Risk Assessment

Francesco Di Maio, PhD

Dipartimento di Energia
Politecnico di Milano
(Very) Short BIO

Education

- **B.Mus** Conservatory degree (2006)
- **M.Sc** in Nuclear Engineering, Politecnico di Milano (2006)
- **Double-PhD** in Energy and Nuclear Science and Technology
  Politecnico di Milano and Tsinghua University (China) (2010)
Laboratory of Analysis of Signal and Analysis of Risk (LASAR)

Research context

Vulnerability & Risk

Reliability & Availability

Logistics & Operations

Maintenance & PHM
Laboratory of Analysis of Signal and Analysis of Risk (LASAR)

Research context

Vulnerability & Risk

Reliability & Availability

Logistics & Operations

Maintenance & PHM

- Energy distribution systems
- Nuclear Power Plants (NPPs)
- Renewable Energy
- Oil&Gas (O&G)
- Transportation
- …
Large amount of deployed algorithms (more than 25 yrs R&D)

- Logic and Physical modeling: FT, ET, …
- MC Simulation: SS, LS, PF, …
- Classification, regression and prediction: NN, DL, RC, SVM, …
- Uncertainty and sensitivity analysis: VD, KL, HD, …
- Optimization: GA, DE
- Decision making: PDA, RL, …

FT = Fault Tree; ET = Event Tree; MC = Monte Carlo; SS = Subset Sampling; LS = Line Sampling; PF = Particle Filtering; NN = Neural Network; DL = Deep Learning; RC = Reservoir Computing; SVM = Support Vector Machine; VD = Variance Decomposition; KL = Kullback-Leibler; HD = Hellinger Distance; PDA = Portfolio Decision Analysis; RL = Reinforcement Learning; GA = Genetic Algorithms; DE = Differential Evolution

- Energy distribution systems
- Nuclear Power Plants (NPPs)
- Renewable Energy
- Oil&Gas (O&G)
- Transportation
- …
Risk Assessment: Foundations

Risk is conditioned on Knowledge

\[ Risk = (S, p, c ; \mathcal{K}) \]

Possible Accident Scenarios

Knowledge Available

Consequences

Uncertainty

Risk is conditioned on Knowledge
Probabilistic Risk Assessment (PRA): Foundations

Systematic framework of analysis aimed at identifying accidental scenarios \((S_i)\) and quantifying their consequences \((C_i)\) and probabilities \((P_i)\)

System:

Initiating Event (IE)

\[ P(A) \]

\[ P(B) \]

\[ P(A) \]

\[ P(B) \]

\[ P(A) \]

\[ P(B) \]

\[ P_1 \]

\[ P_2 \]

\[ P_3 = P(A) P(B) \]

\[ P_i = \prod P(event) \]
Condition monitoring $\rightarrow$ Condition Based PRA (CB-PRA)

**System:**

IE → A → B

Initiating Event (IE)

Plant configuration change

Failure probability

$t = \tau$

$t = 0$

$t = \tau$

Time ($t$)

(PRA)
Condition monitoring $\rightarrow$ Condition Based PRA (CB-PRA)

System:

IE
Initiating Event (IE)

A
Plant configuration change

B

Failure probability

$\Phi(t)$

Time ($t$)

System:

$A$

$B$

$A'$

$B$

$t=0$

$t=\tau$

Time ($t$)

Failure probability

$\Phi(t)$

$\mathcal{K}$
Condition monitoring → Condition Based PRA (CB-PRA)

Initiating Event (IE)

Plant configuration change

Failure probability

System:

$P(A'|\Phi(t))$

$P(B|\Phi(t))$

$P(\bar{A}'|\Phi(t))$

$P(\bar{B}|\Phi(t))$

$S_1 \text{ OK} \quad P_1$

$S_2 \text{ OK} \quad P_2$

$S_3 \text{ Failure} \quad P_3$

Time (t)

Failure probability

$\Phi(t)$

$K$

Time (t)

$P(A) \text{ at } t=\tau$

$P(B) \text{ at } t=\tau$

$P(\bar{A}) \text{ at } t=\tau$

$P(\bar{B}) \text{ at } t=\tau$

$P_1, P_2, P_3$

$S_1, S_2, S_3$

$P_1, P_2, P_3$
Condition monitoring ® Condition Based PRA (CB-PRA)

IE

Initiating Event (IE)

P(A'|Φ(t))

P(\overline{A}'|Φ(t))

P(B|Φ(t))

P(\overline{B}|Φ(t))

System:

A

B

\[
\begin{align*}
P(A'|\Phi(t)) & \\
P(B|\Phi(t)) & \\
P(\overline{A}'|\Phi(t)) & \\
P(\overline{B}|\Phi(t)) & \\
\end{align*}
\]

\[
\begin{align*}
P(A'|\Phi(t)) & \\
P(B|\Phi(t)) & \\
P(\overline{A}'|\Phi(t)) & \\
P(\overline{B}|\Phi(t)) & \\
\end{align*}
\]

Failure probability

Plant configuration change

(CB-PRA)

(PRA)

\[
\begin{align*}
P(\text{Failure}|\Phi(t)) & \\
\end{align*}
\]

decision making (life extension, maintenance, operation, ...)

