The Open-PSA Initiative

Towards a New Generation of Models and Tools for Probabilistic Safety Assessment

Prof. Antoine B. Rauzy
Director of Chair Blériot-Fabre
Centrale-Supélec / SAFRAN
Paris - France
Agenda

- Probabilistic Safety Assessment: a Status
- The Open-PSA Initiative
- The Open-PSA Model Exchange Format (2.0d)
- The Open-PSA Model Exchange Format (3.0)
- Open-PSA Tools
- To Do List
Probabilistic Safety Assessment: a Status
Any **industrial system** presents a **risk** for itself, its users or its environment. Eventually, the only question is to decide whether this risk is acceptable, i.e. if **severe accidents** have a sufficiently low **probability**. **Probabilistic Safety/Risk Assessment** is used to take such a **decision**.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>IEC 61508 Risk Matrix</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Negligible</strong></td>
</tr>
<tr>
<td><strong>Frequent</strong></td>
<td>&gt; $10^{-3}$</td>
<td>Undesirable</td>
</tr>
<tr>
<td><strong>Probable</strong></td>
<td>$10^{-3}$ to $10^{-4}$</td>
<td>Tolerable</td>
</tr>
<tr>
<td><strong>Occasional</strong></td>
<td>$10^{-4}$ to $10^{-5}$</td>
<td>Tolerable</td>
</tr>
<tr>
<td><strong>Remote</strong></td>
<td>$10^{-5}$ to $10^{-6}$</td>
<td>Acceptable</td>
</tr>
<tr>
<td><strong>Improbable</strong></td>
<td>$10^{-6}$ to $10^{-7}$</td>
<td>Acceptable</td>
</tr>
<tr>
<td><strong>Incredible</strong></td>
<td>$\leq 10^{-7}$</td>
<td>Acceptable</td>
</tr>
</tbody>
</table>
Most of the Probability Safety Assessments rely on the Fault Trees/Event Trees technology:

- Mature software
- Large models (typically 2000 Basic Events in Nuclear PSA models)
- Large data bases of experience feedback

Some other formalisms:

- Block Diagrams
- Markov Chains
- Dynamic Fault Trees, BDMP
The Open-PSA Initiative

Typical Assessment Scenarios

- Event Trees
- Block Diagrams
- Fault Trees
- FMEA & Reliability Data
- Dynamic Fault Trees, BDMP
- Minimal Cutsets (Failure Scenarios)
- Reliability Indicators
- Calculations
- Markov Chains
Current PSA/PRA Situation

We have:
- A rather mature technology
- **Which is here for long years**

... but
- Models are hard to master, to check for completeness, to maintain...
- **Models are tool-dependent**
- Calculation engines have flaws due to uncontrolled approximations
- Tools do not provide all expected features

Issues for next generation of PSA/PRA software
- Quality assurance of calculations
- **Portability of models**
- Clarity, completeness and documentation of models
- Visualization of results
- ...

The Open-PSA Initiative
The Open-PSA Initiative
What Is Open-PSA?

- Informal group of PSA analysts, researchers and software developers

- Statement of Purpose:
  “We hope to provide an open and transparent public forum to disseminate information, independently review new ideas, and spread the word. We want to emphasize an openness which will lead to methods and software with higher quality, lead to better understanding of PSA models, encourage peer review, and allow the transportability of models and methods.”

- Practical Objectives:
  - Definition of a standard representation format for PSA models
  - Development of tools
Open-PSA Activities

- Workshops
  - Workshop Goesgen (Switzerland), 06/12/2007, KKG
  - Working Group, Paris (France), 07/19/2007, EdF
  - Hearing ACRS/NRC, Washington DC (USA), 10/02/2007
  - Workshop Washington DC (USA), 10/03/2007, EPRI
  - Workshop Osaka (Japan), 11/13-14/2007, NEL
  - Workshop Vienna (Austria), 12/07-08/2007, IAEA
  - Workshop Madrid (Spain), 02/28-29/2008 CSN
  - Workshop Paris (France), 10/21/2008, Dassault Systèmes
  - Workshop Paris (France), 10,11/12/2012, EdF

- Website
  - www.open-psa.org
Open-PSA Model Exchange Format (2.0d)

Towards an International Standard
Why Do We Need a Standard Representation Format?

