Safety Assessment of Fuzing Systems Using IEC 61508

Applicability, Safety Life-Cycle, Safety Function, Methods for Hardware and Software

54th Annual Fuze Conference
„The Fuzing Evolution
– Smaller, Smarter, Safer“

May 11-13, 2010
Kansas City, Missouri, USA

U. Siebold, M. Larisch, Dr. I. Häring

Contact: Technical Safety Group
Hazard and Risk Analysis Group
haering@emi.fraunhofer.de

Fraunhofer EMI

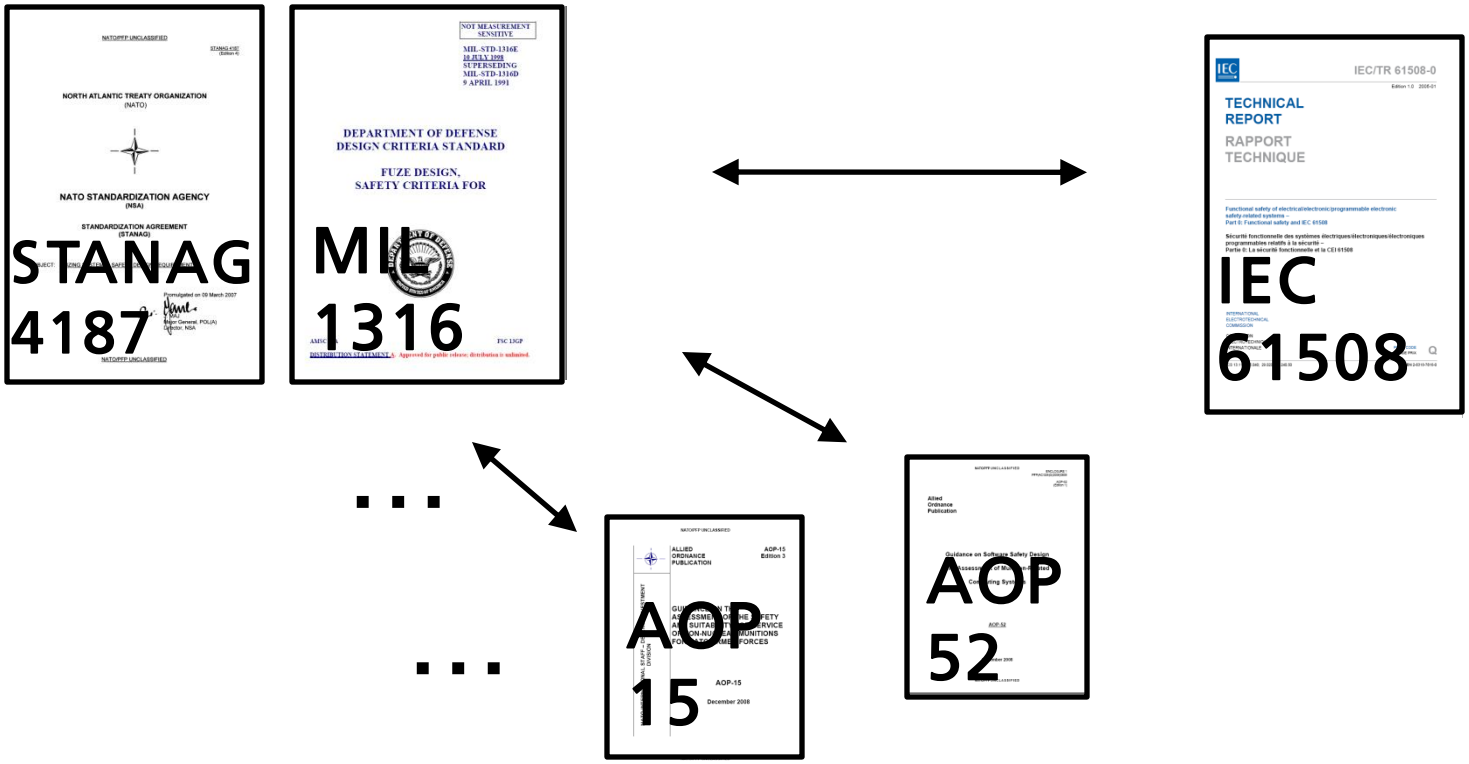
Fraunhofer EMI

German Fraunhofer-Gesellschaft
Largest organization for applied research in Europe
59 Fraunhofer Institutes
17, 000 staff
€ 1.3 billion annual contract research
Customers: industry, service sector, public administration

Fraunhofer Group for Defense and Security
8 Fraunhofer Institutes
Customers: German federal ministry of defense, defense technology industry

Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institute, EMI
Department of safety technologies
Hazard and risk analysis group, Technical safety group

Approach



Use IEC 61508 to fulfill the requirements of STANAG 4187, MIL 1316 for electronic hardware and software

Overview

- Applicability of IEC 61508
- Safety life cycle of IEC 61508 and STANAG 4187 requirements
- Safety features are safety functions
- Specification and allocation of safety functions
- Methods for reliability: hardware and software

Applicability of IEC 61508

- **Generic standard for safety related and safety critical systems**
- **Applicable if electrical, electronic or programmable electronic (E/E/PE) (sub)systems, i.e. electronic hardware and software, perform safety functions**
- Formalism takes into account risk reduction with other technologies, e.g. precision and micro mechanics (MEMS)
- Focus on development of reliable safety functions with hardware and software
- Used in Germany also for weapon systems, active protection systems

- Application sector standards:
  IEC 61513: nuclear power plants,
  IEC 61511: process industry,
  IEC 62061: machinery,
  EN 50128, EN 50129: electronic, software of railway systems
- Drafts:
  IEC 61800-5-2: Adjustable speed electrical power drive systems,
  ISO 26262: automotive industry

Overview

- Applicability of IEC 61508
- **Safety life cycle of IEC 61508 and STANAG 4187 requirements**
- Safety features are safety functions
- Specification and allocation of safety functions
- Methods for reliability: hardware and software

