New developments and applications of PRA (NAPRA)

Presentation at SAFIR2022 final seminar

Ilkka Karanta, NAPRA project manager

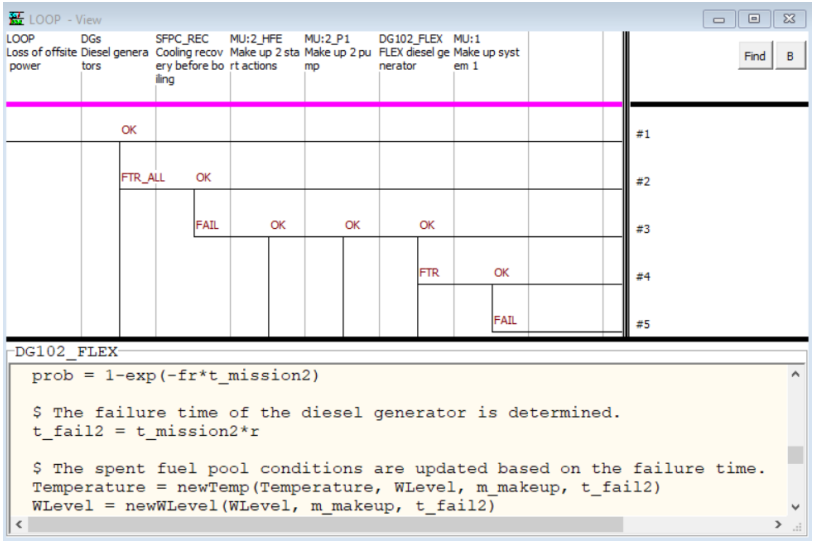
PROSAFE project lays groundwork for PRA with long time windows

- Long time window (> 24 hours) accident scenarios
  - Severe accidents
  - Spent fuel pool (SFP) accidents
  - Some pre core damage scenarios (Fukushima 3)
- PROSAFE project with Nordic partners
  - Literature review and stakeholder survey
    - Information on safe, stable end states, mission times etc.
  - 3 advanced PRA methods compared in SFP analysis
    - Simulation-based event trees (next slide), Markov-based I&AB and graded minimal cut set manipulation approach
    - Approaches to model component repairs in PRA
    - Results consistent
  - HRA methods also compared in SFP analysis
- Results help make long time window models more realistic

Simulation-based PRA for spent fuel pool improves realism of risk estimates

- Simulation-based event tree to analyse top minimal cut sets of a static SFP PRA model
  - Time-dependent conditions of the spent fuel pool are calculated in scripts of FinPSA
  - Time windows for PRA are determined based on spent fuel pool conditions
  - Different possible failure times, repair times and time delays are evaluated in simulations

- More realistic risk estimates were obtained compared to static analysis
  - More realistic definition of mission times
  - Crediting the operation of the cooling/make-up systems before they fail
  - Some repairs are very difficult to model in static manner

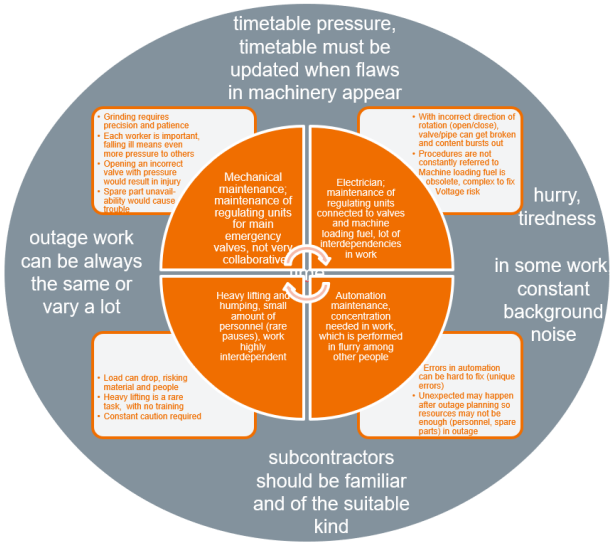


Human reliability analysis (HRA) research to help analysis of planned outages

- Literature survey on dynamic HRA
  - Dynamic HRA can mean
    - Analysis of human reliability in situations that have dynamic aspects
    - Use of methods and tools that enable dynamic modeling (cognitive simulators etc.)
  - State of the art in dynamic HRA methods and tools
- Interviews of main control room operators on dynamic phenomena
  - 2 shift supervisors, 2 reactor operators, 2 turbine operators
  - Asked to imagine given dynamic situations and asked to memorise or contemplate how it would affect the possibility of making an error
    - 6 situations described, furthermore interviewee asked to imagine more
    - Much information was obtained on the kinds of dynamic situations that may be conducive to human error

