Reliability Analysis of Digital I&C in Nuclear Power Plants

Jan-Erik Holmberg, Risk Pilot AB, Espoo Finland
Markus Porthin, Tero Tyrväinen, VTT, Espoo, Finland

SYP 2016, Helsinki, November 2, 2016

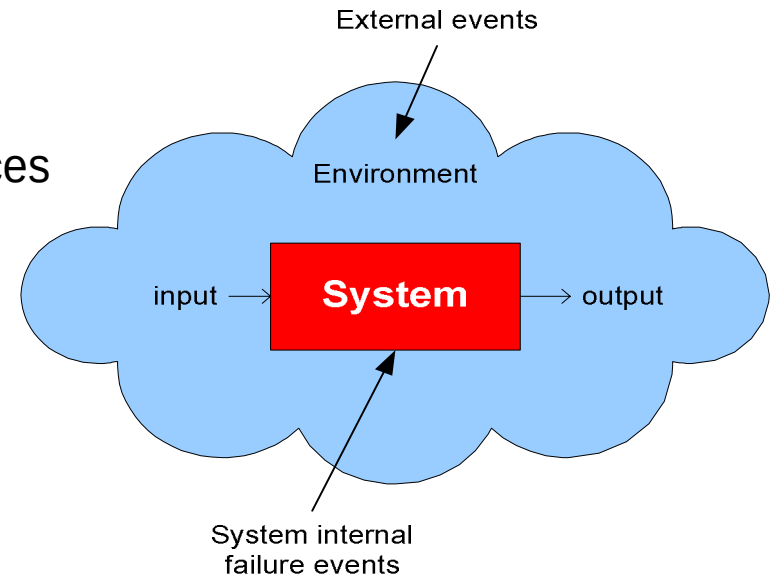
RISK PILOT©
YOUR RISK NAVIGATOR

Scope

- Problem definition
- Results from recent Euratom R&D projects
- Recent achievements in the reliability analysis of digital I&C
- Conclusions

How to demonstrate safety of complex socio-technological system?

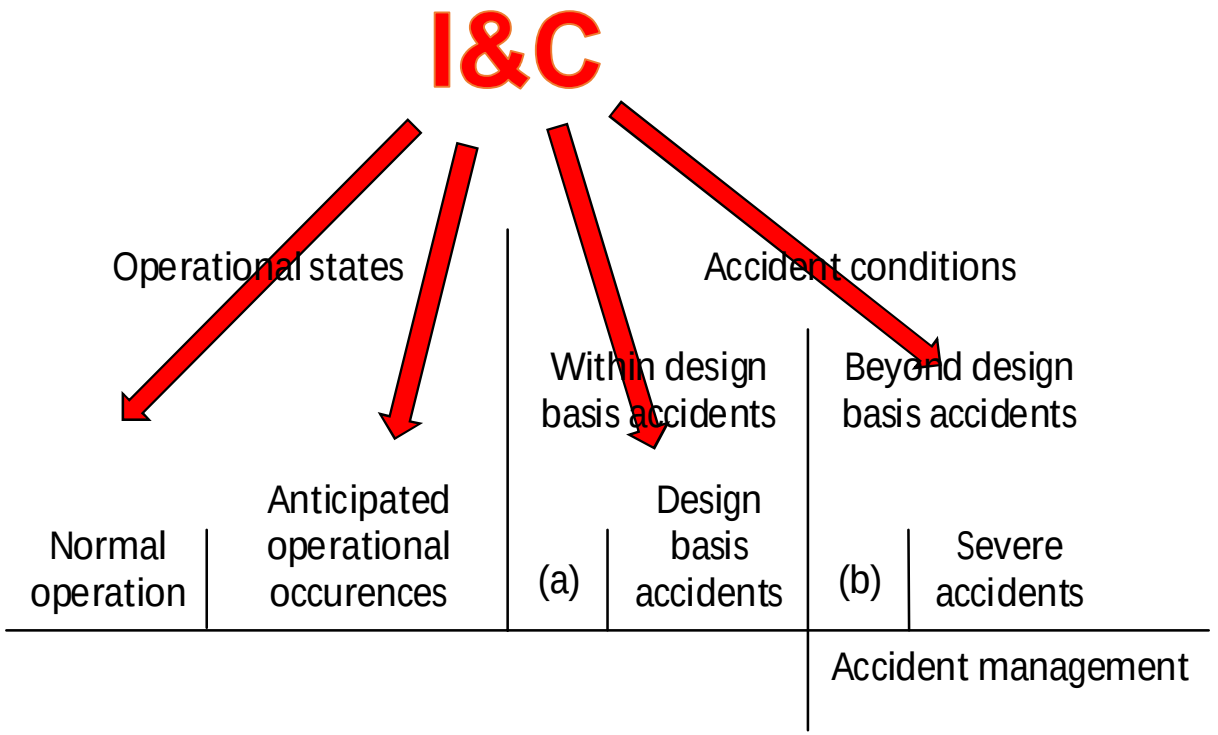
- DSA: Deterministic safety analysis
  - Postulated scenarios may not lead to unwanted consequences
- PRA: Probabilistic risk analysis
  - Quantitative risk criteria shall be met



