Techniques for System Safety Analysis

Advanced Practical Course - 2016

Dr. Mario Gleirscher, Dr. habil. D. Méndez

Prof. Dr. Dr. h.c. M. Broy
Institut für Informatik
Software & Systems Engineering
Why System Safety?
Techniques applied to improve System Safety (1)

Failure Mode Effects Analysis (FMEA)

Fault Tree Analysis (FTA)
Techniques applied to improve System Safety (2)

System Theoretic Process Analysis (STPA)

1. HAZARDOUS CONTROL BY HUMAN OR AUTOMATED CONTROLLER
2. HOW POSSIBLE? FTA + CONTROL LOOP
Techniques applied to improve System Safety (3)

- Event Tree Analysis (ETA)
- Hazard Operability Analysis (HAZOP)
- Hazard Analysis and Critical Control Points (HACCP)
- Layer of Protection Analysis (LOPA)
- Etc.
Challenging Analysis Skills To Learn

- Technological and organizational diversity
  - E/E HW, SW, physical parts
  - Collaboration with tech. specialists
- Control system aspects
  - Humans in the loop
  - Causal loops, stability (amplification, non-linearity)
- System modeling (abstraction)
  - Conceptual & physical phenomena
  - Event chains
  - Defects (i.e. errors, faults, failures)
  - Completeness & correctness
- Risk assessment
  - Expert-based, qualitative & probabilistic approaches
Course Goals

- Lay foundation in system safety analysis techniques
  - Terms and principles
  - Approaches, methods, and tools

- Approach a topic in a self-guided manner
- Apply techniques to practical examples
- Summary of results and presentation in front of peers
# Course Overview

*) 3 blocks with ~3days/24hrs workscope

<table>
<thead>
<tr>
<th>Kick-off</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Matching, Grouping</td>
</tr>
<tr>
<td>Home preparation</td>
<td>Training materials, first exercise</td>
</tr>
<tr>
<td>Tutorials*</td>
<td>Analysis techniques</td>
</tr>
<tr>
<td>Safety Analysis*</td>
<td>Application to 3 systems</td>
</tr>
<tr>
<td></td>
<td>(Identify hazards and safety goals/requirements)</td>
</tr>
<tr>
<td>Safety Assurance</td>
<td>Reporting of analysis results and elaboration of assurance solutions</td>
</tr>
<tr>
<td></td>
<td>(Treat hazards / address safety requirements)</td>
</tr>
<tr>
<td>Wrap-up</td>
<td>Workshop with final presentations</td>
</tr>
</tbody>
</table>
Organization

- Website
  http://www4.in.tum.de/~gleirsch/safety/index.shtml

  → News & supporting material

- Time and Location
  - The course will take place in groups and analysis sessions.
  - Part of the course will be combined with an empirical study, hence, groups will be formed randomly.
  - Exact schedule will be defined according to Doodle requests.
  - The per-group dates of all sessions will be announced about a week after the matching notifications.

- If desired, certificates will be provided.
Course Rules

- Each student needs to prepare for the block based on the provided material
- Language for materials and deliverables: English
- Spoken language: English or German on demand
- Examination criteria (per group)
  - **Active participation** at sessions! Don’t miss them!
  - **Reports** (templates will be provided) of analysis and assurance results
  - Final **presentation** (40 min = 20/20 talk/discussion), aids (slides, etc.) to be delivered to advisor one week before presentation
- Evaluation
  - Participation, reports and presentation are rated by all advisors