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

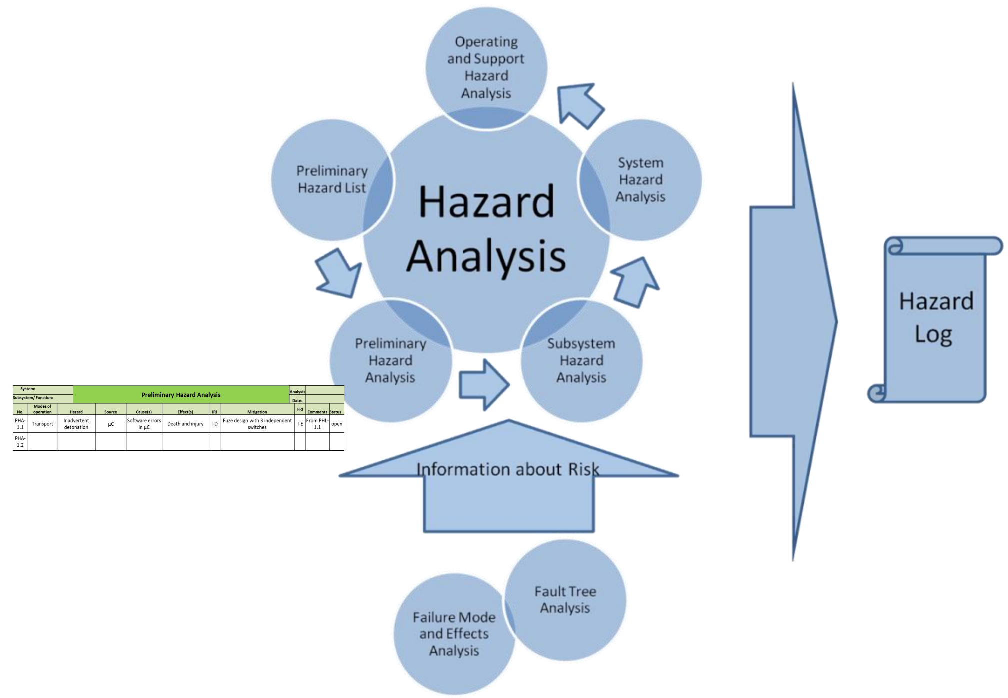
Fraunhofer EMI

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



Fraunhofer EMI

Motivation

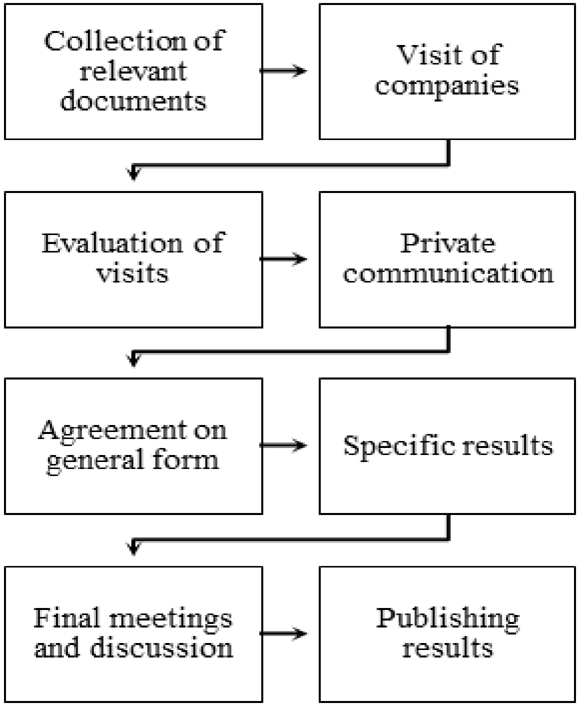
- Identification of »Best Practices«
- Standardization of details of methods rather than list of methods
- Interface optimization between companies
- Improvement of external/societal/legal/technical (foreign) acceptance
- Increase of comparability for customers
- Planning certainty, cost prediction

Project framework and procedure

Number of Companies	Remark
5	Participating
2	Participating, not visited
2	Visited, not participating
1	Participating in early phase
2	Participating auditing companies

