Efficient Exploration of Safety-Relevant Systems Through a Link Between Analysis and Simulation

Moomen Chaari[1,2], Wolfgang Ecker[1,2], Thomas Kruse[1], Cristiano Novello[1], and Bogdan-Andrei Tabacaru[1,2]

[1] Infineon Technologies AG, [2] Technische Universität München

SPONSORED BY THE

Federal Ministry of Education and Research

Contents

Scope: Safety Evaluation for Automotive (1/2)

Technology trends

- ↑ complexity
- ↑ integration density

↑ vulnerability to failures

„absence of unreasonable risk“

ISO 26262

Safety Evaluation

essential aspect in system design & manufacturing

› Evaluation at different levels and process steps:

Conceptual analysis

(early failure analysis, qualitative / quantitative risk assessment)

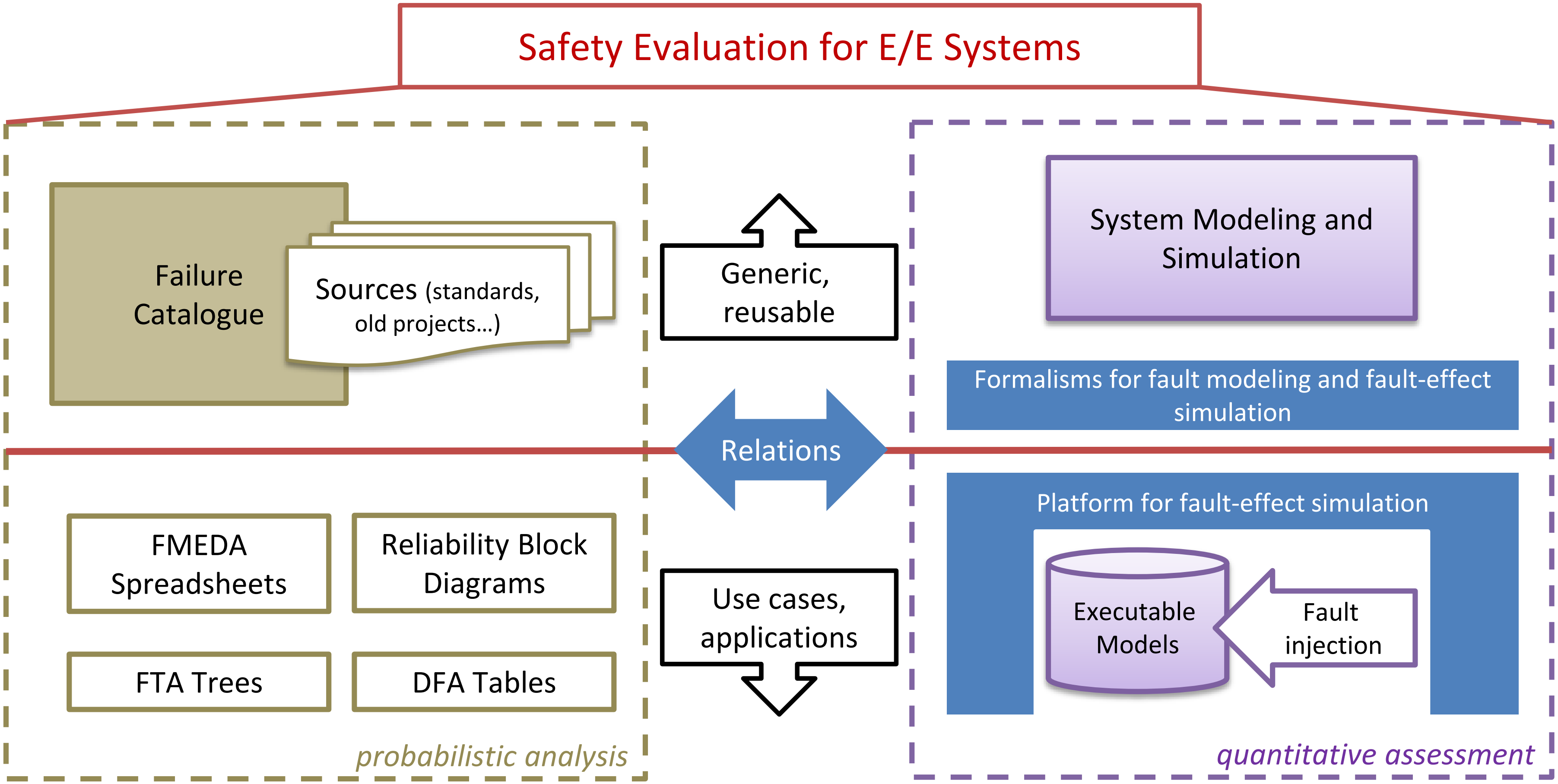
Simulation-oriented system alterations

(fault injection)