- Reduce tool dependency
- Have a better confidence in approximations (quality insurance)
- Cross check calculations
- Develop new calculation engines
- Design new model browsers and safety monitors
- Review and document (existing) models
- Clarify (unify?) modeling methodologies
- Call external tools (Level 2 PSA)
- Extend fault trees/events trees formalism
- ...

The Open-PSA Initiative
The Open-PSA Architecture

- Industry Data
- Model Authoring Tools
- Model Browsers
- Calculation Engines
- Safety Monitors
- Cutsets Browsers

Standard Representation Format

Data Bases, Versioning, Configurations
The Open-PSA Initiative

Requirements

- It should be possible to cast any existing model.

- The role of each element should be clearly identified and have an unambiguous semantics.

- The format should be easy to embed in existing tools and easy to extend.

... XML grammar
Methodology

- We considered models built with the main tools available on the market
  - Cafta, Saphire, RiskSpectrum, Riskman, Fault Tree free...
  - US, Japanese and European PSA
- We made of taxonomy of all syntactic categories we found in these models
  - Gates, basic events, house events, sequences...
- We gave to each category a formal operational semantics
- We designed a XML representation of categories
The Open-PSA Initiative

Five Layers Architecture

- **Report Layer**
  - Results of calculation...
- **Event Tree Layer**
  - Event trees, initiators, sequences, consequences
- **Extra-Logical Layer**
  - CCF-groups, delete terms, exchange events...
- **Fault Tree Layer**
  - Fault Trees, gates, basic events, house events
- **Stochastic Layer**
  - Probability distributions, parameters

Available at www.open-psa.org
The Open-PSA Initiative

- Consequence-terms
- Initiator-sets
- Initiators
- Rules
- Named-rules
- Branches
- States
- Functional-events
- CCF-group
- Delete-terms
- Recovery-rules
- Event-trees
- Extra-logical layer
- Fault-trees
- Formulae
- Gates
- House-events
- Basic-events
- Expressions
- Parameters
- Fault tree layer
- Stochastic layer
- Event trees layer
Declarations of Fault Trees

〈define-fault-tree name="FT1" 〉
  〈define-gate name="Tank Overflow" 〉
    〈or〉
      〈gate name="Loss In Flow Regulation" 〉
        〈basic-event name="Out Valve Failure" 〉
      〈/gate〉
    〈/or〉
  〈/define-gate〉
  〈define-gate name=" Loss In Flow Regulation " 〉
    〈and〉
      〈basic-event name="In Valve Failure" 〉
      〈basic-event name="Sensor Failure" 〉
    〈/and〉
  〈/define-gate〉
  〈define-basic-event name="In Valve Failure" 〉
    〈exponential〉
      〈parameter name="lambdaValve" 〉
    〈/exponential〉
  〈/define-basic-event〉
... 
〈/define-fault-tree〉
## Validation of the Format

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizer</td>
<td>IMdR(*)</td>
<td>France</td>
</tr>
<tr>
<td>Manager</td>
<td>Dassault Systèmes</td>
<td>France</td>
</tr>
<tr>
<td>Participants</td>
<td>Tractabel</td>
<td>Belgium</td>
</tr>
<tr>
<td></td>
<td>Areva</td>
<td>France</td>
</tr>
<tr>
<td></td>
<td>EdF</td>
<td>France</td>
</tr>
<tr>
<td></td>
<td>IRSN</td>
<td>France</td>
</tr>
<tr>
<td></td>
<td>Risa</td>
<td>Germany</td>
</tr>
<tr>
<td></td>
<td>KKB</td>
<td>Germany</td>
</tr>
<tr>
<td></td>
<td>JRC</td>
<td>Italy</td>
</tr>
<tr>
<td></td>
<td>CSN</td>
<td>Spain</td>
</tr>
<tr>
<td></td>
<td>KKG</td>
<td>Swiss</td>
</tr>
<tr>
<td></td>
<td>KKL</td>
<td>Swiss</td>
</tr>
<tr>
<td></td>
<td>NOK</td>
<td>Swiss</td>
</tr>
<tr>
<td></td>
<td>Relcon ScanPower</td>
<td>Sweden</td>
</tr>
</tbody>
</table>