- I&C consists of several system related to practically all safety functions of a nuclear power plant
  - Practical and justifiable approaches are needed to assess I&C

RISK PILOT©
YOUR RISK NAVIGATOR

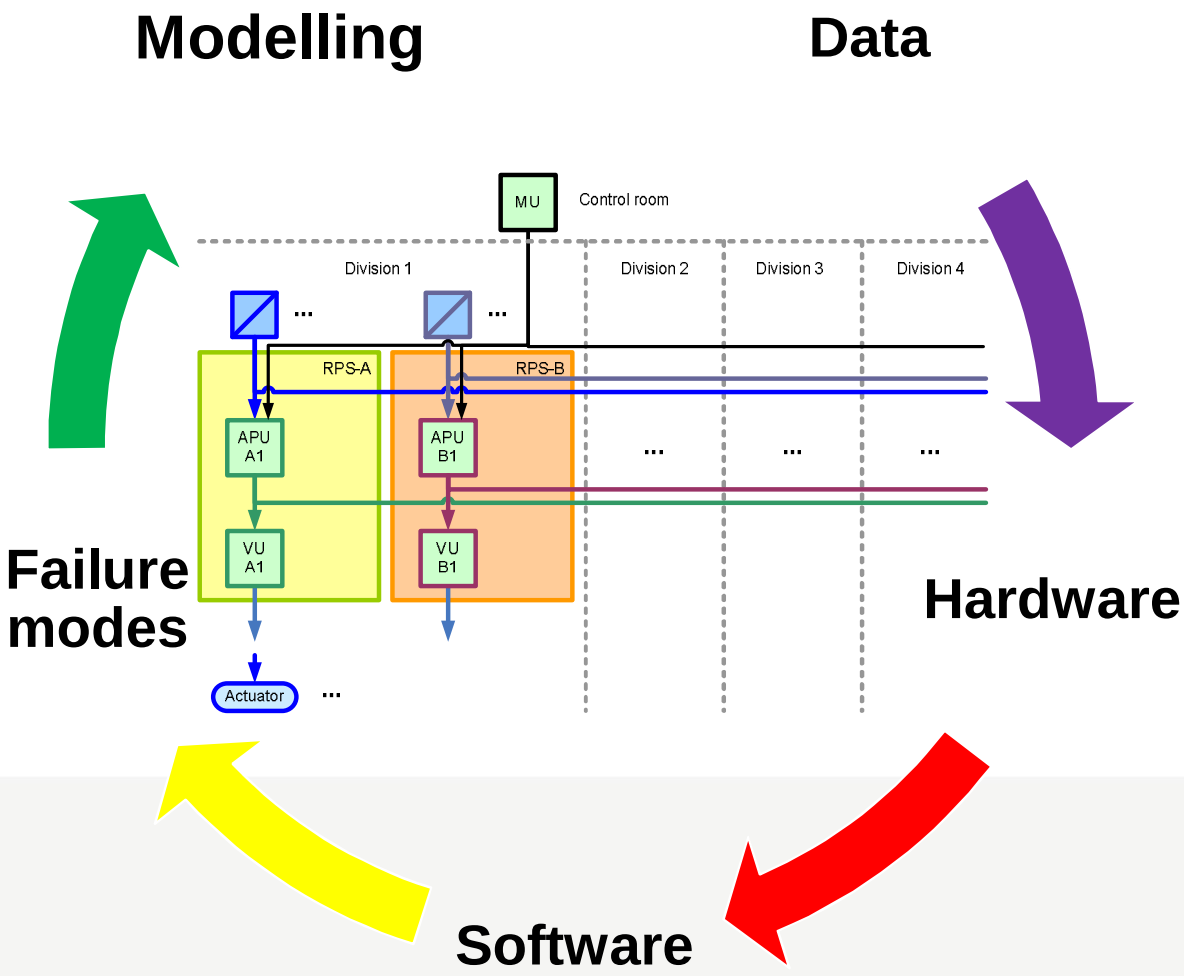
I&C and Defence-in-depth (DiD)



(a) Accident conditions which are not explicitly considered design basis accidents but which are encompassed by them
(b) Beyond design basis accidents without significant core degradation

RISK PILOT©
YOUR RISK NAVIGATOR

Research topics within reliability analysis of digital I&C



RISK PILOT©
YOUR RISK NAVIGATOR

Some history...

