MODEL-DRIVEN SAFETY
ANALYSIS OF CRITICAL
SYSTEMS

Nataliya Yakymets
**CRITICAL SYSTEM** is a system whose failure may result in death or serious injury to people, or damage to equipment or environmental harm.

The Fukushima Daiichi nuclear disaster
11 March 2011
<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61508</td>
<td><strong>Generic</strong> Standard on Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems</td>
</tr>
<tr>
<td>ARP-4761</td>
<td>Guidelines and Methods for Conducting the Safety Assessment Process on Civil <strong>Airborne Systems</strong> and Equipment</td>
</tr>
<tr>
<td>ISO 26262</td>
<td>Functional Safety standard, &quot;<strong>Road vehicles</strong> – Functional safety&quot;</td>
</tr>
<tr>
<td>ISO 10218</td>
<td><strong>Robots and robotic devices</strong> -- Safety requirements for industrial robots</td>
</tr>
</tbody>
</table>
SYSTEM SAFETY ASSESSMENT is a systematic approach to the analysis of risks resulting from hazards that can affect humans, the environment, and mission assets.

TYPICAL SAFETY ASSESSMENT METHODS

- Hazard and Risk Analysis
  - Preliminary Hazard Analysis (PHA)
  - System Hazard Analysis (SHA)
  - HAZOP
  - ...
- Failure Mode Effects & Criticality Analysis (FMECA)
- Reliability Block Diagram (RBD)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Markov Analysis
SAFETY LIFE-CYCLE

SAFETY STANDARDS
- IEC 61508 generic standard on functional safety
- ISO 26262 "Road vehicles – Functional safety"

SAFETY METHODS
- PHA
- SHA
- HAZOP
- ... 
- FTA
- FMEA
- Markov Analysis
- RBD
- ETA

SAFETY ANALYSIS
- Hazard Analysis
- Preliminary System Safety Assessment
- System Safety Assessment

DEVELOPMENT
- Concept & Requirements
- Design & Optimization
- Implementation
- Integration & Test
- Validation
- Acceptance & Maintenance

SAFETY ANALYSIS DEVELOPMENT
SYSTEM ENGINEERING

- Large usage of Model-Based approaches & techniques
- Complete description of the system architecture

CLASSICAL SAFETY ANALYSIS

- Performed mostly manually
- Time consuming, costly, high probability of errors
- No strong links between system engineering and safety analysis

Need for safety analysis assistance!
MODEL-BASED SAFETY ANALYSIS

UML/SYSML
- Flexible and expressive semantics
- Global overview of architecture

PAPYRUS
- UML2 standard
- Domain Specific Languages
- Customizable
  - Reuse UML concepts
  - Use any notations: diagrams, tables, text, symbols

Save time by modeling system before building a physical prototype
Sophia targets early phases of system life-cycle

METHODOLOGY

System Modeling

Propagate Results to the Model

Safety Modeling & Annotation

Result Generation

Analysis

RobotML models

FMEA Tables

AltaRica formal model

Fault Tree

Safety Annotation via Profile

Fault Tree Analysis

Property verification

Failure Mode & Effects Analysis

System Hazard Analysis

Requirement Engineering

Preliminary Hazard Analysis

Fault Tree Analysis

Boolean expressions

Transformation

SysML model to formal languages: AltaRica, NuSMV

State Machines

Fault Trees

FME(C)A tables

Copyright CEA ©

1) How to manage a hierarchy of complex systems?
   - Coherence of dysfunctional behavior on different levels
   - Iterative process

2) How to express dysfunctional behaviour?
   - Convenience, maintainability, coherence with the formal methods
   - Approaches
   - Technical means
1) How to manage a hierarchy of complex systems?

**Flexible Safety Analysis**

- Keep a desired level of precision during SA process
- Control a complexity of SA methods applied
- Reduce time and cost required for SA
2) How to express dysfunctional behaviour?
ANALYTICAL EXPRESSIONS

- Fast annotation
- Easy to analyse

STATE MACHINES

- Separate functional and dysfunctional behavior
- Conform to formal languages: AltaRica, etc.

**Approaches to Express Failure Behavior**

\[
\text{out1} = (\text{in1 AND in2}) \text{ AND NOT (Failure1 OR Failure2)}
\]
For the compatibility of dysfunctional behavior on different levels only Blocks of the finest hierarchical level have an associated set of analytical expressions through dedicated profile.
STATE MACHINES

### METHODOLOGY

**Modeling**

**Safety Analysis**

Blocks of the finest hierarchical level have an associated State Machine

**Annotated and Extended State Machine Diagram**

- Functional Behavior
- Dysfunctional Behavior
MEANS OF FAILURE BEHAVIOR EXPRESSION

Profiles
- EAST-ADL
- DAM
- Custom

Viewpoints, Diagrams
- State Machines
- Activity Diagrams
- ...