POLITECNICO MILANO 1863
Condition Based PRA (CB-PRA): remarks

ADVANTAGES:

• Aging and degradation are considered
• Variable operational conditions are considered
• Effects of plant configurations changes are considered

LIMITATIONS:

• Requires optimal placing of sensors
• Computationally burdensome
  o Data management
  o Data mining
Case study: CB-PRA for Spontaneous Steam Generator Tube Rupture (SGTR) accident scenario
Case study: CB-PRA for Spontaneous Steam Generator Tube Rupture (SGTR) accident scenario

- Spontaneous SGTR
- Operators Depressurization
- Refuelling Water Storage Tank (RWST)
- Reactor Coolant System (RCS)

<table>
<thead>
<tr>
<th>End State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe</td>
</tr>
<tr>
<td>Core Damage</td>
</tr>
<tr>
<td>Core Damage</td>
</tr>
<tr>
<td>ATWS</td>
</tr>
</tbody>
</table>

Diagram showing the containment and core damage scenarios.

[Diagram of a nuclear reactor with highlighted areas indicating core damage and containment.]
Case study: CB-PRA for Spontaneous Steam Generator Tube Rupture (SGTR) accident scenario

Spontaneous rupture of a SG tube due to the Stress Corrosion Cracking (SCC) phenomenon, during normal operating condition.

| Spontaneous SGTR | Operators
Depressurization | Refuelling Water Storage Tank | Reactor Coolant System | End State |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IE</td>
<td>T</td>
<td>RWST</td>
<td>RCS</td>
<td>Safe</td>
</tr>
</tbody>
</table>

IE

Core Damage

Core Damage

ATWS
Case study: CB-PRA for Spontaneous Steam Generator Tube Rupture (SGTR) accident scenario

Spontaneous rupture of a SG tube due to the Stress Corrosion Cracking (SCC) phenomenon, during normal operating condition.

Objective:
\[ P(\text{Core Damage} \mid \theta(t)) = \text{Core Damage Frequency} (\theta(t)) \]
The SCC failure mechanism: crack onset model

ONSET
Crack onset probability is modelled by a Weibull distribution

\[ \Phi(t) = \text{Crack length} \]

\[ \text{Onset probability} \]

\[ \text{Time [inspection cycle]} \]

\[ \text{Time (t)} \]
The SCC failure mechanism: crack onset & formation model

**ONSET**
Crack onset probability is modelled by a Weibull distribution

**FORMATION**
Crack onset length is modelled by a normal distribution

\[ \Phi(t) = \text{Crack length} \]
The SCC failure mechanism: crack propagation model

**ONSET**
Crack onset probability is modelled by a Weibull distribution.

**FORMATION**
Crack onset length is modelled by a normal distribution.

**PROPAGATION**
Propagation is modelled with the Scott model (that depends on the operating conditions, such as pressure).

Propagation is modelled with the Scott model (that depends on the operating conditions, such as pressure).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Minimum</th>
<th>Nominal</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k_0$ (MPa/m)</td>
<td>$2.5 \times 10^{-4}$</td>
<td>$2.8 \times 10^{-2}$</td>
<td>$3.1 \times 10^{-2}$</td>
</tr>
<tr>
<td>$\beta$</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>$F$</td>
<td>$1.07$</td>
<td>$1.16$</td>
<td>$1.25$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Nominal Value</th>
<th>Uncertainty (uniform distribution)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside diameter $d$</td>
<td>$22.23$ mm</td>
<td>$\pm 0.5$ mm</td>
</tr>
<tr>
<td>Thickness $t$</td>
<td>$1.27$ mm</td>
<td>$\pm 12.5%$</td>
</tr>
<tr>
<td>Nominal pressure difference $\Delta P_{\text{nom}}$</td>
<td>$8.3$ MPa</td>
<td>$\pm 1$ MPa</td>
</tr>
</tbody>
</table>
The overall SCC Model

**ONSET**
Crack onset probability is modelled by a Weibull distribution

**FORMATION**
Crack onset length is modelled by a normal distribution

**PROPAGATION**
Propagation is modelled with the Scott model (that depends on the operating conditions, such as pressure)