ATS **Ydintekniikka n:o 1/1977**

alkanut toiminta oli aluksi tietojen hankkimista, menetelmien kehittämistä ja perusvalmiuden luomista. Projektin puitteissa on tehty huomattavan suuri työ luotettavuustekniikkaa koskevan tietouden ja ajattelutavan kehittämisessä teollisuuteen. Loviisaa koskevia luotettavuusanalyyseja on suoritettu yli 30 kpl (kukin useita henkilötyökuukausia) ja parhaillaan on työn alla eräitä Olkiluotoa koskevia analyyseja. Muista luotettavuus-tekniikan alueella tehdyistä tai tekeillä olevista töistä on tässä syytä mainita

- pohjoismaisen lämmitysreaktorin turvallisuusryhmän työhön osallistuminen
- esitutkimus ydinvoimalaitosten luotettavuustietojärjestelmän toteuttamisesta Suomessa
- ydinvoimalaitosten käytettävyystilastot
- software luotettavuus.

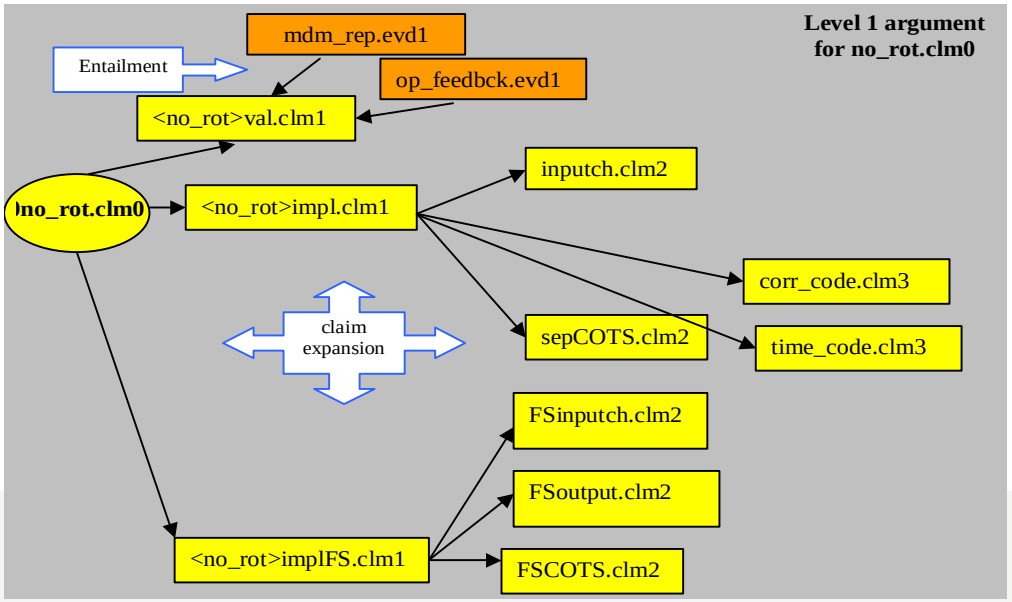
RISK PILOT©
YOUR RISK NAVIGATOR

Further history

- Euratom projects 2001-2003 CEMSIS & BE-SECBS
- Earlier Finnish nuclear safety research programme projects
- Ongoing activities

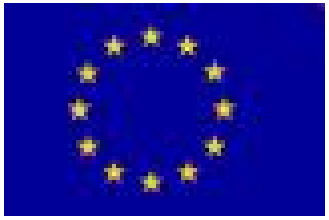
Euratom FP5 project Cost-effective modernisation of systems important to safety (CEMSIS), 2001-2003

- Advice to those involved in control system refurbishment projects
- Guidance on requirements definition, construction of safety justification, and pre-qualification of COTS
- Increased harmonisation of regulatory practises across Europe was stimulated
- www.cemsis.org