Physical prototype testing

(hardware/software certification)

Scope: Safety Evaluation for Automotive (2/2)



Motivation and Challenges

Safety Analysis

+ Established methodologies in the industry
+ ISO 26262 compliant

– Manual character
– Huge documents
– High effort and time costs

Missing link

Fault Injection and Simulation

+ Easy integration in common design/verification platforms

– Late application
– Implementation details required
– Slow simulation

Missing link

State of the Art

Safety Analysis Methods (1/2)

Safety Analysis
essential aspect in system design & manufacturing

Tasks

- predict potential risks
- identify causes & effects
- deploy countermeasures
- compute evaluation metrics

Methods & techniques

	deductive	inductive
qualitative	FTA (1)	FMEA (3)
	DFA(4)	DFA(4)
quantitative	FTA (1) RBD (2)	FMEDA Failure Modes, Effects, and Diagnostic Analysis

(1) Fault Tree Analysis
(2) Reliability Block Diagram
(3) Failure Modes and Effects Analysis
(4) Dependent Failure Analysis

State of the Art
Safety Analysis Methods (2/2)

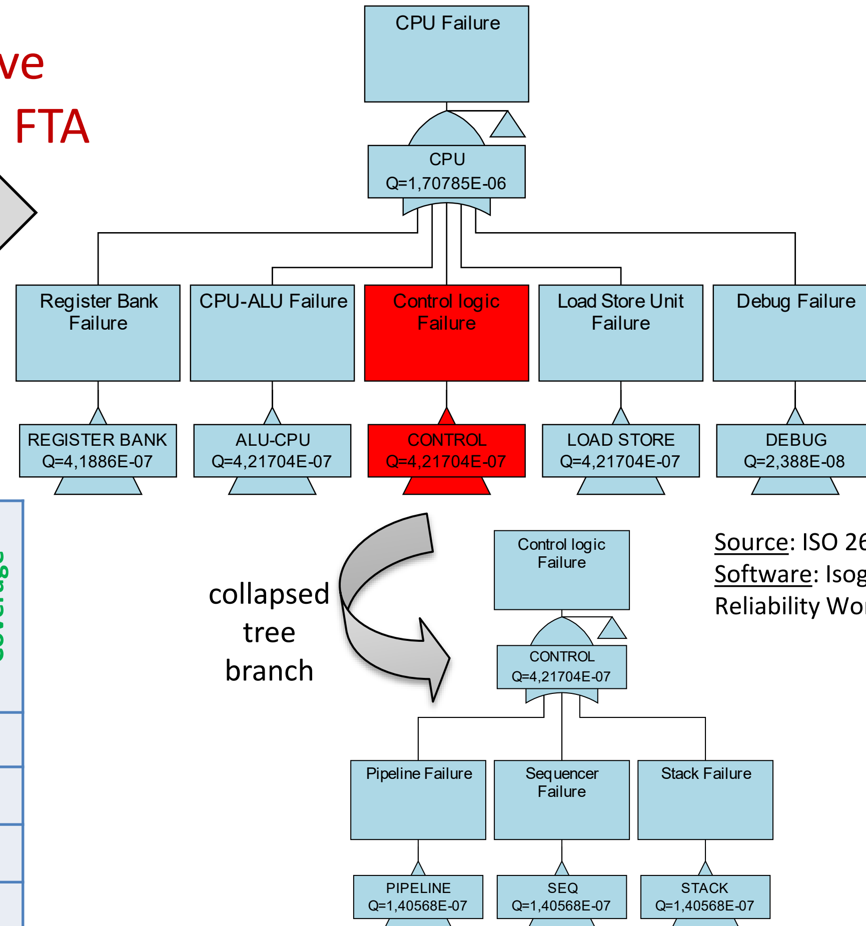
Safety Analysis Documentation (State-of-practice)