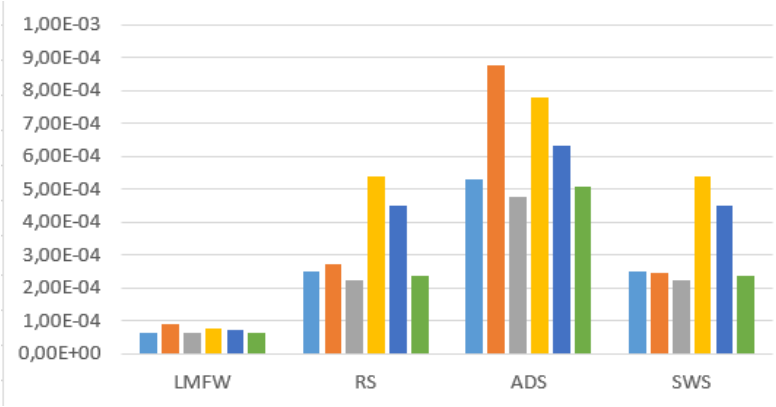
HRA research on planned outages identifies human error possibilities and factors affecting error likelihood

- Literature survey
  - Factors that characterize human error possibilities in outages
  - Outage process (planning, execution, evaluation)
  - Methods, issues and results of outage HRA
- Interviews of outage experts
  - Mechanic, electrician, crane driver, etc.
  - 22 human error possibilities, 22 factors affecting human error identified
  - Results can be used as input in qualitative outage HRA
- Study on heavy lifting
  - Lifting of protective tube unit in focus
  - Previous interview data was reanalysed to identify demanding dynamic features in heavy lifting
  - New interviews were conducted for hierarchical task analysis
  - Results: hierarchical task description, with human error possibilities and factors affecting error
  - Results can be used in outage HRA, and mitigating human error possibilities and factors predisposing to human error



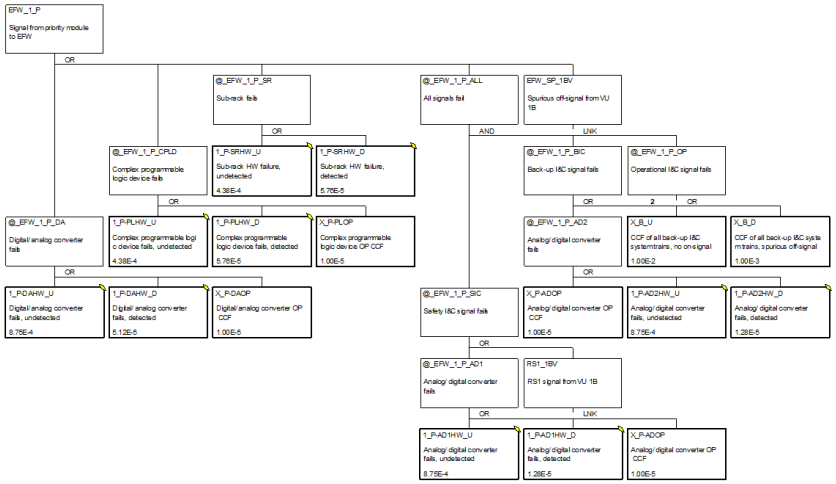
International digital I&C PRA benchmark clarifies modelling issues