(*) Institute for Risk Management (non for profit organization)
Open-PSA Model Exchange Format (3.0)
Objectives & Constraints

- Correct defaults of the version 2.0d:
  - Simplify the scope of variables
  - Simplify/clarify the notion of container
  - Simplify descriptions of probability distributions
  - Simplify/clarify processing rules

- Extend the format:
  - User defined probability distributions
  - Block Diagrams
  - Multiphase Markov Chains with Rewards

- Markov chains can be very big (up to millions of states and transitions), so it must be possible to implement efficient parsers.
  - Indices rather than identifiers (O(1) vs O(log n))
  - SAX rather than DOM
The Open-PSA Initiative

Modules

- **Event Trees**
  - Event Trees, Initiating Events, Consequences...

- **Fault Trees**
  - Basic Events, House Events, gates, Minimal Cutsets...

- **Stochastic Equations**
  - Probability distributions, parameters, random-deviates...

- **Processing Rules**
  - Common Cause Groups, delete terms, recovery rules...

- **Block Diagrams**
  - Blocks

- **Markov Chains**
  - Chains, states, transitions, rewards, matrices, missions...

The diagram illustrates the relationships between different modules and their associated techniques and concepts.
Fault Trees: Example

```
<fault-tree name="FT1">
  <define-gate name="Tank Overflow">
    <or>
      <gate name="Loss In Flow Regulation" />
      <basic-event name="Out Valve Failure" />
    </or>
  </define-gate>
  <define-gate name="Loss In Flow Regulation">
    <and>
      <basic-event name="In Valve Failure" />
      <basic-event name="Sensor Failure" />
    </and>
  </define-gate>
  <define-basic-event name="In Valve Failure">
    <exponential>
      <parameter name="lambdaValve" />
    </exponential>
  </define-basic-event>
  ...
</fault-tree>
```
Declarations: Conventions

- Containers:
  
  <fault-tree name="FT1"> ... </fault-tree>

- Variables that can be referred directly outside the container in which they are defined:
  
  <define-gate name="PumpFailure"> ... </define-gate>
  
  <gate name="PumpFailure" />

- Other variables:
  
  <transition number="33"> ... </transition>

- Terms:
  
  <or> ... </or>

- Rules:
  
  <delete-term> ... </delete-term>

- Files
  
  <?xml version="1.0" ?>
  
  <!DOCTYPE open-psa>
  
  <open-psa>
    ... 
  </open-psa>
Fault Trees: Variables & Containers
Minimal Cutsets are stored in the TSV format (loadable by spreadsheet editors)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Order</th>
<th>Probability</th>
<th>Contribution</th>
<th>Basic Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>3.03E-07</td>
<td>0.0888725</td>
<td>B1090 B725 B798</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>1.26E-07</td>
<td>0.0370669</td>
<td>B1313 B1633 B2283 B361 B798</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>1.14E-07</td>
<td>0.0333475</td>
<td>B1090 B1313 B798 B879</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>1.06E-07</td>
<td>0.0310406</td>
<td>B1313 B1633 B2014 B2104 B548</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>9.46E-08</td>
<td>0.0277825</td>
<td>B1313 B1633 B2014 B2283 B548</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>7.59E-08</td>
<td>0.0222808</td>
<td>B1633 B2283 B725 B740 B798</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>7.34E-08</td>
<td>0.0215527</td>
<td>B1771 B1785</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>6.82E-08</td>
<td>0.0200333</td>
<td>B1090 B1276 B1313 B798</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>6.60E-08</td>
<td>0.0193688</td>
<td>B1244 B1787</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>5.30E-08</td>
<td>0.015566</td>
<td>B1244 B1455</td>
</tr>
<tr>
<td>...</td>
<td>....</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>....</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Block Diagrams: Container, Variables & Terms

