Continuous FMEDA – from Circuit to System

Challenge

Product **complexity** is **growing** exponentially while **safety engineering** remains **manual**

FMEDA in practice is

- labor-intensive,
- prone to human error,
- often delayed until end of the development life-cycle

more features, more electronics

higher complexity due to interconnectivity

increasing safety expectations

Late-stage verification raises the **risk of preventable safety issues** and **costly rework**

For "continuous safety" to become reality, we need to automate activities of the safety engineering life-cycle.

Solution

Automating FMEDA* introduces a paradigm shift to the development of safety-critical systems, enabling frequent iterations of the system design due to faster, more accurate analyses.

*successfully evaluated by TÜV Süd according to IEC61508 for use up to SIL4

seamless toolchain and workflow integration**

* rapid identification of critical components

 \rightarrow more than 90% coverage of applicable failure modes

(automated computation of safety and reliability metrics) SFF, MTBF, λ SR, PFD, PFH

Electronic Circuit			**a "spell-checker" for electric circuit designs
	Engineering design import from EDA tools		
	Safety requirements	Al Engine	
- • - •		Automated Madel Automated Page	



import from requirement tool or define manually



Failure modes & rates from industry databases – e.g., SN 29500, MIL-HDBK-217F

Automated Model	Automated Reasoning	
Transformation	on Failure Behavior	

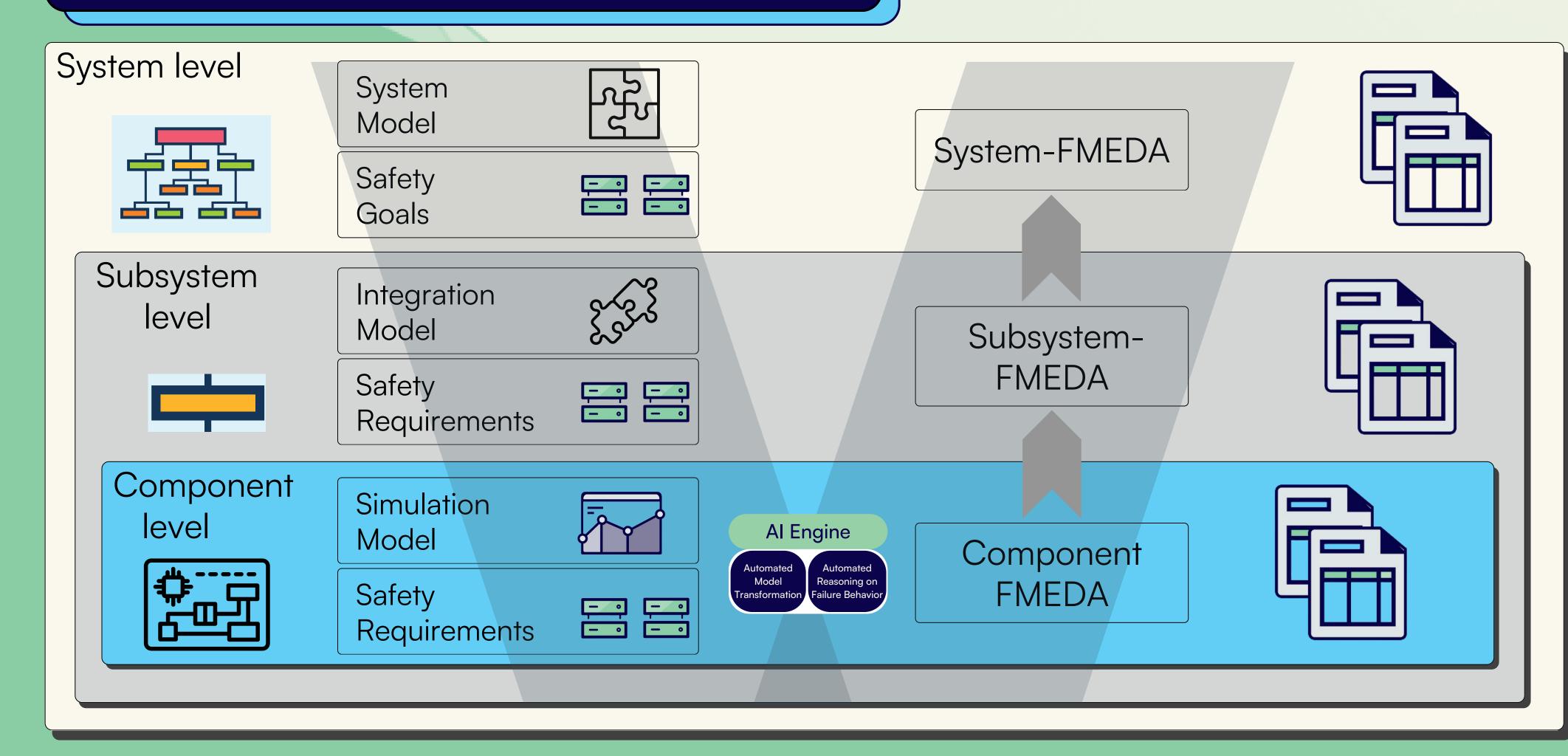


FMEDA report ready for assessment

Different stakeholders verify design artifacts on different levels separately.

This fragmented safety engineering life-cycle poses the risk of design flaws being overlooked.

Outlook – from Circuit to System



Realizing continuous FMEDA throughout the development lifecycle requires FMEDA automation to be elevated to the system level.



Engage with us to **discuss** the **challenges** that still lie ahead!



Claudius Jordan, Arnold Bitner