Standardization of classical system analysis methods for fuzing systems

56th Fuze Conference, Baltimore
Wednesday, 16 May 2012
Open Session VA, 3:20 p.m.

Funded by German Military Engineering and Procurement Agency BWB K 1.3

Dr. I. Häring, U. Siebold, B. Kanat

Contact: Ivo.Haering@emi.fraunhofer.de
Content

- Motivation
- Project framework
- Process:
  1. Reference standards
  2. Visits of Companies
  3. Methods used for analysis
  4. Utilized software
  5. Recommendations: Safety analysis methods
  6. Recommendations: Software
  7. Essential remarks
- Summary
Motivation

- Identification of »Best Practices«
- Standardization of details of methods rather than list of methods
- Interface optimization between companies
- Improvement of external/societal/legal/technical (foreign) acceptance
- Increase of comparability for customers
- Planning certainty, cost prediction
Project framework and procedure

- Duration: 01.07.2008 – 31.03.2011
- 12 participating companies

Procedure:
- Review of Standards, guidelines
- Detail descriptions of key methods
- Visits of companies: survey/questionnaire
- Individual participant and group feedback
- Recommendations
- Approved common final report

<table>
<thead>
<tr>
<th>Number of Companies</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Participating</td>
</tr>
<tr>
<td>2</td>
<td>Participating, not visited</td>
</tr>
<tr>
<td>2</td>
<td>Visited, not participating</td>
</tr>
<tr>
<td>1</td>
<td>Participating in early phase</td>
</tr>
<tr>
<td>2</td>
<td>Participating auditing companies</td>
</tr>
</tbody>
</table>

Flowchart:
- Collection of relevant documents → Visit of companies
  - Evaluation of visits → Private communication
    - Agreement on general form → Specific results
      - Final meetings and discussion → Publishing results
Topics of Questionnaire

- General organization of QM
- Failure mode and effects analysis (FMEA)
- Fault tree analysis (FTA)
- Hazard analysis and Hazard log
- Software tools
- Style of reporting
- Optionally additional procedures
- General questions regarding safety analyses
- General questions about company

<table>
<thead>
<tr>
<th>Sections of questionnaire and number of respective questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
</tr>
<tr>
<td>General management of Quality Management</td>
</tr>
<tr>
<td>General questions about the company</td>
</tr>
<tr>
<td>General questions about safety analyses</td>
</tr>
<tr>
<td>FMEA</td>
</tr>
<tr>
<td>Fault Tree Analysis</td>
</tr>
<tr>
<td>Hazard analyses and Hazard Log</td>
</tr>
<tr>
<td>Alternative techniques</td>
</tr>
<tr>
<td>Software tools</td>
</tr>
<tr>
<td>Documentation practices</td>
</tr>
<tr>
<td>Questionnaire feedback</td>
</tr>
</tbody>
</table>
Methods for analysis

- Preliminary Hazard List (PHL)
- Preliminary Hazard Analysis (PHA)
- (Sub) System Hazard Analysis (SSHA)
- FMEA and FTA as supporting analyses
- Methods include (system) documentation
- Application of fault tree analysis depends on complexity of product
- Additional analytical safety analysis methods were not applied

<table>
<thead>
<tr>
<th>No.</th>
<th>Modes of operation</th>
<th>Hazard</th>
<th>Source</th>
<th>Cause(s)</th>
<th>Effect(s)</th>
<th>IRI</th>
<th>Mitigation</th>
<th>Analyst</th>
<th>Date</th>
<th>Comments</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHA-1.1</td>
<td>Transport</td>
<td>Inadvertent detonation</td>
<td>μC</td>
<td>Software errors in μC</td>
<td>Death and injury</td>
<td>I-D</td>
<td>Fuze design with 3 independent switches</td>
<td></td>
<td></td>
<td></td>
<td>open</td>
</tr>
<tr>
<td>PHA-1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Utilized Software

- Best known software: Relex.
- Widespread: Isograph Reliability Workbench
- Plato Scio (No integration of established Standards, e.g. MIL217, FIDES).
Standards used for reliability prediction

- FIDES
- MIL217
- No additional databases.
- MIL217 is old, but supports the description of shock, e.g. cannon launch
- Problems: short loading duration of shock, differences between shock and vibration loads, determination of environmental factors for electronics.
Recommendation: Safety analyses

- PHL
- PHA
- SSHA
- SHA
- Operating and Support HA
- Supporting methods:
  - FMEA
  - Depending on complexity: FTA
- Hazard Log

All methods include appropriate system model and documentation.
## Recommended (minimum) columns

