Hazard-based Selection of Test Cases
Functional Safety of Mechatronic Systems

Mario Gleirscher

Software & Systems Engineering
Institut für Informatik
Technische Universität München

May 24, 2011
Safety Case\(^1\): Assurance of an Airbag Control

Machine \(I\): An airbag system . . .

\(^1\)Cf. Safety case management [Kel98]  
\(^2\)Cf. [Wik11]
Safety Case¹: Assurance of an Airbag Control

Machine I: An airbag system . . .

Safety Case G: Does the airbag release iff it’s intended?

¹Cf. Safety case management [Kel98]
²Cf. [Wik11]
Safety Case\textsuperscript{1}: Assurance of an Airbag Control

Machine \textit{I}: An airbag system . . .

Context \textit{E}: . . . in a car operated out in a street by a human driver.

\textquotedblleft . . . functional safety methods have to extend to non-E/E/PS parts of the system . . . \textquotedblright \textsuperscript{2}

\textquotedblleft . . . functional safety can[not] be determined without considering the environment . . . \textquotedblright \textsuperscript{2}

\textsuperscript{1} Cf. Safety case management [Kel98]
\textsuperscript{2} Cf. [Wik11]
1 **Functional Safety**
   System Modelling
   Property Analysis and Specification

2 **Hazards**
   Property Analysis and Specification
   Test Case Selection

3 **Conclusion**
1. **Functional Safety**
   System Modelling
   Property Analysis and Specification

2. **Hazards**
   Property Analysis and Specification
   Test Case Selection

3. **Conclusion**
Functional model $M_W$:

$M_I$ describing the mechatronic system $I$ and $M_E$ describing its operational environment $E$.

\[^1\text{Cf. [Bro10].}\]
A system boundary allows interaction across shared phenomena:\(^1\):

\[ M_E \xrightarrow{\triangleright} M_I \triangleq \text{repaired(Airbag), refilled(Gas), signal(activate,Airbag), on(crashSensor), ...} \]

\[ M_E \xleftarrow{\blacktriangleright} M_I \triangleq \text{released(Airbag), ...} \]

where \( A \xrightarrow{\triangleright} B = \text{ctrVar}(A) \cap \text{monVar}(B) \).

\(^1\text{Cf. [Jac01, PM95]}\)
A System Model $M_W$ of the Airbag World $W$

Supportive phenomena for safety modelling and measurement:

$M_E \setminus M_I \triangleq \text{crashed(Car), shocked(Car), deformed(Car), protected(Person), driving(Car), irritated(Passenger),} \ldots$

$M_I \setminus M_E \triangleq \text{empty(Airbag),} \ldots$
A System Model $M_W$ of the Airbag World $W$

Interface behaviour $\triangleq$ histories of shared phenomena states:

\[
\begin{array}{cc}
M_E & M_I \\
\end{array}
\]

<table>
<thead>
<tr>
<th>Intervals</th>
<th>...</th>
<th>n</th>
<th>...</th>
<th>...</th>
<th>n + j</th>
<th>...</th>
<th>m</th>
</tr>
</thead>
<tbody>
<tr>
<td>shocked(Car)</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>deformed(Car)</td>
<td>0</td>
<td>2</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>crashed(Car)</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>signal(crash)</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>released(Airbag)</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5/20 Hazard-based Selection of Test Cases Mario Gleirscher
Motivation

Functional Safety

Hazards

Conclusion

MW as a Test Model

Where to get the information?

System use cases  →  MI, ME
Domain and context analysis  →  ME

Independent control states, transitions with action preconditions and effects\(^1\).

\(^1\)Details in GOLOG script, cf. [Rei01].
Motivation

Functional Safety

Hazards

Conclusion

$M_W$ as a Test Model

$M_E$

$M_I$

Problem: Which of $M_W$’s possible or mutated transitions may obstruct safety in $M_E$?

1Details in GOLOG script, cf. [Rei01].