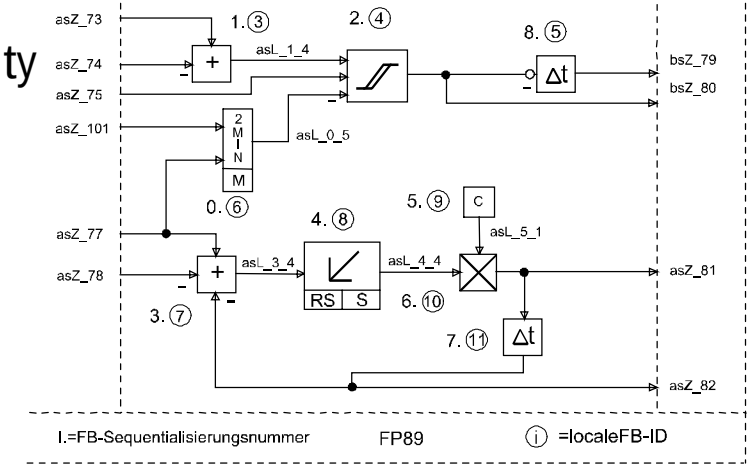


RISK PILOT©
YOUR RISK NAVIGATOR

Euratom FP5 project: Benchmark Exercise on Safety Evaluation of Computer Based Systems (BE-SECBS), 2001-2003



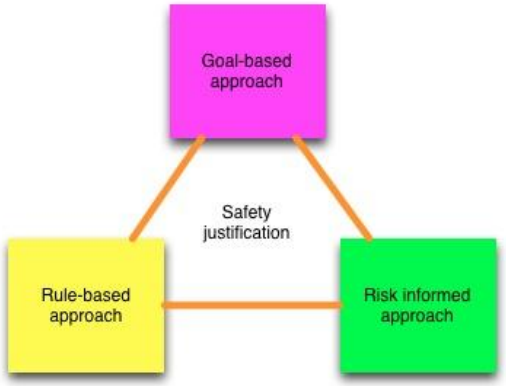
- The different approaches to software safety assessment were compared, making use of same reactor safety system test case
- QA process, Requirements specification, System specification, Detailed design, Source code, Testing, and Quantitative reliability analysis
- Regulatory requirements were based on IEC 60880. In addition relevant assessment tools were used
- Harmonisation of EU approaches, promoting standards' development



RISK PILOT©
YOUR RISK NAVIGATOR

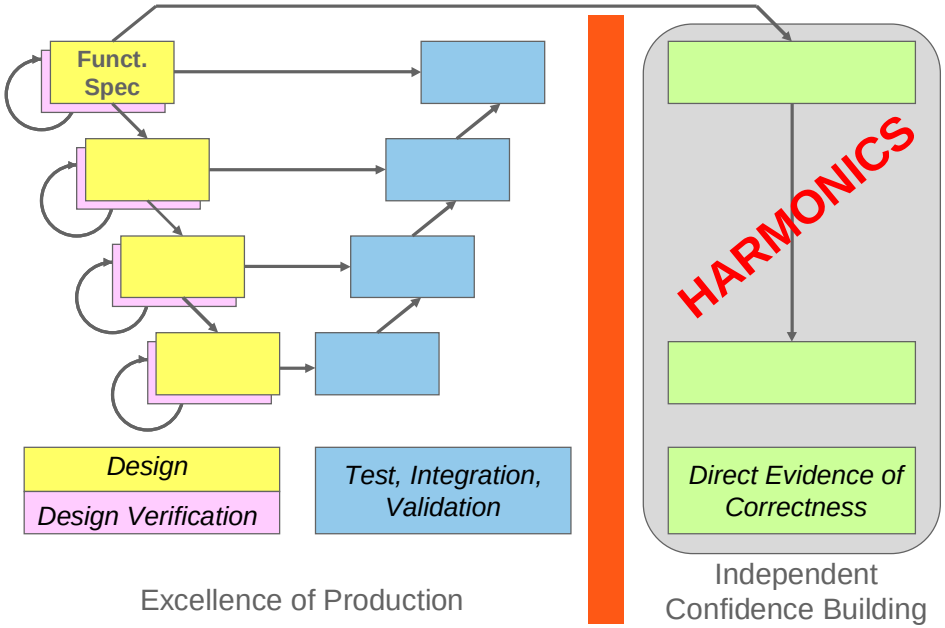
Euratom FP7 project Harmonised Assessment of Reliability of Modern Nuclear I&C software (HARMONICS), 2011-14

- independent V&V of software (IV&V)
- software safety justification
- software reliability assessment