- 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

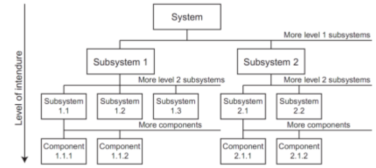


Topics of Questionaire

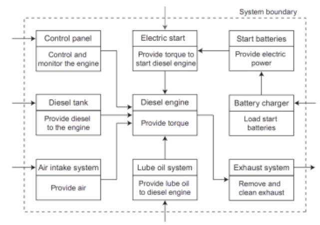
- General organization of QM
- Failure mode and effects analysis (FMEA)
- Fault tree analysis (FTA)
- Hazard analysis and Hazard log
- Software tools
- Style of reporting
- Optionally additional procedures
- General questions regarding safety analyses
- General questions about company

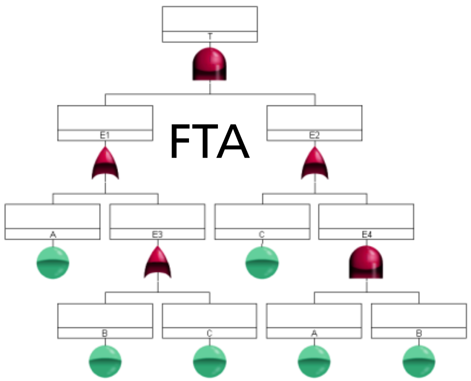
Sections of questionnaire and number of respective questions	
Section	**Number of questions**
General management of Quality Management	11
General questions about the company	14
General questions about safety analyses	27
FMEA	41
Fault Tree Analysis	26
Hazard analyses and Hazard Log	18
Alternative techniques	14
Software tools	15
Documentation practices	12
Questionnaire feedback	3

Methods for analysis



System model





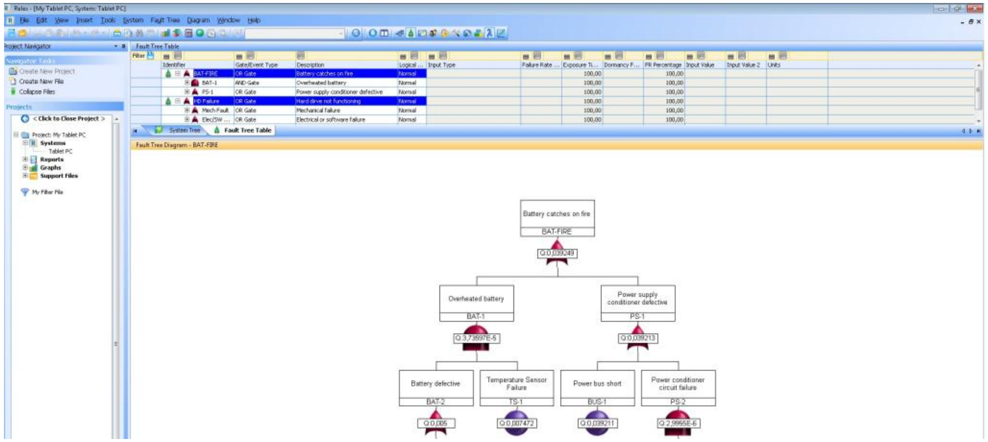
- Preliminary Hazard List (PHL)
- Preliminary Hazard Analysis (PHA)
- (Sub) System Hazard Analysis (SSHA)
- FMEA and FTA as supporting analyses
- Methods include (system) documentation
- Application of fault tree analysis depends on complexity of product
- Additional analytical safety analysis methods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

System:		Preliminary Hazard Analysis						Analyst:		
Subsystem/ Function:								Date:		
No.	Modes of operation	Hazard	Source	Cause(s)	Effect(s)	IRI	Mitigation	FRI	Comments	Status
PHA-1.1	Transport	Inadvertent detonation	µC	Software errors in µC	Death and injury	I-D	Fuze design with 3 independent switches	I-E	From PHL-1.1	open
PHA-1.2										

Fraunhofer EMI

Utilized Software

- Best known software: Relex.
- Widespread: Isograph Reliability Workbench
- Plato Scio (No integration of established Standards, e.g. MIL217, FIDES).
- Rodon: Numerical simulation of electronic devices.