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unique identifier</td>
</tr>
<tr>
<td>2</td>
<td>Operating mode/mission phase</td>
</tr>
<tr>
<td>3</td>
<td>Hazard</td>
</tr>
<tr>
<td>4</td>
<td>Source</td>
</tr>
<tr>
<td>5</td>
<td>Cause/Trigger</td>
</tr>
<tr>
<td>6</td>
<td>Effects</td>
</tr>
<tr>
<td>7</td>
<td>Initial risk</td>
</tr>
<tr>
<td>8</td>
<td>Recommended actions</td>
</tr>
<tr>
<td>9</td>
<td>Remaining risk after actions</td>
</tr>
<tr>
<td>10</td>
<td>Planned verification procedure</td>
</tr>
<tr>
<td>11</td>
<td>Comment</td>
</tr>
<tr>
<td>12</td>
<td>Date and status</td>
</tr>
<tr>
<td>13</td>
<td>Element</td>
</tr>
<tr>
<td>14</td>
<td>Failure mode</td>
</tr>
<tr>
<td>15</td>
<td>Failure rate</td>
</tr>
<tr>
<td>16</td>
<td>Immediate effects</td>
</tr>
<tr>
<td>17</td>
<td>System effect</td>
</tr>
</tbody>
</table>

- **HL:** 1-6
- **PHA, SSHA, SHA, O&SHA, Hazard Log:** 1-12
- **FMEA:** 1, 5, 8, 11, 12-17

---

**Systematic build-up and extension**
Recommendations for safety analyses

- Hazard identification and analysis should be guided by MIL-STD-882D.
- In case of predefined limiting quantitative requirements (e.g. STANAG 4187), the quantitative analyses must be performed as early as possible.
- STANAG 4297, AOP-15 do not include quantitative requirements for simple munitions. Quantitative requirements for munition without fuze can be derived from minimum requirements of STANAG 4187. These requirements are met in practice.
- Safety analyses must also be performed to fulfill the requirements of the safety lifecycle phases of the functional safety standard IEC 61508, e.g. determination of safety integrity levels.
- Application of FTA for treatment of combinations of failures if relevant
Recommendation: Software

• Criteria should be defined for software. For example:
  • Support for FMEA, FTA, HA
  • Integration of reliability predictions standards: e.g. FIDES, MIL217
  • Compatibility
• A list of recommended software products should be generated on the basis of criteria.
• The list should be regularly updated.
Essential results

• Standardization of safety analyses feasible for existing best practices and not for new practices
• Existing safety analysis practices depend mainly on customer requirements and are rather project-specific
• A major potential of safety analyses was found to be their usage in an early phase of development, e.g. along with project milestones
• A beyond-project/contract /company standardization is expected to facilitate planning, to increase comparability of products and to control costs
Essential results II

- Standardization of safety analyses should be an on-going process. Competitiveness in a free-market economic system must not be hindered.
  - This is also in the long-term interest of industry
- Enhancements of safety analyses have to come mainly from the different industry branches (bottom-up standardization of existing best practices)
  - Examples: Aviation, astronautics, nuclear energy, automotive industry.
- Absence of initiative for standardization from industry results in additional rather project-specific and varying requirements of procurement agencies
- Results of study are accessible in short report containing: method (objective) description, column description and domain-specific hints
Conclusion and Outlook

• Analytical safety analysis methods, software and standards were presented that are to be used in industrial applications in the fuzing (and munition) domain

• Safety analysis methods were presented in detail that form the basis of the standardization.

• Procedure for software selection indicated

• Fundamental considerations regarding the future enhancement of safety analyses were addressed

• Study results available in short hand-book

• Follow-up projects beyond national level feasible: e.g. NATO level

• Transfer to other domains/applications feasible: Methods for Software, Electronic, systems/platforms
Frequently used documents

- STANAG 4297 / AOP 15
- STANAG 4187 / AOP 16
- MIL-STD-882D(E)
- Machinery directive 98/37/EG
- VDI 4003 Reliability management
- Handbuch zum Nachweis der Waffensystemsicherheit (TMS)
- Handbuch für die Systemsicherheit von Waffen und Munition
- Handbuch für den Prüfungsausschuss Munitionssicherheit und die Zusammenarbeit mit dem Projektleiter (PAMS)
Contact

**Dr. Ivo Häring**
Fraunhofer EMI
Am Klingelberg 1
79588 Efringen-Kirchen
Germany
Tel.: +49 7628 90 50 638
Ivo.Haering@emi.fraunhofer.de