Safety comments, requirements

Safety Modeling & Annotation

Model in UML/SysML/RobotML
SOPHIA MODULES

Build accident scenarios

Preliminary Hazard Analysis

Property Verification

Verification of safety properties, Reachability analysis

Fault Tree Analysis

Fault tree generation, minimal cut sets, probabilistic calculations

System Hazard Analysis

Fault Mode & Effects Analysis

Analyze functional causes of accidents

Requirement Engineering

Requirement classification, Report generation, Import/Export to ReqIF

Verification of safety properties, Reachability analysis

FME(C)A tables, Report generation
FAILURE MODE AND EFFECTS ANALYSIS

FME(C)A is an inductive bottom up method used to analyze a system on component level and check what happens on system level.

Cause → Failure → Effect

- Automatic safety annotation
- FME(C)A
- Generation & display of FME(C)A tables within the model
- Automatic document generation
- Export results in excel format
FAULT TREE ANALYSIS

FTA is a deductive top-down method in which an undesired state of a system is analyzed at component level by combining a series of lower-level events using Boolean logic.

- Automatic safety annotation
- HW/SW allocation and propagation of failure behavior
- Automatic fault trees generation
  - Diagrams
  - OpenPSA format
- Qualitative FTA
  - Minimal cut sets, dysfunctional scenarios
- Quantitative FTA
  - Minimal cut sets probabilistic analysis
  - Sensitivity analysis
  - Importance analysis (marginal, critical, diagnostic, risk achievement/reduce factors)
  - Unavailability and SIL analysis
PROPERTY VERIFICATION

Given a model of a system, exhaustively and automatically check whether this model meets a given specification

- State Machines for safety annotation
- Transformation from SysML to SMV state machine
- Verification of system properties (and safety requirements) with NuSMV
- Support of CTL and LTL

Provide a technology to express system requirements/hazards in a quasi natural language

System property in CTL format for NuSMV
REQUIREMENT MANAGEMENT

- Support requirements through system life-cycle
- Display requirements within modeling environment (Tables, Requirement Diagrams)
- Requirement classification
- Automatic report generation

Sophia Modeling Environment

Automatically Generated Requirement Report
## COLLABORATION

<table>
<thead>
<tr>
<th>SAFETY</th>
<th>SAFETY &amp; SECURITY</th>
<th>SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RESEARCH</strong></td>
<td><strong>EXPERTISE</strong></td>
<td><strong>VALORISATION &amp; DEVELOPMENT</strong></td>
</tr>
<tr>
<td>Automotive &amp; Railway domain</td>
<td>Robotic domain</td>
<td>CALL4S</td>
</tr>
<tr>
<td>openETCS</td>
<td>PROJET ROMEO2</td>
<td>Inergy</td>
</tr>
<tr>
<td>IMOFIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Build-IT Safe</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SECURITY</strong></td>
<td><strong>Energy &amp; Smart Grids</strong></td>
<td><strong>Energy &amp; Smart Grids</strong></td>
</tr>
<tr>
<td>Energy &amp; Smart Grids</td>
<td>Transportation domain</td>
<td>MOSARIS</td>
</tr>
<tr>
<td>MOSARIS</td>
<td>Transportation domain</td>
<td></td>
</tr>
<tr>
<td>RISC</td>
<td>RISC</td>
<td></td>
</tr>
<tr>
<td><strong>SAFETY</strong></td>
<td><strong>Energy &amp; Smart Grids</strong></td>
<td><strong>Energy &amp; Smart Grids</strong></td>
</tr>
<tr>
<td>Energy &amp; Smart Grids</td>
<td></td>
<td>MOSARIS</td>
</tr>
<tr>
<td>SESAM-GRID</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Copyright CEA ©**
CONCLUSION

SOPHIA

- Integration of safety techniques within a model-driven engineering process
- Support of generic standard on functional safety design IEC61508 and ISO 13482 safety standard (non-industrial personal care robots)
- Graphical and accessible modeling language (SysML and RobotML)
- Modelling of architecture, behaviour and failure logic
- Automatic document generation

PERSPECTIVES

- Sophia becomes a part of Eclipse Safety Framework (ESF), an open-source model-based tool for safety analysis
  - ESF is a PolarSys project co-managed by CEA and ALL4TEC
  - Industrialization of Sophia in Safety Architect v 3.0
  - Extension of the Sophia research platform with RAMS and security

Copyright CEA ©
THANK YOU!