Independent control states, transitions with action preconditions and effects.
Motivation

Functional Safety

Hazards

Conclusion

Functional Safety in $M_W$

Functional safety goal

Behavioral property to globally maintain (or avoid) in $E$, formally: $\square \phi$

$G \triangleq \square \text{protected}(\text{Body})$

$G' \triangleq \square [\text{crashed}(\text{Car}) \rightarrow \Diamond <400ms \text{absorbed}(\text{Body}) \land \Box \neg \text{crashed}(\text{Car}) \rightarrow \Box \neg \text{released}(\text{Airbag})]$

$3$Cf. [MP95].
**Functional Safety in $M_W$**

**A/G safety specification**

$G$ split into **Assumptions for $E$** and **Guarantees for $I$**, formally: $\bigvee_i As_i \rightarrow Gr_i \models G$

$As_1 \triangleq \square[crashed(Car) \leftrightarrow \bullet signal(crash)]$

... "reliable crash sensing expected from $E$"

$Gr_1 \triangleq \square[signal(crash) \leftrightarrow \diamond <200 ms released(Airbag)]$

... "reliable bag disengaging required from $I$"
1. **Functional Safety**
   - System Modelling
   - Property Analysis and Specification

2. **Hazards**
   - Property Analysis and Specification
   - Test Case Selection

3. **Conclusion**
Obstacles$^2$ to Functional Safety in $M_W$

What obstructs a functional safety goal $G$ in $W$?

Hazard $H$  Risk of human or environmental harm in $E$

$H_1 \rightarrow G'$ \; $\triangleq \; \Diamond[\text{crashed}(\text{Car}) \; \land \; \bullet \text{harmed}(\text{Person})]$  

$H_2 \rightarrow G'$ \; $\triangleq \; \Diamond[\neg \text{crashed}(\text{Car}) \; \land \; \bullet \text{harmed}(\text{Person})]$

$^2$Automated inference possible, e.g. [Let01].
Obstacles\(^2\) to Functional Safety in \(M_W\)

How can such obstructions happen in \(W\)?

Hazardous state \(\sigma\) State of \(M_E\) (or \(M_E \cap M_I\)) leading to \(H\)

\[
\begin{align*}
\sigma_{H_1 G} & \triangleq \text{signal(crash)} \rightarrow \neg \text{released(Airbag)} \\
\sigma_{H_2 G} & \triangleq \neg \text{signal(crash)} \rightarrow \text{released(Airbag)} \\
\sigma_{H_3 A} & \triangleq \text{crashed(Car)} \rightarrow \neg \text{signal(crash)} \\
\sigma_{H_4 A} & \triangleq \neg \text{crashed(Car)} \rightarrow \text{signal(crash)}
\end{align*}
\]

\(^2\)Automated inference possible, e.g. [Let01].
Obstacles\textsuperscript{2} to Functional Safety in $M_W$

**How** can such obstructions be generated from $M_W$?

![Diagram](image)

**Hazardous state** $\sigma$  
State of $M_E$ (or $M_E \cap M_I$) leading to $H$

- $\sigma_{H_1G}$ $\triangleq signal(crash) \rightarrow ¬released(Airbag)$
- $\sigma_{H_2G}$ $\triangleq ¬signal(crash) \rightarrow released(Airbag)$
- $\sigma_{H_3A}$ $\triangleq crashed(Car) \rightarrow ¬signal(crash)$
- $\sigma_{H_4A}$ $\triangleq ¬crashed(Car) \rightarrow signal(crash)$

\textsuperscript{2}Automated inference possible, e.g. [Let01].
Defects concerning Functional Safety

Causes of (hazardous) system failures:

\[
M_W \quad (as \ specified)
\]

\[
M_E \rightarrow M_I
\]

\[
W \quad (as \ built & \ run)
\]

\[
E \rightarrow I
\]

\[
M_W \quad (as \ intended)
\]

\[
M_E \rightarrow M_I
\]

a) Potential bug or runtime error.