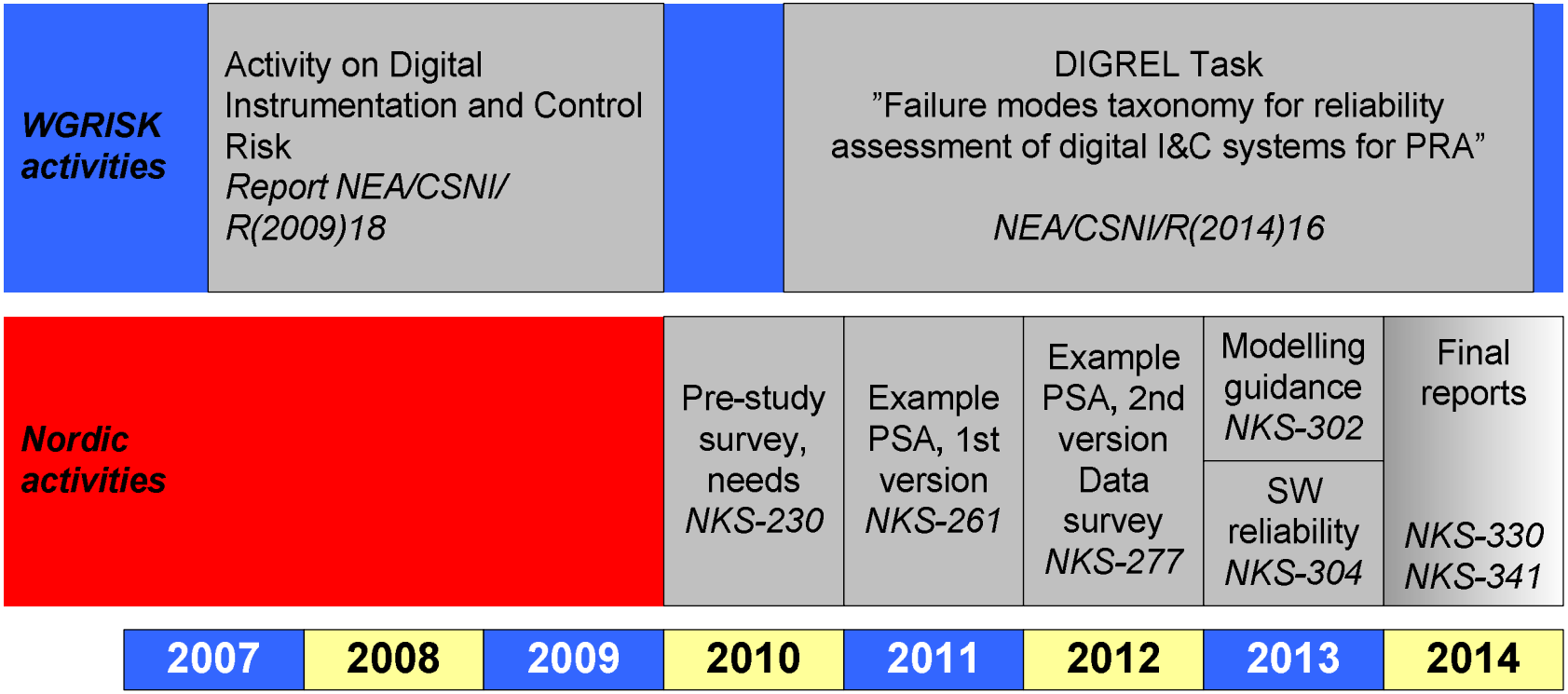


- VTT, EDF, ISTEc, Adelard, SSM

For more information http://harmonics.vtt.fi/



DIGREL (DIGital I&C RELiability) project(s)



- Reports can be loaded from www.nks.org and http://www.oecd-nea.org/nsd/docs/indexcsni.html

RISK PILOT©
YOUR RISK NAVIGATOR

DIGREL failure modes taxonomy

- Failure mode = physical or functional manifestation of a failure
- Failure modes taxonomy is a cornerstone for reliability analysis

