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

Moomen Chaari\textsuperscript{1,2}, Wolfgang Ecker\textsuperscript{1,2}, Thomas Kruse\textsuperscript{1}, Cristiano Novello\textsuperscript{1}, and Bogdan-Andrei Tabacaru\textsuperscript{1,2}

\textsuperscript{1}Infineon Technologies AG, \textsuperscript{2}Technische Universität München
Contents

• Scope: Safety Evaluation for Automotive
• Motivation and Challenges
• State of the Art
  – Safety Analysis Methods
  – Fault Injection Techniques
• Model-Based Safety Analysis
• Link to Fault Injection and Simulation
• Summary and Outlook
Scope: Safety Evaluation for Automotive (1/2)

Technology trends

- ↑ complexity
- ↑ integration density
- ↑ vulnerability to failures

Safety Evaluation

- "absence of unreasonable risk"

ISO 26262

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)

Safety Evaluation for E/E Systems

- Failure Catalogue
- Sources (standards, old projects...)
- FMEDA Spreadsheets
- Reliability Block Diagrams
- FTA Trees
- DFA Tables

probabilistic analysis

- Generic, reusable
- Relations
- Use cases, applications

quantitative assessment

- System Modeling and Simulation
- Formalisms for fault modeling and fault-effect simulation
- Platform for fault-effect simulation
- Executable Models
- Fault injection
Motivation and Challenges

Safety Analysis

+ Established methodologies in the industry
+ ISO 26262 compliant

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

Fault Injection and Simulation

+ Easy integration in common design/verification platforms

− Late application
− Implementation details required
− Slow simulation
State of the Art
Safety Analysis Methods (1/2)

Safety Analysis
essential aspect in system design & manufacturing

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Methods &amp; techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>predict potential risks</td>
<td>deductive</td>
</tr>
<tr>
<td>identify causes &amp; effects</td>
<td>qualitative</td>
</tr>
<tr>
<td>deploy countermeasures</td>
<td>quantitative</td>
</tr>
<tr>
<td>compute evaluation metrics</td>
<td>inductive</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>qualitative</th>
<th>FTA (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FTA (1)</td>
</tr>
<tr>
<td></td>
<td>RBD (2)</td>
</tr>
<tr>
<td>deductive</td>
<td>DFA (4)</td>
</tr>
<tr>
<td></td>
<td>FMEA (3)</td>
</tr>
<tr>
<td></td>
<td>FMEDA</td>
</tr>
<tr>
<td></td>
<td>Failure Modes, Effects, and Diagnostic Analysis</td>
</tr>
</tbody>
</table>

(1) Fault Tree Analysis
(2) Reliability Block Diagram
(3) Failure Modes and Effects Analysis
(4) Dependent Failure Analysis
Example of an FMEDA Table

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

Example of a Fault Tree Extract

Deductive approach: FTA

Inductive approach: FMEDA

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

Source: ISO 26262
Software: Isograph Reliability Workbench 11
State of the Art
Fault Injection Techniques

Fault Injection and Simulation
highly recommended for ASIL C and D

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

© Accellera Systems Initiative
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:

- **Design Specification**
- **Area Information**
- **Safety Requirements**

**Safety Analysis Platform**

- **Failure Modes Database** (Failure Catalogue + Reliability Data)
- **Parse/Readers**
- **Safening Analysis**
  - DFA Metamodel
  - FTA Metamodel
  - FMEDA Metamodel
  - Parsers/Readers
- **Calculations**
  - Failure Rates
  - Diagnostic Coverage Metrics

**Fault Simulation Platform**

- **Fault Library**
- **Automated fault injection**
- **Nominal System Model**
- **Generation of concrete faults to be injected**
- **Measured Diagnostic Coverage Values**
- **Mapping**
  - back-annotate
  - run simulations

**Automated data extraction**

© Accellera Systems Initiative 2016
Model-Based Safety Analysis (3/3)

Example of Metamodel-Based Formalization:

- **Simplified FMEDA Metamodel**

## Example of an FMEDA Spreadsheet Extract

### Part

<table>
<thead>
<tr>
<th>ISO Element</th>
<th>Failure Rate</th>
<th>Function</th>
<th>Failure Mode</th>
<th>Failure Distribution</th>
<th>Failure Type</th>
<th>Failure Effect</th>
<th>Severity</th>
<th>Safety Measure</th>
<th>Diagnostic Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALU</td>
<td>0.348 FIT</td>
<td>Ft. 1</td>
<td>FM1</td>
<td>25%</td>
<td>HE</td>
<td>FE1</td>
<td>Negligible</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FM2</td>
<td>25%</td>
<td>HE</td>
<td>FE2</td>
<td>Dangerous</td>
<td>SM1</td>
<td>90%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Ft. 2</td>
<td>50%</td>
<td>SE</td>
<td>FE4</td>
<td>Negligible</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Conducted based on correlations with FMEDA flow and documentation.
Link to Fault Injection and Simulation (1/2)

- **Safety Evaluation**
- **Basic Element Groups**
  - **Targets**
  - **Threats**
  - **Counter-measures**

- **System parts**
- **Failure modes**
- **Failure effects**
- **Undesired events**
- **Safety measures**

- **Probabilistic safety analysis**
- **Fault injection and simulation**

- **Sensitivity zones**
- **Injection points**
- **Observation points**
- **Diagnostic points**

- **Risks?**
- **Actions?**

- System elements or functions that must be protected to ensure the safe operation of the system.
- Malfunctions, discrepancies, and failures against which the targets must be protected.
- Mechanisms and measures used to protect the targets and mitigate the threats.
# Link to Fault Injection and Simulation (2/2) – Data Mapping

## Targets
- Parts, Functions (FMEDA), Elements (DFA)

## Threats
- Failure modes (FMEDA), Dependent failures (DFA), Events (FTA)
- Failure Effects (FMEDA/DFA), Events (FTA)

## Counter-measures
- Safety measures (FMEDA, DFA)

## Safety Analysis

## Fault Injection
- Modules, Submodules, Entities, Components...
- Injection points (signals, ports, variables, sockets, processes...)
- Observation points (signals, ports...)
- Diagnostic and correction points (modules, submodules, signals...)

---

**Condition:** full model consistency

**Object in safety analysis model**
- **ID:** ~
- **Name:** ~
- **Description:** ~

**Object in system model**
- **ID:** ~
- **Name:** ~
- **Description:** ~

**Detect potential candidates**
**Selection by user**
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.