
RISK PILOT©
YOUR RISK NAVIGATOR

Prolonged Available Time and Safe States, PROSAFE, NKS-444

NKS Seminar 2022-05-25, Finlandshuset, Stockholm

Stefan Authén

Vysus Group

Institute for Energy Technology

VTT

RISK PILOT©
YOUR RISK NAVIGATOR

Introduction

- Project performed during 2019 and 2020.
- Project partners: Risk Pilot, Vysus, VTT and IFE
- Financiers: NKS, NPSAG and SAFIR

RISK PILOT©
YOUR RISK NAVIGATOR

PROSAFE Objective

“To improve the quality of safety assessment methods with respect to safe and stable state definition and assessment of long time windows, including human reliability analysis in long time window scenarios, use of dynamic success criteria, crediting repairs and modelling of different time windows.”

Keywords: PSA, HRA, Mission Time, Repair Modelling, Long Time Windows, Safe and Stable State, Dynamic Success Criteria.

RISK PILOT©
YOUR RISK NAVIGATOR

PROSAFE Scope

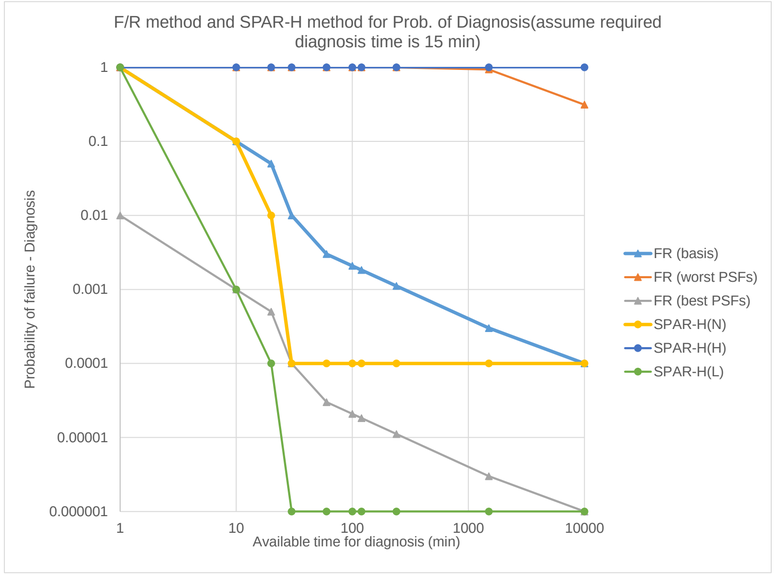
Work package	2019 1st half	2019 2nd half	2020 1st half	2020 2nd half
WP1 Information collection				
WP2 Safe and stable state				
WP3 Methods				
WP4 Pilot studies				
WP5 Meetings, dissemination and management				

- WP1 included literature study and questionnaire to stakeholders
- WP3 and WP4 were further divided in two parts: HRA and Reliability modelling.
- WP4 Pilot studies were performed on PROSAFE example model (DIGREL PSA model expanded to also cover SFP) and Ringhals 4 PSA

RISK PILOT©
YOUR RISK NAVIGATOR

PROSAFE HRA

- WP3 activities:
  - Identify the human actions related to the long time window
  - Define times from HRA perspective: available time, required time, etc.
  - Define the requirements on HRA methods related to the long time window
  - Methods for Qualitative HRA
  - Methods for Quantitative HRA
  - HRA quantification in FLEX context



- WP4 activities:
  - Study the existing human actions (methods, time windows, the other PSFs)
  - Apply developed HRA methods in the pilot study
  - Refine the HRA methods
  - Benchmark with HRA results from existing analysis
  - Dependency analysis for multiple human actions in one MCS
  - Identify potential new human actions, e.g. recovery actions, repair actions and their dependencies with existing actions.
  - Model FLEX human actions

RISK PILOT©
YOUR RISK NAVIGATOR

Conclusions HRA

- Diagnosis HEP (human error probability)
  - In general low when long time windows is considered.
  - Suitable methods exists (F/R and SPAR-H)
  - PSFs (performing shaping factors) exists for most important aspects.

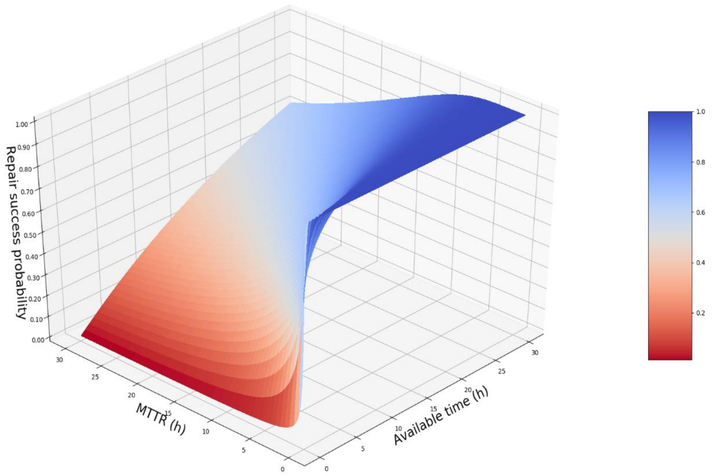
- Execution HEP
  - Is typically higher than diagnosis HEP.
  - F/R method is conservative but has good PSF coverage.
  - THERP method is based on task decomposition, though some tasks do not have suitable HEPs.
  - ASEP method is simplified, conservative version of THERP.

- The MTTR exponential approach is an acceptable choice for repair execution HEP.