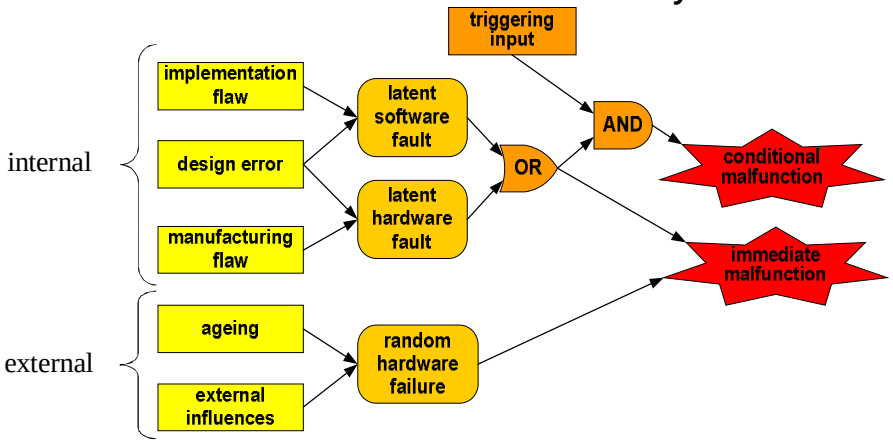
- Functional failure modes
  - Failure to actuate: failure to provide an I&C function when demanded)
  - Spurious actuation: an actuation of an I&C function occurred without a demand

- Hierarchical taxonomy
  - System – subsystem - I&C units – modules – basic components
  - Distinction is made between HW and SW at the module level and below

- NEA/CSNI/R(2014)16

Software reliability

- Failures of software based systems are due to specification errors
  - Latent errors triggered by the context
  - Risk for common cause failures
  - Difficult to apply statistical methods in the reliability assessment



- How to deal with software reliability is very debated => no consensus
- Licensing of software based safety systems has become difficult

RISK PILOT©
YOUR RISK NAVIGATOR

Software reliability

- Software module level failure modes taxonomy
  - fatal failure, non-fatal failure
- Module level is needed for appropriate modelling of dependences
- Different approaches for quantification depending on SW module type
- Combined use of operating experience and indirect evidence

Software modules:
- system software (operating system)
- application function modules
- library functions
- proprietary software modules
- data communication protocol
- data tables
- functional requirements specification (virtual software)

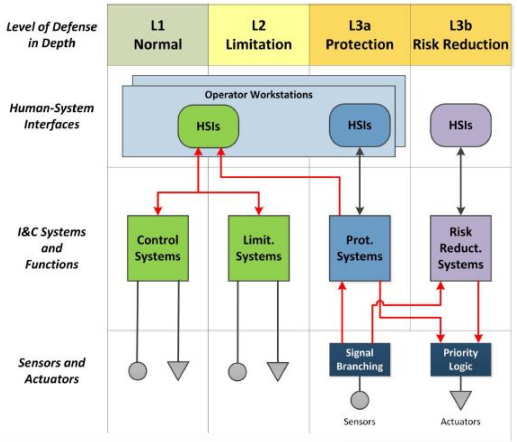
SAFIR/NKS project MODIG (MOdelling of DIGital I&C) 2015-

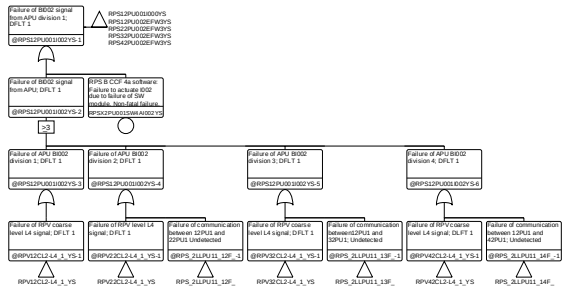
- To get a consensus approach for a reliability analysis of a plant design with digital I&C
- To get improved integration of probabilistic and deterministic approaches in licensing of digital I&C
- To improve failure data collection including software failure probability quantification
- To perform practical application of PSA to compare design alternatives

RISK PILOT©
YOUR RISK NAVIGATOR

What do we try to achieve?

- Better integration between DSA (DiD) and PRA
- More accurate consideration of failure modes
- More accurate consideration of the I&C architecture
- Reasonable approach to model a complex system
- Better justification of reliability numbers





RISK PILOT©
YOUR RISK NAVIGATOR

Conclusions

- Reliability analysis of Digital I&C is an essential part of safety demonstration of modern NPP
  - fulfilment of DiD requirements
  - risk criteria are related to DiD levels 3 and 4
  - integration with deterministic safety analysis
  - interpretation of standards

- Challenges of the analysis depends on the I&C architecture
  - reactor protection system is manageable
  - control systems are much more difficult
  - software reliability assessment remains challenging

- International collaboration important to reach common understanding


Jan-Erik Holmberg
jan-erik.holmberg@riskpilot.fi
+358(0)40 827 6656
RISK PILOT©
YOUR RISK NAVIGATOR