I&C modelling in FinPSA software

Tero Tyrväinen, Ilkka Niemelä (STUK)
VTT Technical Research Centre of Finland
I&C modelling in FinPSA

- I&C modelling feature of FinPSA is based on RELVEC algorithm.
- Models are built with success logic.
- Models are written in text files with simple and compact expressions.
- Fault trees can contain links to control tasks of I&C model and I&C model can include links to top events of fault trees.
- I&C models are automatically transformed into fault trees.
I&C Model Based on RELVEC Algorithm

RELVEC - A TOOL FOR CONTROL SYSTEM RELIABILITY ANALYSIS
Technical Research Centre of Finland, VTT, Electrical Engineering Laboratory, Espoo, Finland.
(Received for publication 7th July 1983)

Developed in 1980s for reliability analysis and design of distributed control systems:

- Oil refinery
- Paper mills
- Power plants
- Hazardous plants
- Satellite earth station
- Offshore
- PRA fault tree analysis

Background is communication matrix, expressed with vectors

RELVEC = RELiability VECTors
Isolation = Interface

Event tree / Fault tree model

Control tasks

I&C system model

Support functions
Communication: Path Nets

Control tasks define functional entities inside the I&C system.

Path nets of control tasks are created and converted to fault trees.

\[
\begin{align*}
\text{control system} & : D1 + D2 = C1 \\
& D3 + D4 = C2 \\
& D5 = C3 \\
& D6 + D7 = C4 \\
& D8 + D9 = C5 \\
& C1 + C2 + C3 = B1 \\
& C4 + C5 = B2 \\
& B1 + B2 = A1 \\
\text{interface to instrumentation} & : FC1 = D2 \\
& LT1 = D4 \\
& P1 = D5 \\
& K1 = D8 \\
& MON1 = D9 \\
\text{control tasks} & : \text{Manual}_P1 = MON1 \times K1 \times P1 \\
& L\_TANK1 = FC1 \times LT1 \\
& \text{Water} = P1 \times L\_TANK1 \times \text{CONTR} \\
& \text{CONTR} = MON1 \times K1
\end{align*}
\]
Interface: Fault trees ↔ I&C Model

- Fault tree gate type LIC links to control tasks.

- Fault tree of the task is created and linked to LIC gate
  - Extremely fast routines, practically no delay in fault tree construction.
  - I&C fault tree is automatically created also when minimal cut set is double-clicked

- I&C model links to fault tree using fault tree name
  \[ \text{Rack01} = \text{Pow01} \times \text{Rack01} \times \text{DC24V}\_Tr\_A \]
Example PSA model

- Fictive and simplified nuclear power plant (BWR).

- 4-redundant safety systems.

- Fault trees for AC power system, component cooling water system, emergency core cooling system, emergency feedwater system, depressurisation valve system, residual heat removal system, service water system and main feedwater system.

- Event trees for large LOCA, loss of main feedwater, transient and loss-of-offsite power.

- I&C systems are modelled using the I&C modelling feature of FinPSA.
Fault tree of ECC system pump

A link to an I&C-model.

Representing the failure of the start signal.
ECC pump start signal I&C model

Functioning water level sensor and functioning communication link required.

Links to top events of fault trees.

Positive voting result from APU and functioning communication link required.

Positive voting result and functioning digital output module required.
I&C model is automatically transformed into fault tree
Fail-safe principles

- How to handle detected failures in I&C system?

- When a failure is detected, the signal can be replaced by a default value of 0 or 1.

- Fixed binary variables can be used to control the fail-safe principle.

\[
\text{RPS10PU00110002} \_4 \_I = \text{RPS40PU001VL004} \_F \_S \times \text{RPS14LAPULAPU4} \_F \_S \times (\text{RPS40PU001VL004} \_E \_S \times \text{RPS14LAPULAPU4} \_E \_S) + \text{RPS0PU00110002} \_V \_DE
\]

- If the first and second detected failures are handled differently, the modelling is much more challenging.
Implementation in FinPSA

Integrated to PRA data base:
- CCFs between I&C model parts
- Hazard Table mapping
  - Fires, floods, seismic…

Display and analyze fault tree of any control task

Natural import & export of model
Summary

- I&C model is isolated from PRA model via interface
  - Simple communication system model
  - Compact and computationally efficient representation
  - Not much new as such

- Isolation makes it possible to develop I&C modeling as a part of a full-scale PRA model
  - I&C model development can take its own course

- Text-based model offers freedom of future development
  - Expansion of modelling language
    - Dynamic properties
References

VTT - 70 years of technology for business and society