Risk Pilot
Your Risk Navigator

NKS/DIGREL

Investigation of state-of-the art in Nordic PSA-studies

Stefan Authén
Risk Pilot

Background

- A study of existing PSA:s with digital I&C included in order to identify similarities and differences, i.e. what is present state-of-the art?

- Three PSA:s included:
  - Olkiluoto 1/2, Siemens, ABB I&C design + other
  - Ringhals 1, Siemens I&C design
  - Ringhals 2, Westinghouse I&C design

- Investigation of
  - Level of detail
  - Failure modes
  - Data References

- Investigation not yet completed

Investigation features

- Only three PSA:s and performed by different contractors/personnel
- Different designs
  - Different prerequisites for the PSA:s
    - Different possibilities and boundary conditions
  - Different assumptions and simplifications
    - Detailed study needed in order to estimate impact/result of assumptions and simplifications
      - What appears to be similarly treated may not be and vice versa

PSA Investigation, part 1

Modelling aspects	OL1/2	R1	R2	Comments
Loss of (RPS) Actuation	●	●	●	
Spurious (RPS) Actuation	-	●	-	
Engineered Failure Detection	○	●	●	
Failure of Eng. Failure Detection	○	-	○	
Engineered Fail-Safe Actions	○	●	-	
Degraded Voting Logic	s	●	-	
Intra Division Communication	○	●	●	
Inter Division Communication	○	●	●	
Dynamic Interactions	-	-	-	

● Modelled as standard ○ Modelled as exception, special case or qualitatively s Screened out from the PSA model

PSA Investigation, part 2

Failures and modes	OL1/2	R1	R2	Comments
Hardware Failure Single Comp.	○	●	○	
Hardware Failure Super Comp.	●	-	●	
Hardware CCF Single Comp.	○	●	○	
Hardware CCF Super Comp.	●	-	●	
Software Failure	s	s	○	For sensitivity analysis
Software CCF Single Comp.	s	s	s	
Software CCF Super Comp.	●	●	s	
Undetected Failure	●	●	●	
Detected Failure	●	●	○	
Spurious Failure	-	s	s	
Corr. Maint. Single Comp.	○	○	○	
Corr. Maint. Super Comp.	○	●	●	

● Modelled as standard ○ Modelled as exception, special case or qualitatively s Screened out from the PSA model

PSA Investigation, part 3

Hardware Components	OL1/2	R1	R2	Comments
Processor, Super Comp.	●	-	●	
Processor	-	●	-	
Communication Module	-	●	●	
Digital Input/Output Module	-	●	○	
Digital Input/Output Channel	-	●	-	
Analog Input/Output Module	-	●	-	
Analog Input/Output Channel	-	●	-	
Signal Conditioning Module	-	●	-	
Subrack	-	●	-	
Misc. Modules	●	●	●	
Watchdog	-	-	○	
Controller Module for Continuous Closed-loop Control	-	-	-	

● Modelled as standard ○ Modelled as exception, special case or qualitatively s Screened out from the PSA model

PSA Investigation, part 4

- Hardware failure data
  - OL1/2: Supplier data
  - R1: Supplier data
  - R2: Supplier data
- Hardware CCF parameters
  - OL1/2: Eng. Judge
  - R1: IEC 61508 / Supplier
  - R2: IEC 61508 / RAB
- Software CCF
  - OL1/2: Supplier data / Eng. Judge
  - R1: Supplier data
  - R2: -

Reflections

- Three different approaches in the three PSA:s
  - Independently developed by different contractors/personnel
  - No real consensus anywhere

- State-of-the art may need to consider differences in I&C design and reactor types (BWR/PWR)
  - Level of detail, critical failure modes, consideration of fail-safe design