- **Block Diagram name**
- **0..* Internal Block**
  - **1 Composition Operation**
  - **1..* Reference to Block**
- **0..* Basic Block**
  - **0..1 Stochastic Expression**
  - **1..* Parallel Composition**
  - **1..* Series Composition**
  - **Voter min**
- **0..* Parameter**
- **0..* Common Cause Group**
- **0..* Substitution**
- **Reference to Event**
<block-diagram name="System">
  <define-internal-block name="B1">
    <series>
      <internal-block name="B2" />
      <basic-block name="B3">
        <voter min="2">
          <basic-block name="BB5" />
          <basic-block name="BB6" />
          <basic-block name="BB7" />
        </voter>
      </basic-block>
    </series>
  </define-internal-block>
  <define-internal-block name="B2">
    <parallel>
      <basic-block name="BB1" />
      <basic-block name="BB2" />
      <basic-block name="BB3" />
    </parallel>
  </define-internal-block>
  <define-basic-block name="BB1">
    ...
  </define-basic-block>
</block-diagram>
Stochastic Expressions: Terms

- Stochastic Expression
  - Ground Expression
    - Built-in Random Deviate
    - User-Defined Random Deviate
  - Random Deviate
    - 0..*
    - 0..*
  - Probability Distribution
    - Built-In Probability Distribution
    - User-Defined Probability Distribution

Mission-Time Expression
<define-basic-event name="Pump1Failure">
  <sub>
    <float value="1.0" />
    <exp>
      <mul>
        <neg>
          <parameter name="lambda" />
        </neg>
        <mission-time />
      </mul>
    </exp>
  </sub>
</define-basic-event>

<define-basic-event name="Pump2Failure">
  <exponential>
    <parameter name="lambda" />
  </exponential>
</define-basic-event>

<define-parameter name="lambda">
  <float value="1.23e-4" />
</define-parameter>
Stochastic Expressions: Example

```xml
<define-parameter name="lambda">
  <switch>
  <case>
    <eq>
      <parameter name="StressLevel" />
      <int value="1" />
    </eq>
    <float value="1.0e-4" />
  </case>
  <case>
    <eq>
      <parameter name="StressLevel" />
      <int value="2" />
    </eq>
    <float value="2.5e-4" />
  </case>
  <float value="1.0e-3" />
  </switch>
</define-parameter>
```
User Defined Probability Distributions

<probability-distribution interpolation="lines">
  <point time="0" probability="0" />
  <point time="730" probability="0.135842" />
  <point time="1460" probability="0.253231" />
  <point time="2190" probability="0.354674" />
  <point time="2920" probability="0.442337" />
  <point time="3650" probability="0.518091" />
  ...
</probability-distribution>
<common-cause-group name="pumps" model="MGL">
    <members>
        <basic-event name="pumpA" />
        <basic-event name="pumpB" />
        <basic-event name="pumpC" />
        <basic-event name="pumpD" />
    </members>
    <factors>
        <float value="0.10" />
        <float value="0.20" />
        <float value="0.30" />
    </factors>
    <distribution>
        <exponential>
            <parameter name="lambda" />
            <mission-time />
        </exponential>
    </distribution>
</common-cause-group>
<recovery-rule>
  <condition>
    <basic-event name="valve-V-broken"/>
    <basic-event name="overpressure-pipe-P"/>
  </condition>
  <action>
    <basic-event name="failure-action-A"/>
  </action>
</recovery-rule>

<exchange-events>
  <or>
    <house-event name="magnitude-5"/>
    <house-event name="magnitude-6"/>
    <house-event name="magnitude-7"/>
  </or>
  <basic-event name="small-leak-pipe-P"/>
  <basic-event name="large-leak-pipe-P"/>
</exchange-events>
Elements to be represented:

- Markov chains
  - states, transitions
- Transition matrices to transfer from one chain to the other
  - transitions
- Rewards to associate a real value to each state of each chains
  - chains, states
- Missions that describes how phases are chained
Before first test duration $\theta$

<table>
<thead>
<tr>
<th></th>
<th>W1</th>
<th>F1</th>
<th>R1</th>
</tr>
</thead>
<tbody>
<tr>
<td>W0</td>
<td>$1-\gamma$</td>
<td>$\gamma \times (1-\sigma)$</td>
<td>$\gamma \times \sigma$</td>
</tr>
<tr>
<td>F0</td>
<td>$1-\sigma$</td>
<td>$\sigma$</td>
<td></td>
</tr>
</tbody>
</table>