Comparison of key concepts

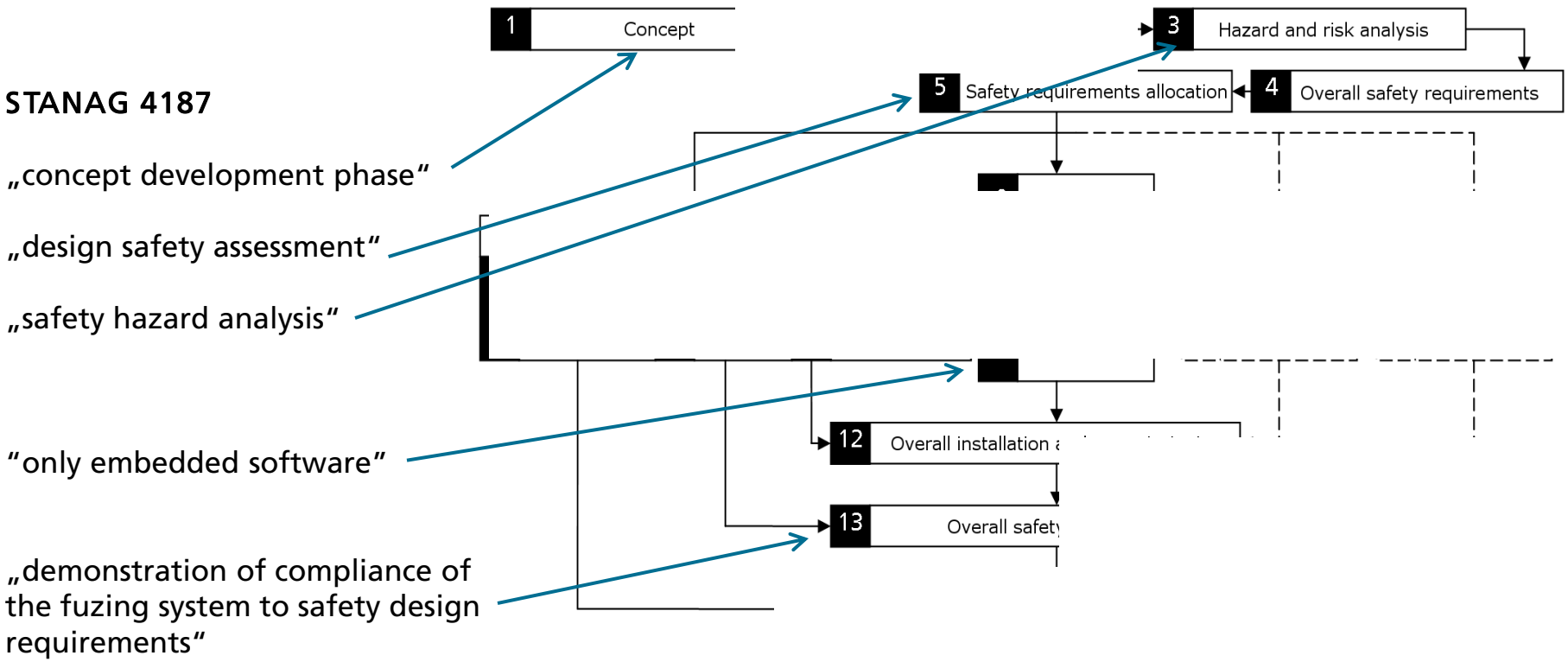
STANAG 4187

- life cycle environmental profile
- **Safety feature**; includes independence of physical detection principle
- Some phases correspond directly to phases of IEC 61508 safety lifecycle
- **Quantitative** safety requirements: unintentional functioning/arming shall not exceed one in a thousand/ in a million
- At least two independent safety features till launch
- Some techniques and measures are given

IEC 61508

- **Safety lifecycle** and life cycle
- **Safety functions** reduce risks of the system to an acceptable level
- Risks of the system are identified based on system analysis
- Risk comparison with risk criteria determines necessary risk reduction
- **Quantification** of reliability of safety functions using safety integrity levels (SILs)
- Hardware redundancy for higher safety requirements (SIL 3, SIL 4). More than one independent E/E/PE safety function for high safety requirements (> SIL 4)
- **Techniques and measures for hardware and software**

Sorting STANAG 4187 requirements with IEC safety life cycle



IEC 61508 suggests systematic (iterative) approach for development and assessment

Fraunhofer EMI

Correspondence of sections of STANAG 4187, Ed. 4 to content of phases of IEC 61508

IEC phase No.	Safety lifecycle phase of IEC 61508	Section of STANAG 4187
1		3., 4., 5.b.
2		2., 5.a., 5.d.
3		5.d., 7.a., 7.e., 14.a., 14.c.
4		5.d, 6.a.(3), 6.b.(3), 7.b., 7.c., 8.a.(1)-(3), 8.b.(1), 9.c., 10.b.(1), 10.d., 10.f., 11.a.-f., 12.a.
5		5.a., 5.b, 14.f.
6		
7		5.b.
8		
9		5.d.
10		5.d.
11		5.d.
12		
13		14.b., 15
14		
15		
16		

Overview

- Applicability of IEC 61508
- Safety life cycle of IEC 61508 and STANAG 4187 requirements
- **Safety features are safety functions**
- Specification and allocation of safety functions
- Methods for reliability: hardware and software

Definitions of safety feature and safety function

- **STANAG 4187, Ed. 4 – Safety Feature:**
  Section 6.a.(1):
  Fuzing systems shall include at least two safety features. The control and operation of these safety features are to be functionally isolated from other processes within the munition system and each of which shall prevent unintentional arming of the fuzing system. At least two of the safety features shall be independent and designed to minimize the potential for common cause failures.
  Section 6.a.(3):
  At least one of the independent safety features shall prevent arming after launch or deployment until the specified safe separation distance or equivalent delay has been achieved.