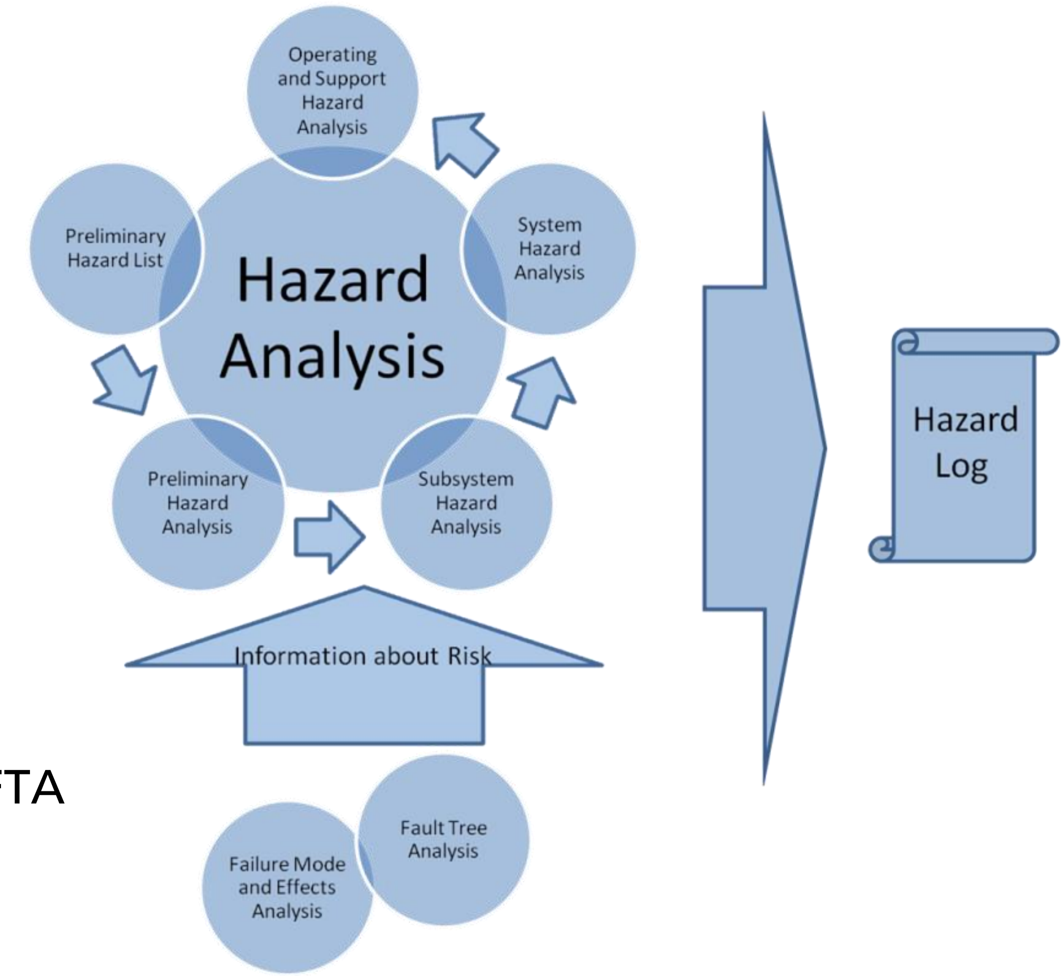


Standards used for reliability prediction

- 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.

Fraunhofer EMI

Recommended (minimum) columns

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

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

Systematic build-up and extension

Fraunhofer EMI

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


Fraunhofer
EMI

Vereinheitlichung von Sicherheitsanalysen für Zünder und Munition
Abschlussbericht

Bericht xx/11

Berichterstatter:
N. Echterling
Mit Beiträgen von:

Projektleiter:
I. Häring

März 2011
Efringen-Kirchen

- 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