During tests duration $\pi$

<table>
<thead>
<tr>
<th></th>
<th>W1</th>
<th>F1</th>
<th>R1</th>
</tr>
</thead>
<tbody>
<tr>
<td>W1</td>
<td>$1-\omega_1$</td>
<td>$\omega_1$</td>
<td></td>
</tr>
<tr>
<td>F1</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R1</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Between tests duration $\tau$

<table>
<thead>
<tr>
<th></th>
<th>W1</th>
<th>F1</th>
<th>R1</th>
</tr>
</thead>
<tbody>
<tr>
<td>W2</td>
<td>$1-\gamma$</td>
<td>$\gamma \times (1-\sigma)$</td>
<td>$\gamma \times \sigma$</td>
</tr>
<tr>
<td>F2</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R2</td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
<Markov-chain name="During tests" states="4" transitions="4">
  <state number="1" name="W1" />
  <state number="2" name="F1" />
  <state number="3" name="S1" immediate="true" />
  <state number="4" name="R1" />
  <transition number="1" source="1" target="2" parameter="lambdaStar" />
  <transition number="2" source="3" target="1">
    <sub>
      <float value="1.0" />
      <parameter name="omega2" />
    </sub>
  </transition>
</Markov-chain>
Markov Chains: Matrices

\[
\begin{array}{ccc}
W1 & F1 & R1 \\
W0 & 1-\gamma & \gamma \times (1-\sigma) & \gamma \times \sigma \\
F0 & 1-\sigma & \sigma \\
\end{array}
\]

<Markov-matrix name="First test" source="Before first test" target="During test" transitions="5">
  <transition number="1" source="1" target="1">
    <sub>
      <float value="1.0"/>
      <parameter name="gamma"/>
    </sub>
    ... 
  </transition>
</Markov-matrix>
Markov Chains: Reward

<Markov-reward name="Unavailable">
  <chain name="Before first test">
    <state number="2" value="1.0" />
  </chain>
  <chain name="During test">
    <state number="2" value="1.0" />
    <state number="4" value="1.0" />
  </chain>
  <chain name="Between test">
    <state number="2" value="1.0" />
    <state number="4" value="1.0" />
  </chain>
</Markov-reward>
<Markov-mission name="My Mission">
  <chain name="Before first test" parameter="theta"/>
  <matrix name="First test" />
  <loop>
    <chain name="During test" parameter="pi" />
    <matrix name="End test" />
    <chain name="Between tests" parameter="tau" />
    <matrix name="Start test" />
  </loop>
</Markov-mission>
Open-PSA Tools
Tools

- XFTA: a solver for Fault Trees
  - MCS based engine (BDD solver coming)
  - All probabilistic calculations (including importance factors, sensitivity analyses, SIL)
  - Freeware, version 1.2 available on my web page (OpenPSA 2.0d)
- XMRK: a solver for Multiphase Markov Chains with Rewards
  - Freeware, version 1.0 scheduled for end of 2014
- OpenPSA Toolkit
  - Set of small tools around the OpenPSA format
  - Open source (Python), version 1.0 scheduled fall 2014
- Andromeda
- ArbreAnalyste
- Simfia (?)
- SATODEV Tools (?)
- Others (RiskSpectrum, Relex ?, ItemToolkit ?)
Arbre Analyste

- Fault Tree Tool
- Developed par E. Clément
- Freeware (http://www.arbre-analyste.fr/)
- XFTA inside
- will be presented at Lambda-Mu 2014
Andromeda

- Fault Trees, Event Trees, Sequence Diagrams (and potentially others)
- Developed by Thomas Friedlhuber (formally EdF and now EdgeMind)
- Status to be determined, a priori Freeware
- XFTA Inside
- Don’t miss Thomas PhD Defense September the 26th 2014
Andromeda

Variant management, model comparison
Andromeda

Sequence Diagrams
To Do List

- Documentation
- Community
- Tools
• Write the new version of the report (Antoine, 2014 October)
• Reviewers needed
Community

- Community manager needed
  - Organize regular meetings
  - Update contact list
- Web site: web master needed

- Publications
Networking

- Establish formal contacts with software editors and major players
  - Relcon, Relex, ItemSoftware, Satodev
  - Safety authorities: ASN, NRC...
  - Large groups: EdF, Airbus, Safran...
  - Professional associations: IMdR...

- Go to standardization?
  - W3C? ISO?