Crack growth parameters (Lewandowski, 2013; Czadz and *Marko*, 1995).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Minimum</th>
<th>Nominal</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha$</td>
<td>$2.5 \times 10^{-8}$</td>
<td>$2.8 \times 10^{-2}$</td>
<td>$3.1 \times 10^{-2}$</td>
</tr>
<tr>
<td>$K_a$ (MPa/W)</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>$\beta$</td>
<td>1.07</td>
<td>1.16</td>
<td>1.26</td>
</tr>
<tr>
<td>$F$</td>
<td>–</td>
<td>0.91</td>
<td>–</td>
</tr>
</tbody>
</table>

Tubes parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Nominal Value</th>
<th>Uncertainty (uniform distribution)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside diameter $d$</td>
<td>22.23 mm</td>
<td>± 0.5 mm</td>
</tr>
<tr>
<td>Thickness $t$</td>
<td>1.27 mm</td>
<td>± 12.5%</td>
</tr>
<tr>
<td>Nominal pressure difference $\Delta P_{\text{nom}}$</td>
<td>8.3 MPa</td>
<td>± 1 MPa</td>
</tr>
</tbody>
</table>
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions

Simulate the stochastic crack evolutions throughout the following operation time (predictive modeling)
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions

Operational variation (e.g. power demand)

Total pressure

Tube rupture critical length

$\Phi(t) = \frac{\text{Crack length}}{\text{Pressure}}$

Simulate the stochastic crack evolutions throughout the following operation time (predictive modeling)

Calculate the probability of exceeding the tube critical length

Operational variation (e.g. power demand)

Total pressure

Tube rupture critical length

$\Phi(t) = \frac{\text{Crack length}}{\text{Pressure}}$

NRC plugging threshold

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions

Operational variation (e.g. power demand)

Total pressure

Tube rupture critical length

$\Phi(t) = \frac{\text{Crack length}}{\text{Pressure}}$

NRC plugging threshold

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions

Operational variation (e.g. power demand)

Total pressure

Tube rupture critical length

$\Phi(t) = \frac{\text{Crack length}}{\text{Pressure}}$

NRC plugging threshold

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions

Operational variation (e.g. power demand)

Total pressure

Tube rupture critical length

$\Phi(t) = \frac{\text{Crack length}}{\text{Pressure}}$

NRC plugging threshold

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions

Update the SGTR frequency (upon plant configuration changes (i.e. number of plugged tubes))
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Operational variation (e.g. power demand)

Total pressure

Tube rupture critical length

\[ \Phi(t) = \text{Crack length} \]

Decide whether to plug or not the tube

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions

Simulate the onset, formation and propagation of cracks in the tubes bundle
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Operational variation (e.g. power demand)

Total pressure

Tube rupture critical length

NRC plugging threshold

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions

Simulate the onset, formation and propagation of cracks in the tubes bundle
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions

Decide whether to plug or not the tube

Operational variation (e.g. power demand)

Total pressure

Tube rupture critical length

NRC plugging threshold
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions
The SGTR frequency estimation by CB-PRA approach

Set the nominal operating conditions and evaluate the critical crack length

Simulate the onset, formation and propagation of cracks in the tubes bundle

Plug tubes exceeding the NRC plugging threshold, and update the operating conditions

Periodically update the SGTR frequency (upon plant configuration changes (i.e. number of plugged tubes))
The SGTR frequency estimation by CB-PRA approach

- Physical modeling: Stress Corrosion Cracking degradation (Scott model)
- Simulation: MC Simulation embedding Predictive Modeling
- Logic modeling: Event Tree (ET), with condition based update of events probabilities

## RISK ASSESSMENT

<table>
<thead>
<tr>
<th>SAFETY</th>
<th>SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Considers components/systems <strong>failures</strong> and human <strong>errors</strong></td>
<td>Considers (cyber) <strong>attacks</strong> by humans</td>
</tr>
</tbody>
</table>
## Cyber → Risk assessment for safety and security

### RISK ASSESSMENT

<table>
<thead>
<tr>
<th>SAFETY</th>
<th>SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Considers components/systems <strong>failures</strong> and human <strong>errors</strong></td>
<td>Considers (cyber) <strong>attacks</strong> by humans</td>
</tr>
<tr>
<td>Probabilities and consequences on functionality</td>
<td>Uncertainty and consequences on functionality</td>
</tr>
</tbody>
</table>

*Cyber → Risk assessment for safety and security*
### Cyber → Risk assessment for safety and security