PROSAFE Reliability Modelling

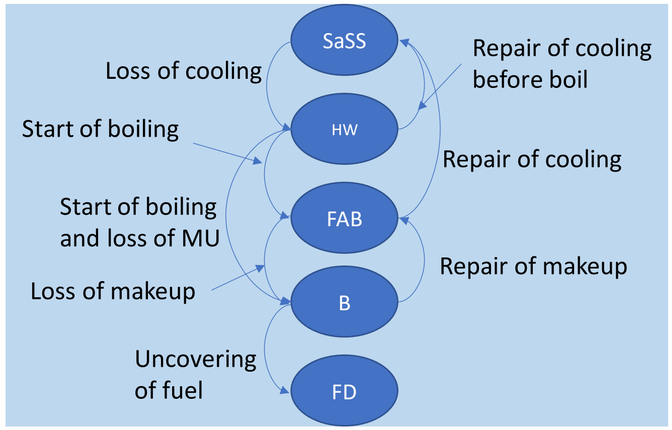
- WP3 activities:
  - Identification of requirements and abbreviations
  - Investigation and ranking of available methods for modelling of repair.
  - Time window modelling with respect to dynamic success criteria and failure data.
  - Failure data for long mission times.
  - Common cause failures: modelling of failure times and repair
  - Consideration of uncertainties

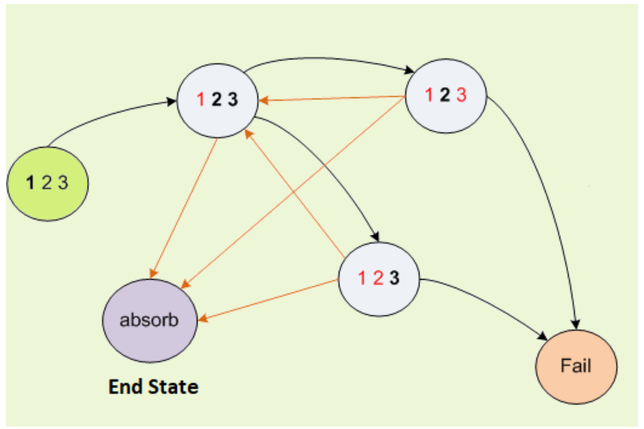
- WP4 activities:
  - Elaboration and hypothesis testing in existing PSAs
  - Development of PROSAFE PSA-model
  - Reliability modelling and analysis with selected approaches/tools
    - Expanded FT/ET
    - RiskSpectrum PSA add-on for Markov-type analysis, I&AB
    - Simulation tool based on FinPSA L2 module
  - Benchmark of evaluated modelling approaches

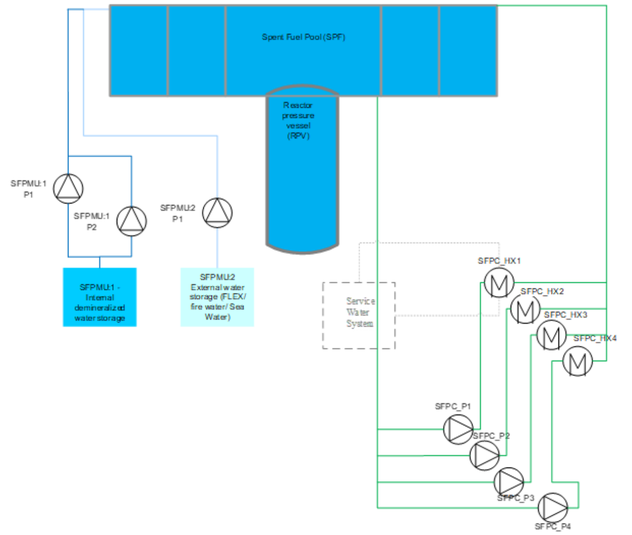


RISK PILOT©
YOUR RISK NAVIGATOR

PROSAFE Reliability Modelling







Initiating Event	Enhanced fault/event tree			Initiators & All Barriers			Simulation-based event tree		
	Static[1)]	EFET	Diff	Static[2)]	I&AB	Diff	Static[3)]	SBET	Diff
EX SNOW	4,4E-07	1,8E-07	-58%	4,2E-07	8,8E-08	-79%	-	-	-
LOOP	2,3E-07	1,0E-09	-100%	2,2E-07	2,6E-10	-100%	1,1E-07	1,1E-10	-100%
TRANS	6,3E-08	6,4E-09	-90%	6,0E-08	4,5E-09	-93%	3,5E-08	1,3E-9	-96%

RISK PILOT©
YOUR RISK NAVIGATOR

Conclusions Reliability Modelling

- All three tested methods are viable.
  - Most of the defined method requirements are met for all methods.
  - Similarity in results, though with increased dynamic dependencies the differences increases.
  - Method of choice depends on scope and complexity of the problem.

- Repair modelling has the greatest impact on PSA results.
  - Modelling of repair for a small number of failures will probably be sufficient in most cases.

- Time dependencies have smaller impact, though still significant.
  - Mainly related to available time for manual actions and repair.
  - Dynamic success criterias are in general of low importance.

- Identification of relevant failures to repair and relevant time windows are relatively straight-forward tasks.

- Timing and repair of CCF:s important to consider, though simple approach is acceptable.
  - “CCF events excluded at first repair”

Possible issues for further work

- Further improve the HRA execution quantification for PROSAFE actions.
- Further investigations on CCF timing issues to improve repair probability estimates.
- Further testing e.g. on PSA level 2
- **Data analysis on the timing elements of MTTR.**
  - Investigation/collection of historical data for repairs, consideration of spares availability, etc.
  - NPSAG project DIOR
- Guidelines for implementation of developed methods

Stefan Authén

stefan.authen@riskpilot.se
+46(0)70 857 00 40

RISK PILOT©
YOUR RISK NAVIGATOR