- **IEC 61508-4 – Safety Function:**
  Function to be implemented by an E/E/PE safety-related system, other technology safety related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the equipment under control, in respect of a specific hazardous event.

Overview

- Applicability of IEC 61508
- Safety life cycle of IEC 61508 and STANAG 4187 requirements
- Safety features are safety functions
- **Specification and allocation of safety functions**
- Methods for reliability: hardware and software

Quantitative measure for reliability of qualitatively described safety function: Safety Integrity Level (SIL)

- Reliability of safety function greater than SIL 4: at least 2 independent safety functions
- Techniques and measures depend on required SIL
- Quantity and quality (rigor) of techniques and measures increase with increasing SIL

IEC 61508-1

Low Demand Rate

SIL	Probability of failure (PFD) on demand
4	[1.e-5,1.e-4[
3	
2	
1	

High Demand Rate

SIL	Probability (Frequency) of failure (PFD) per hour
4	
3	
2	
1	

Example: the barrier has to be in safe position during overflight with a failure probability on demand (per life cycle) of less than 1.e-5 (SIL 4)

Fraunhofer EMI

SIL determination for overall safety function for fuzing systems using STANAG 4187

Prevention of unintended arming/ functioning till launch/ safe separation

High demand rate:

(1) P = Required probability of **non**-arming/functioning per life cycle (e.g.1.e-6, 1.e-3)

(2) T = Average duration of considered life cycle phase of fuzing system (e.g. 1 s, 20 min 1 d, 1M, 1 y, 10 y)

(3) P/T <= PFD per hour = maximum failure rate per hour of overall safety function

Example, till launch: 1.e-6/10 y < 1.e-6/(10*1.e4 h) = 1. e-11/h < 1.e-9/h: more than SIL 4

If the *SIL definition is linearly continued* this corresponds to a "SIL 6" requirement.

Low demand rate:

(1) P = Required probability of **non**-arming/functioning on demand (e.g.1.e-6, 1.e-3)

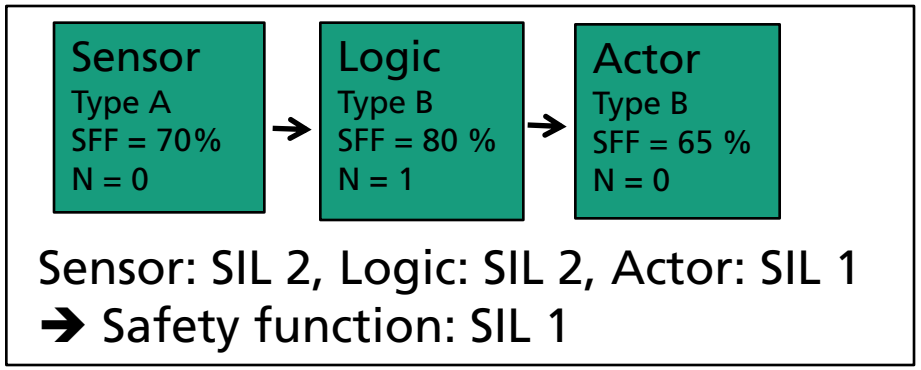
(2) P <= PFD on demand = maximum failure rate on demand of overall safety function

Example, till launch: 1.e-6 < 1.e-5: more than SIL 4, "SIL 5"

Till launch: At least two independent (E/E/PE) safety systems required by IEC 61508.