#### RISK ASSESSMENT

<table>
<thead>
<tr>
<th>SAFETY</th>
<th>SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Considers components/systems <strong>failures</strong> and human <strong>errors</strong></td>
<td>Considers (cyber) <strong>attacks</strong> by humans</td>
</tr>
<tr>
<td>Probabilities and consequences on functionality</td>
<td>Uncertainty and consequences on functionality</td>
</tr>
</tbody>
</table>

#### INTEGRATED RISK ASSESSMENT for safety and security
Risk assessment for safety and security: the GTST-MLD

The Goal Tree (GT) Success Tree (ST) Master Logic Diagram (MLD) hierarchically decomposes the system safety goal function into sub-functions, accomplished by the system components, and impaired by dysfunctional aspects.

Results:

\[ P(\text{Goal fulfillment}) \]

Time (t)
The Goal Tree (GT) Success Tree (ST) Master Logic Diagram (MLD) hierarchically decomposes the system safety *goal function* into sub-functions, accomplished by the system components, and impaired by dysfunctional aspects.
The Goal Tree (GT) hierarchically decomposes the system safety goal function into $n_f$ sub-functions.
The ST describes the interactions between the *physical elements* of the system.
The Influencing Factors (IFs) are the dysfunctional aspects (i.e., components failures & cyber attacks) that can prevent the system to achieve the goal function.
The relationships between GT, ST and IFs are represented by the Master Logic Diagram (MLD).

Risk assessment for safety and security: the GTST-MLD
The GTST-MLD Risk assessment for safety and security: remarks

ADVANTAGES:

• Intuitive construction of relationships between events
  • no need to enumerate all failure scenarios
• Capability of dealing with scarcity of data in defining events probability

LIMITATIONS:

• Expert-based weights assignment
• Computationally burdensome
  o Data management
Case study: The Advanced Lead-cooled Fast Reactor European Demonstrator (ALFRED)

ALFRED parameters values, at full power nominal conditions.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter description</th>
<th>Value</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_{Th}$</td>
<td>Thermal power</td>
<td>$300 \times 10^6$</td>
<td>W</td>
</tr>
<tr>
<td>$h_{CR}$</td>
<td>Height of control rods</td>
<td>12.3</td>
<td>cm</td>
</tr>
<tr>
<td>$T_{L,hot}$</td>
<td>Coolant core outlet temperature</td>
<td>480</td>
<td>°C</td>
</tr>
<tr>
<td>$T_{L,cold}$</td>
<td>Coolant SG outlet temperature</td>
<td>400</td>
<td>°C</td>
</tr>
<tr>
<td>$\Gamma$</td>
<td>Coolant mass flow rate</td>
<td>25,984</td>
<td>kg s$^{-1}$</td>
</tr>
<tr>
<td>$T_{fbed}$</td>
<td>Feedwater SG inlet temperature</td>
<td>335</td>
<td>°C</td>
</tr>
<tr>
<td>$T_{steam}$</td>
<td>Steam SG outlet temperature</td>
<td>450</td>
<td>°C</td>
</tr>
<tr>
<td>$P_{SG}$</td>
<td>SG pressure</td>
<td>$180 \times 10^5$</td>
<td>Pa</td>
</tr>
<tr>
<td>$G_{water}$</td>
<td>Feedwater mass flow rate</td>
<td>192</td>
<td>kg s$^{-1}$</td>
</tr>
<tr>
<td>$G_{att}$</td>
<td>Attemperator mass flow rate</td>
<td>0.5</td>
<td>kg s$^{-1}$</td>
</tr>
<tr>
<td>$k_v$</td>
<td>Turbine admission valve coefficient</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>$P_{Mech}$</td>
<td>Mechanical power</td>
<td>$146 \times 10^6$</td>
<td>W</td>
</tr>
</tbody>
</table>

Parameters of PI controllers.

<table>
<thead>
<tr>
<th>PI</th>
<th>Control loop</th>
<th>Controller parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PI_1$</td>
<td>$T_{steam}$ (°C)</td>
<td>$G_{at} (kg s^{-1})$</td>
</tr>
<tr>
<td>$PI_2$</td>
<td>$P_{Mech}$ (W)</td>
<td>$h_{CR}$ (cm)</td>
</tr>
</tbody>
</table>

Case study: The Advanced Lead-cooled Fast Reactor European Demonstrator (ALFRED)

