaos Papakonstantinou
Finland	Fortum	Ville Nurmilaukas
Sweden	ÅF	Bengt Lidh
Finland	Fortum	Martti Välisuo
Germany	Siemens AG	Kurt Schulmeister
Norway	IFE	Vikash Katta
Norway	IFE	Peter Karpati
Norway	IFE	Sunil Nair
Norway	UiB	Eivind Korssjøen
Sweden	Solvina AB	Pontus Ryd
Finland	Fortum	Mikko Pihlanko
Germany	GRS	Jan Stiller
Finland	Fortum	Kalle Jänkälä
Finland	STUK	Mika Johansson
Finland	Fennovoima	Juho Helander
Finland	STUK	Pia Humalajoki
Finland	VTT	Kim Björkman
Sweden	Westinghouse Electric Sweden AB	Kim Andersson
Sweden	SSM	Niclas Larsson
Sweden	SSM	Stefan Persson
Finland	TVO	Lauri Tuominen
Finland	Fortum	Antti Rautakaulio
Sweden	Solvina AB	Olle Palmqvist
Sweden	Ringhals AB	Dennis Andersson
UK	CRA Consultant	Garth Rowlands
Finland	VTT	Teemu Tommila
Finland	VTT	Atte Helminen
Sweden	ÅF	Henrik Hildesson
Finland	Fortum	Sami Siren
Finland	STUK	Heimo Takala