Architectural requirements: IEC Block diagrams, IEC estimate of achievable reliability of safety function (SIL)

- Block diagrams consider redundancy (serial, parallel) using "SIL decomposition rules"; similar to reliability block diagrams
- SIL (estimate) of hardware components is determined by: type, SFF, hardware fault tolerance



Safe failure fraction (SFF)	Type A Non-complex component		
	Hardware fault tolerance N		
	N = 0	N = 1	N = 2
< 60%	SIL 1		

Safe failure fraction (SFF)	Type B Complex component		
	Hardware fault tolerance N		
	N = 0	N = 1	N = 2

Fraunhofer EMI

Overview

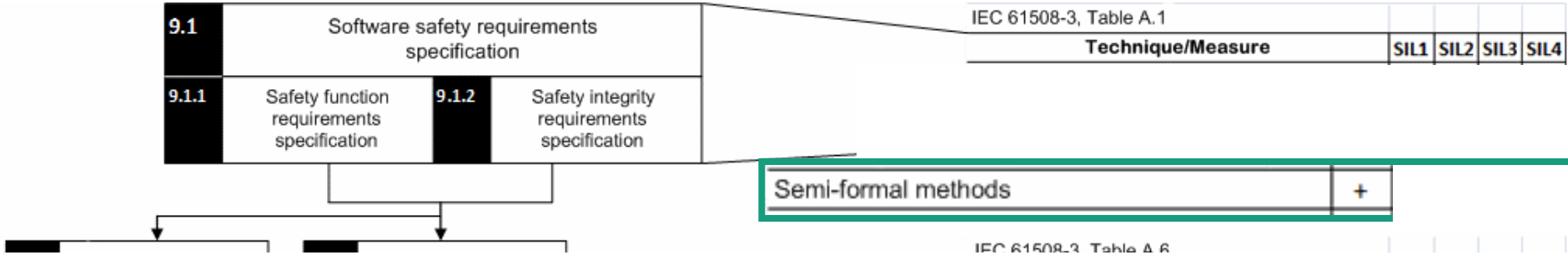
- Applicability of IEC 61508
- Safety life cycle of IEC 61508 and STANAG 4187 requirements
- Safety features are safety functions
- Specification and reliability of safety functions
- **Methods for reliability: hardware and software**

Selection of techniques and measures for hardware and software for the development of reliable (safety) functions

- Method pool: STANAG 4187, AOP 52, AOP 15, IEC 61508

- **IEC 61508 recommends or advises against techniques and measures depending on the required reliability of the safety function (SIL) and the safety life cycle phase**
- Techniques and measures for the control of **systematic software and hardware errors**, statistic errors, soft errors
- Methods for specification, development, testing, integration, verification, validation, includes organizational measures
- Description of methods, links to literature
- Updates of method list for new editions of standard (scheduled for 2010), domain specific methods can also be used

Techniques and measures for the realization of software safety functions according to IEC 61508