ALFRED parameters values, at full power nominal conditions.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter description</th>
<th>Value</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_{Th}$</td>
<td>Thermal power</td>
<td>30010^6</td>
<td>W</td>
</tr>
<tr>
<td>$h_{CR}$</td>
<td>Height of control rods</td>
<td>12.3</td>
<td>cm</td>
</tr>
<tr>
<td>$T_{L,hot}$</td>
<td>Coolant core outlet temperature</td>
<td>480</td>
<td>°C</td>
</tr>
<tr>
<td>$T_{L,cold}$</td>
<td>Coolant SG outlet temperature</td>
<td>490</td>
<td>°C</td>
</tr>
<tr>
<td>$\Gamma$</td>
<td>Coolant mass flow rate</td>
<td>25.984</td>
<td>kg s^{-1}</td>
</tr>
<tr>
<td>$T_{feed}$</td>
<td>Feedwater SG inlet temperature</td>
<td>335</td>
<td>°C</td>
</tr>
<tr>
<td>$T_{steam}$</td>
<td>Steam SG outlet temperature</td>
<td>450</td>
<td>°C</td>
</tr>
<tr>
<td>$P_{SG}$</td>
<td>SG pressure</td>
<td>18010^5</td>
<td>Pa</td>
</tr>
<tr>
<td>$G_{water}$</td>
<td>Feedwater mass flow rate</td>
<td>192</td>
<td>kg s^{-1}</td>
</tr>
<tr>
<td>$G_{att}$</td>
<td>Attemperator mass flow rate</td>
<td>0.5</td>
<td>kg s^{-1}</td>
</tr>
<tr>
<td>$k_v$</td>
<td>Turbine admission valve coefficient</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$P_{Mech}$</td>
<td>Mechanical power</td>
<td>14610^6</td>
<td>W</td>
</tr>
</tbody>
</table>

Parameters of PI controllers.

<table>
<thead>
<tr>
<th>PI</th>
<th>Control loop</th>
<th>Control variable</th>
<th>Controller parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>PI</td>
<td>$T_{steam}$ (°C)</td>
<td>$G_{att}$ (kg s^{-1})</td>
<td>$K_{ref}$</td>
</tr>
<tr>
<td>PI</td>
<td>$P_{Th}$ (W)</td>
<td>$h_{CR}$ (cm)</td>
<td>$310^{-1}$</td>
</tr>
</tbody>
</table>

The GTST-MLD for the ALFRED control system

- GT
- ST
- MLD
- IFs

ALFRED critical parameters at nominal conditions
- Steam temperature control
- Steam generator pressure control
- Cold leg lead temperature control
- Thermal power control
The GTST-MLD for the ALFRED control system
The GTST-MLD for the ALFRED control system

COMPONENTS FAILURES

**Sensors**: bias, drift, wider noise, freezing

**PIs**: proportional gain change, integral gain change, set point change

**Actuators**: stuck

**CYBER-ATTACKS**

- Doorknob rattling
- STUXNET virus
- Key logger
- Man in the middle
- Denial of Service (DoS)
- Message spoofing
- Replay
- Buffer overflow
The GTST-MLD for the ALFRED control system
The integrated safety and security risk assessment: results

- Physical modeling: Modelica (Dymola)
- Logic modeling: GTST-MLD (Goal-Tree Success Tree Master Logic Diagram)
- MC Simulation for uncertainty propagation through the GTST-MLD

The integrated safety and security risk assessment: results

- Physical modeling: Modelica (Dymola)
- Logic modeling: GTST-MLD (Goal-Tree Success Tree Master Logic Diagram)
- MC Simulation for uncertainty propagation through the GTST-MLD

Conclusions & Perspectives

\[ \text{Risk} = (S, p, x; \mathcal{K}) \]
Conclusions & Perspectives

\[ Risk = (S, p, x; \mathcal{K}) \rightarrow CB-PRA \]

LIMITATIONS:

- Requires optimal placing of sensors
- Computationally burdensome
  - Data management
  - Data mining
Risk = (S, p, x; K) → CB-PRA

LIMITATIONS:

- Requires optimal placing of sensors
- Computationally burdensome
  - Data management
  - Data mining

CONCLUSIONS & PERSPECTIVES

- Value of Information (VOI) for optimal placing of sensors
- Artificial Intelligence (AI) for predictive modeling
Conclusions & Perspectives

\[ \text{Risk} = (S, p, x; \mathcal{K}) \rightarrow \text{GTST-MLD} \]

Limitations:
- Expert-based weights assignment
- Computationally burdensome
  - Data management

- Simulation-based weights assignment
- Computationally burdensome
- Artificial Intelligence (AI) for surrogate modeling
Conclusions & Perspectives

\[ \text{Risk} = (S, p, x; K) \]

Component failures

(Malicious) external events

External events

- energy grid
- smart meters
- electric car
- smart factory
- smart city