- Digital I&C PRA models overly simplified and conservative
  - Modelling and quantification of software failures
  - Modelling of fault-tolerance features
  - Common cause failures: postulation, parameter estimation
- OECD/NEA WGRISK task DIGMAP
  - Benchmark study on PRA modelling of digital I&C, 6 countries
  - PRA models of a fictive reactor protection system
  - VTT's modelling approach: simple fault trees, perform complex computations in the background
  - Conclusions
    - Understanding the diversity of RPS important
    - Identification of common cause failure groups important
    - Level of modeling detail doesn't greatly impact the results
- Results help improve realism of digital I&C PRA models



Other digital I&C PRA studies aid in addressing more specific modelling problems

- Literature survey on common cause failure modelling of digital I&C systems
  - Available methods and data clarified
- Spurious OFF-signals caused by detected failures were implemented in the DIGMAP model
  - In this case, only significance for initiating event frequency
  - Result very sensitive to the fail-safe behaviour and detection coverage parameters
- A fault tree model for a fictive priority unit was developed
  - Failures of the priority unit dominated failures in other systems
  - Spurious OFF-signals from RPS can also be important if they have the priority

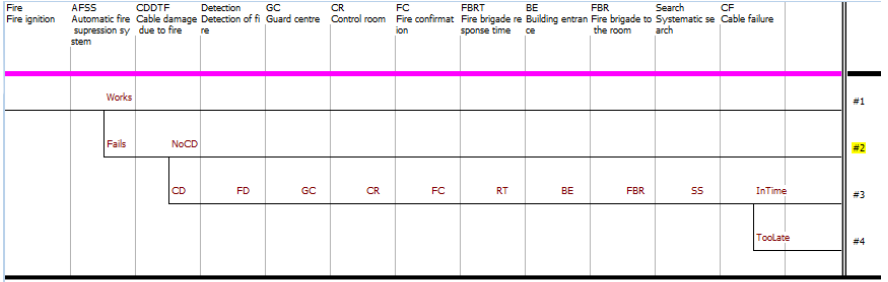


Survey and example help conducting failure tolerance analysis

- Failure tolerance: the system will fill safety requirements even though some parts of it have failed
- Failure tolerance analysis (FTA): a framework to organize individual analyses (e.g. failure modes and effects analysis) to demonstrate that a system is failure tolerant
- Survey
  - Objectives: clarify issues related to FTA, clarify the role of PRA as a part of FTA
  - Findings
    - PRA is not a promising approach to FTA
    - Results of individual FTA analyses have many uses in PRA
- FTA application example
  - Some FTA analyses applied to a cooling division of a fictive boiling water reactor
  - Model checking is a viable and promising approach to certain FTA tasks
- Results may help license applicants and holders in understanding and conducting FTA

A fire PRA model that combines PRA, plant fire dynamics, human aspects

- Simulation-based event tree: reliability aspects and accident progression
- Fire dynamics simulator: results of deterministic fire analyses
- Simulation scripts: model of fire brigade actions (timings)
- Provides an example of a fire PRA model that is
  - integrated
  - dynamic
  - well-structured
- Realistic and cost-effective fire PRA helps risk-informed decision making




```
function real TooLate
  $ Operation time from the detection to the beginning of the systematic search is calculated
  t_oper = t_co+t_v
  if t_cr < t_gc+t_rt+t_be+t_re then
  begin
    t_oper = t_oper+t_gc+t_rt+t_be+t_re
  end
  else
  begin
    t_oper = t_oper+t_cr
  end
```

SMR PRA review provides information on modeling issues and approaches

- SMR PRA literature review
  - PRA should be used for SMRs, as for large reactors, to complement the deterministic approach
  - Especially methods to handle passive features and multi-module issues in PRAs should be investigated or enhanced

- Potential approaches for multi-module PRA reviewed
  - Most multi-unit PRA methods are based on a single-unit model developed using event trees and fault trees
  - Multi-unit PRA methods seem in general quite well applicable to multi-module PRA
    - Analysis details may however differ significantly
  - Also dynamic methodologies have been proposed
    - However, it is a bit unclear why a conventional PRA approach would not be sufficient

VTT

beyond
the obvious

Ilkka Karanta
firstname.surname@vtt.fi
+358 722 4509

@VTTFinland
@your_account

www.vtt.fi