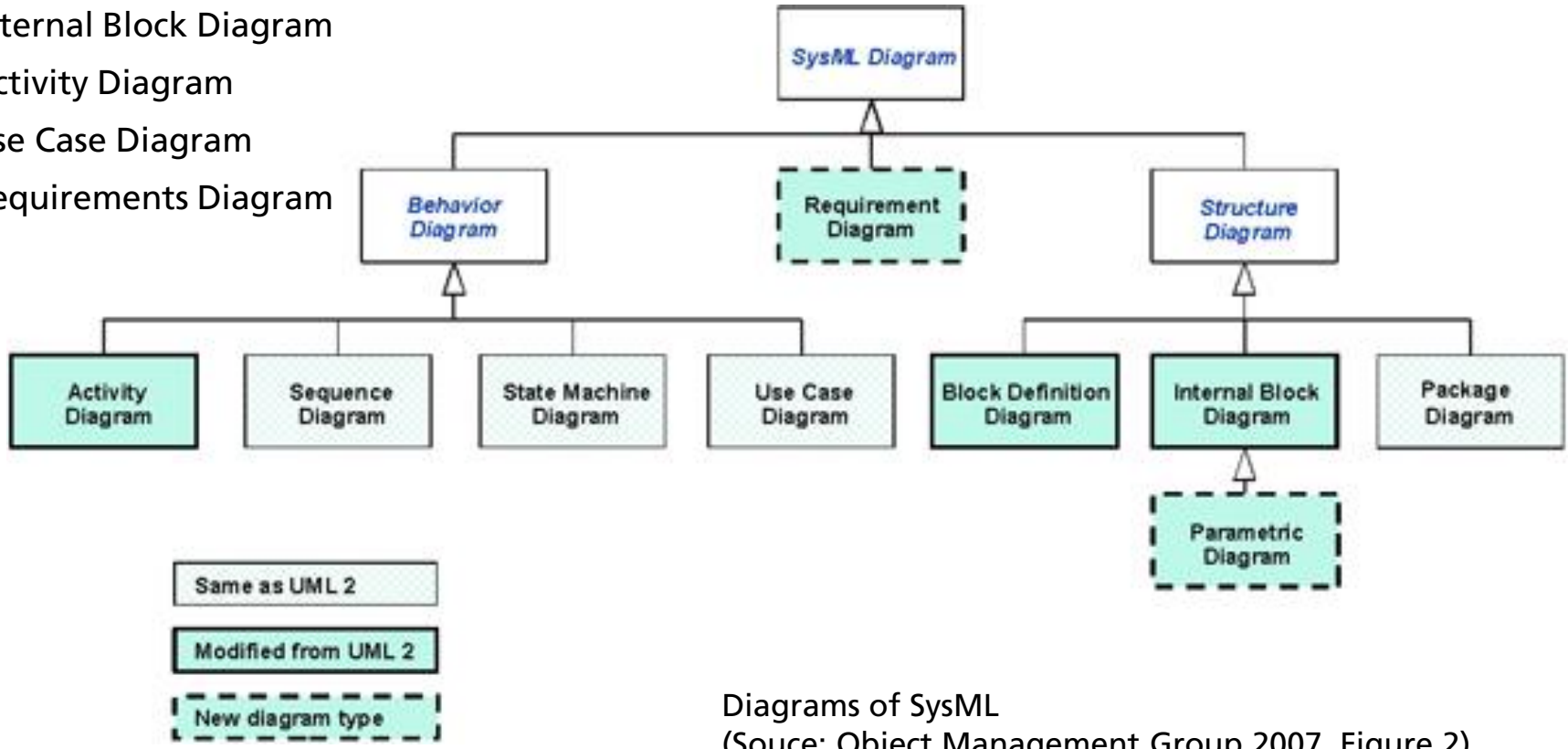


So
(in
(IE

Fraunhofer EMI

Example: semi-formal System Modeling Language (SysML) Diagrams

1) Block Definition Diagram
2) Internal Block Diagram
3) Activity Diagram
4) Use Case Diagram
5) Requirements Diagram



Diagrams of SysML
(Souce: Object Management Group 2007, Figure 2)

Fraunhofer EMI

Appropriate SysML diagrams for all safety lifecylce phases of IEC 61508

Phase	Block Defi-nition D.	Internal Block D.	Activity Diagram	State Machine D.	Se-quence Diagram	Use Case Diagram	Require-ment D.
1	x	x	x				
2	x	x	x				
3			x	x	x		
4						x	x
5						x	x
6			x				
7			x				
8			x				
9	o	o	o	o	o	o	o
10							
11							
12			o				
13	o	o	o	o	o	o	o
14			o				
15							
16							

SysML can be used beyond realization phase

"x" means first use
"o" reuse in a later phase

When arriving at the realisation phase a rather detailed SysML model has been generated.

The SysML model of the Systems consists of all SysML diagrams.