Deductive approach: FTA

Inductive approach: FMEDA

Part	ISO Element	Failure Rate	Function	Failure Mode	Failure Distribution	Failure Type	Failure Effect	Severity	Safety Measure	Diagnostic Coverage
ALU	Processing Units (ALU -Data Path)	0.348 FIT	Ft. 1	FM1	25%	HE	FE1	Negligible	-	-
							FE2	Dangerous	SM1	90%
				FM2	25%	HE	FE3	Critical	SM2	60%
			Ft. 2	FM3	50%	SE	FE4	Negligible	-	-

Example of an FMEDA Table



Source: ISO 26262
Software: Isograph Reliability Workbench 11

Example of a Fault Tree Extract

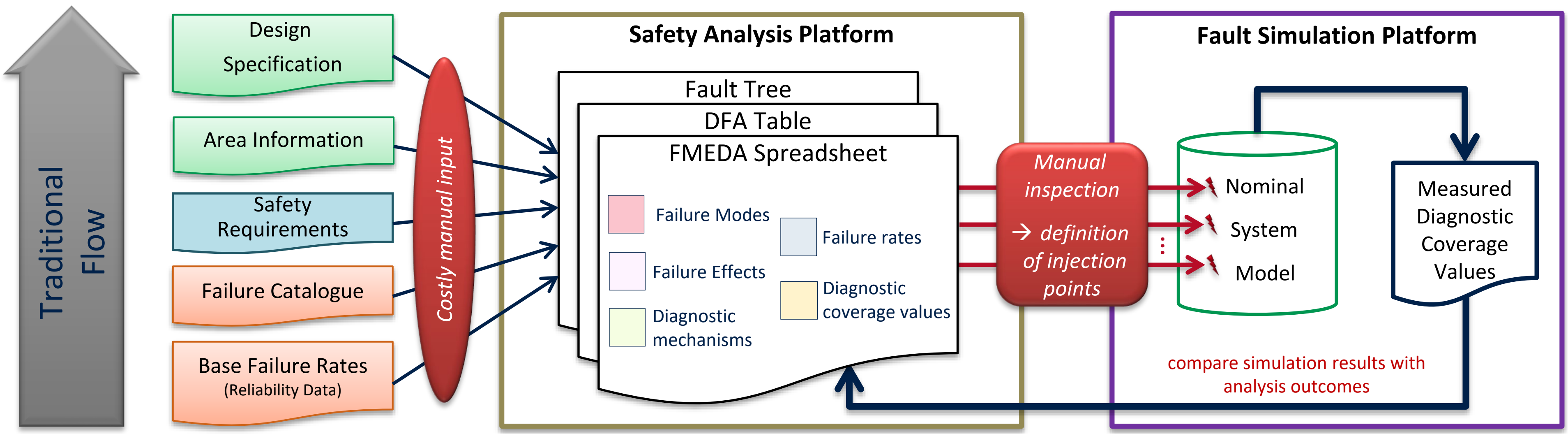
State of the Art
Fault Injection Techniques

Fault Injection and Simulation
highly recommended for ASIL C and D

Tasks	Methods & techniques	
identify sensitivity zones → injection points	hardware-based	• deviate environment parameters • modify circuit pin values • disturb power supply…
identify observation and diagnostic points	software-based	• compile-time alterations • runtime alterations
deploy appropriate workloads	simulation-based	• code modification (saboteurs / mutants) • simulator commands
monitor system reaction	…	
validate detection/correction		

Model-Based Safety Analysis (1/3)

› Traditional flow:

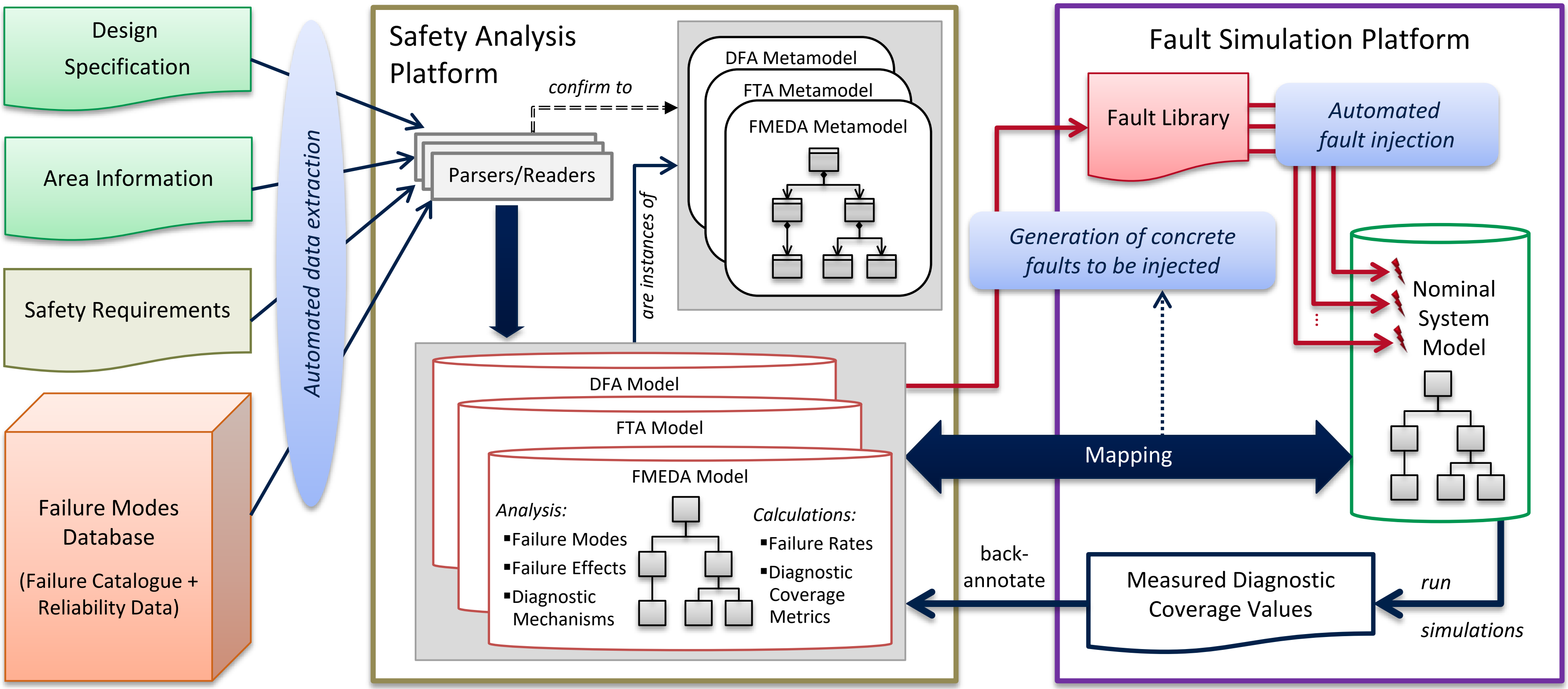


› Strategy to reduce efforts and costs in the flow:

Use **data models** constructed as instances of so-called **metamodels** as substitution of huge documents.

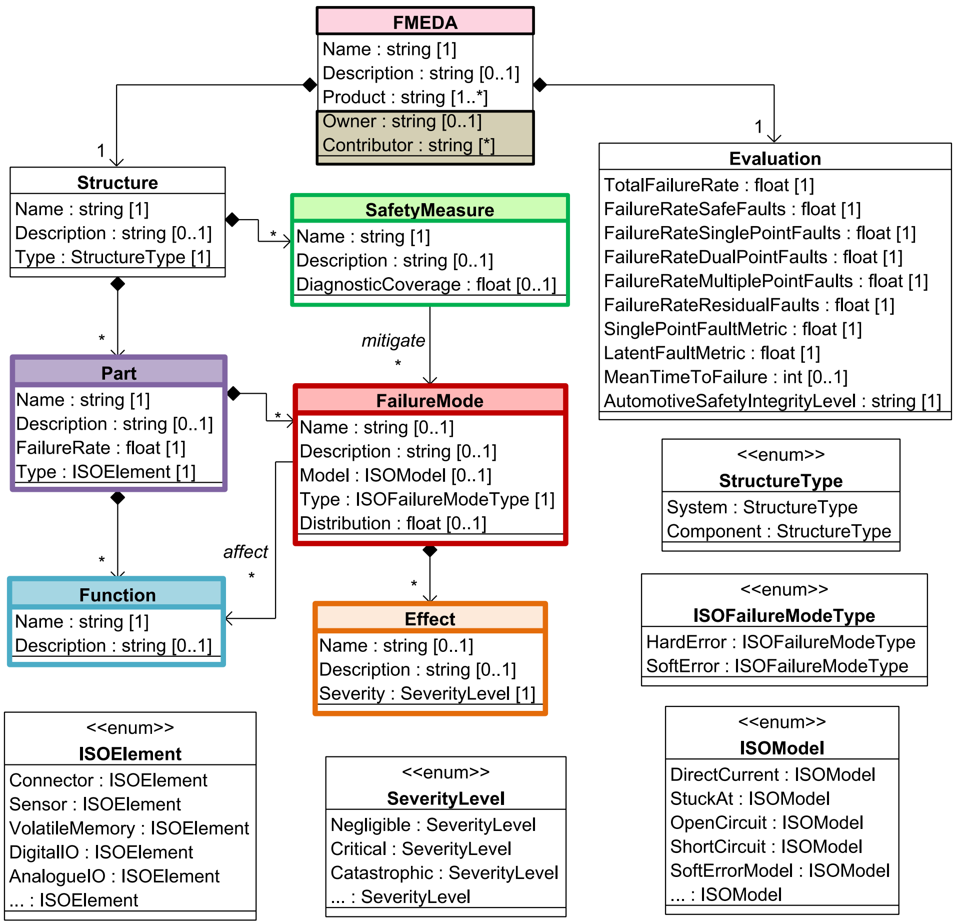
Model-Based Safety Analysis (2/3)