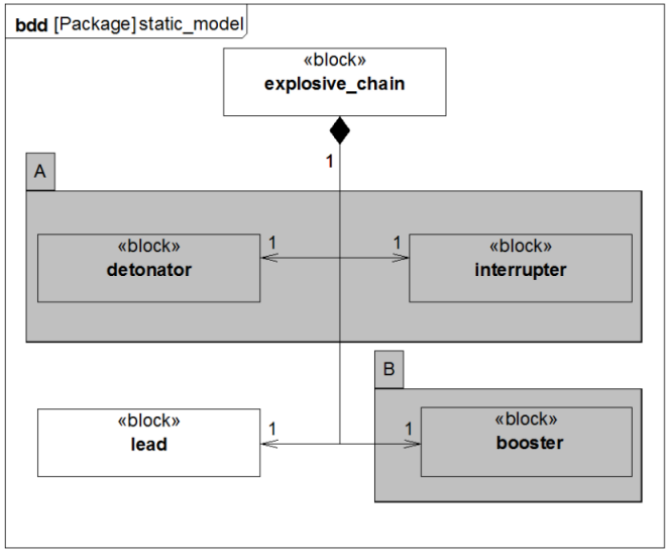
We have only indicated the first and in our opinion most relevant use of the diagrams.

Structure diagrams are used in the early phases, behavior diagrams in later phases.

SysML: simple small generic sample system

SysML structure diagrams

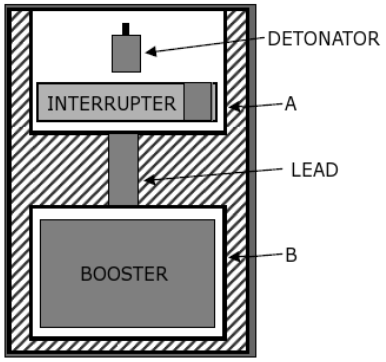
Standardized visualization with SysML – diagrams

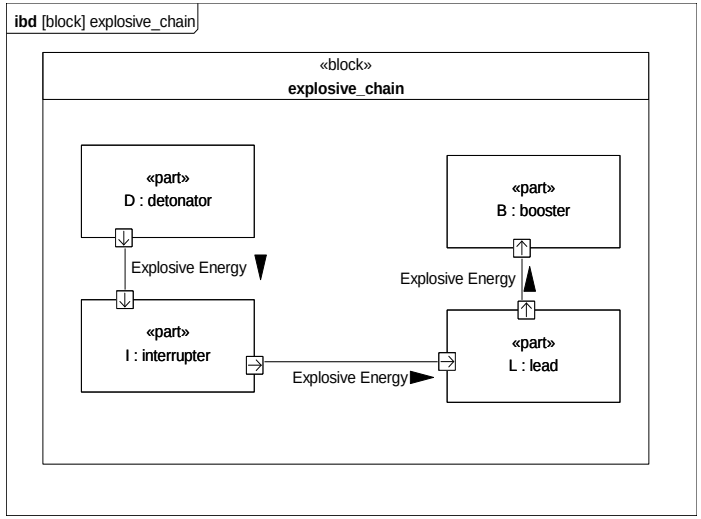


Block Definition Diagram

Internal Block Diagram

Example: Ad-Hoc visualization of out-of-line fuzing chain





Fraunhofer EMI

Conclusions

The IEC 61508 can be applied to fuzing systems.

STANAG 4187/ MIL 1316 and IEC 61508 use similar concepts, e.g. safety functions.

Safety life cycle of IEC 61508 is a systematic approach for the development of safety critical systems:
system understanding, identification of risks of the system, determination of the necessary risk reduction, explicit qualitative and quantitative specification of safety functions, realistic architecture (no bottlenecks), development of hardware and software for safety functions applying appropriate techniques and measures.

If comfort functions and safety functions cannot be separated comfort functions must be treated as safety functions.

According to the required reliability of the safety functions suitable techniques and measures must be applied for hardware and software.

The active development of safety functions suits developers.