- Proposed flow:



Model-Based Safety Analysis (3/3)

- Example of Metamodel-Based Formalization:



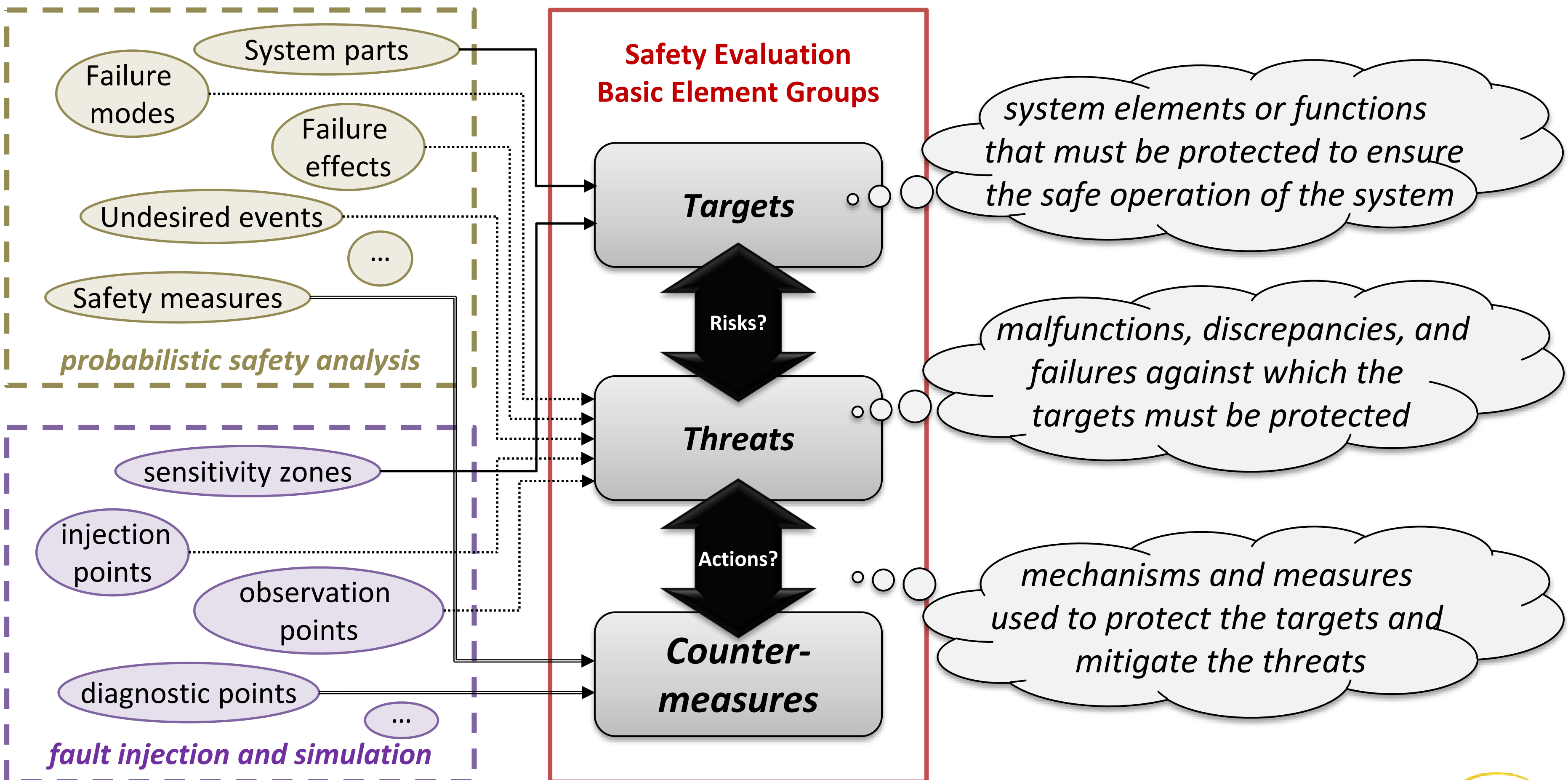
Simplified FMEDA Metamodel

Constructed based on correlations with FMEDA flow and documentation

Part	ISO Element	Failure Rate	Function	Failure Mode	Failure Distribution	Failure Type	Failure Effect	Severity	Safety Measure	Diagnostic Coverage
ALU	Processing Units (ALU -Data Path)	0.348 FIT	Ft. 1	FM1	25%	HE	FE1	Negligible	-	-
							FE2	Dangerous	SM1	90%
				FM2	25%	HE	FE3	Critical	SM2	60%
			Ft. 2	FM3	50%	SE	FE4	Negligible	-	-

Example of an FMEDA Spreadsheet Extract

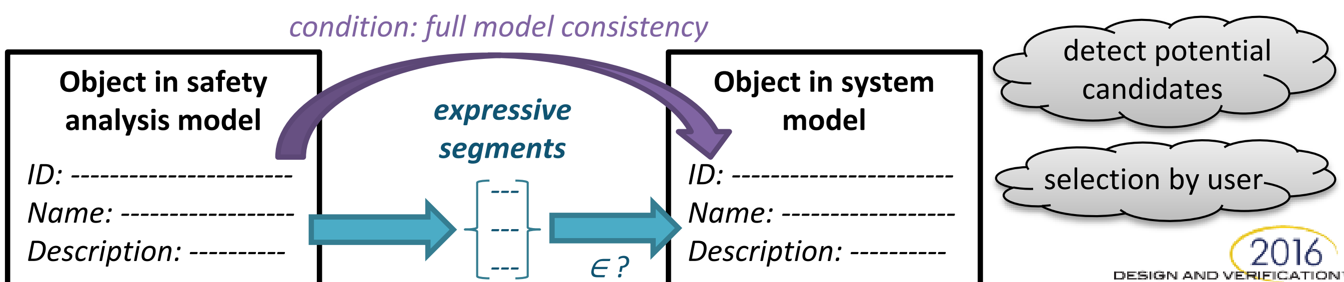
Link to Fault Injection and Simulation (1/2)



Link to Fault Injection and Simulation (2/2) – Data Mapping

	Safety Analysis	Fault Injection
Targets	Parts, Functions (FMEDA), Elements (DFA)	Modules, Submodules, Entities, Components…
Threats	Failure modes (FMEDA), Dependent failures (DFA), Events (FTA)	Injection points (signals, ports, variables, sockets, processes…)
	Failure Effects (FMEDA/DFA), Events (FTA)	Observation points (signals, ports…)
Counter-measures	Safety measures (FMEDA, DFA)	Diagnostic and correction points (modules, submodules, signals…)

- ✓ ID matching
- ✓ Name/description matching



Summary and Outlook

- **Model-Based Safety Analysis and Link to Fault Injection**
  - Formalization and automated support
  - Comprehensive and flexible framework (partly synthesized)
  - Model-to-model mapping
- **Main Benefits**
  - Systematic and well-organized approaches for safety analysis
  - Dynamic failure modes database
  - Generation of fault libraries to stimulate fault injection
  - Effort savings and speed-up reaching 70%
- **Future Work and Planned Improvements**
  - Refinements of data mapping algorithms
  - Link to requirements-engineering

Questions?

Thank you for your attention.