Assurance by system testing too weak and incomplete.
Defects concerning Functional Safety

Causes of (hazardous) system failures:

- **MW** (as specified)
  - **ME**
  - **MI**

- **W** (as built & run)
  - **E**
  - **I**

- **MW** (as intended)
  - **ME**
  - **MI**

b) **Requirements error**, e.g. wrong assumption or guarantee; wrong, incomplete or missing transition.

Assurance by requirements validation.

10/20

Hazard-based Selection of Test Cases

Mario Gleirscher
Defects concerning Functional Safety

Causes of (hazardous) system failures:

MW (as specified)

ME MI

W (as built & run)

E I

MW (as intended)

ME MI

(Im)mature Specs

Realization

c) Bug or runtime error.

Assurance by automated system testing strengthened by validation.
Assure Functional Safety $G$ of a Machine $I$ in a Context $E$

**Constructive Safety Assurance (Requirements Engineer)**

1. **Safety risks**: Does the airbag’s behaviour cause hazards?
2. **Hazardous exceptions**: Is it completely specified?
3. **Automation**: How to systematically explore such situations?
4. **How can they be avoided or kept at minimum risk?**

**Analytic Safety Assurance (Test Engineer)**

1. **Selection**: How to test beyond the airbag’s specification?
2. **Coverage**: Have all relevant situations be explored, i.e. does an airbag’s realization exhibit hazardous behaviour?
3. **How to mutate $M_W$ to get interesting test cases?**
4. **How to automatically generate and execute them?**
Assure Functional Safety $G$ of a Machine $I$ in a Context $E$

**Constructive Safety Assurance (Requirements Engineer)**

1. **Safety risks**: Does the airbag’s behaviour cause hazards?
2. **Hazardous exceptions**: Is it completely specified?
3. **Automation**: How to systematically explore such situations?
4. **How can they be avoided or kept at minimum risk?**

**Analytic Safety Assurance (Test Engineer)**

1. **Selection**: How to test beyond the airbag’s specification?
2. **Coverage**: Have all relevant situations be explored, i.e. does an airbag’s realization exhibit hazardous behaviour?
3. **How to mutate $M_W$ to get interesting test cases?**
4. **How to automatically generate and execute them?**
Hazard-based Test Case Specifications as Test Goals

Notions relevant for testing-based safety assurance:

\[ t = \text{action sequence possible in } M_W \]

\[ \mathcal{T} = \text{set of test cases, e.g.:} \]

\[ \langle \text{collide, release} \rangle, \langle \text{release, looseControl} \rangle, \ldots \]

\[ \tau = \text{state expression over phenomena capturing a test goal} \]

\[^3\text{Cf. [Bri10, Pre03].}\]
Hazard-based Test Case Specifications as Test Goals

Specifying negative test cases $t$ based on a hazardous state $\sigma$:

Informal: Are there test sequences based on $M_W$ that exhibit unwanted airbag behaviour?

Formal: $\tau_1 \triangleq (\exists t). \sigma_{H_2 G} \models H$
$\triangleq (\exists t). \neg \text{signal(crash, } t) \rightarrow \text{released(Airbag, } t)$
Validate $M_W$ and Generate Test Cases

Generate test cases of length 7 in \texttt{GOLOG}:

\[
\text{propOfInterest}(T) :- \text{not(signal(crash,T))}, \\
\text{released(Airbag,T)}.
\]

\[
\text{do(testcontrol(7),s0,T), propOfInterest(T)}.
\]

The selection results in a suite $\mathcal{T}_{\tau_1}$ leading to $\sigma_{H_2G}$, e.g.:

\[
\cong \langle \text{activate, boot, collide, activate, release} \rangle
\]

\[
T = \text{do(step, do(release(airbag1),} \\
\text{do(step, do(activate(airbag2),} \\
\text{do(step, do(collide(_G110, _G111),} \\
\text{do(step, do(boot(airbag1),} \\
\text{do(step, do(activate(airbag1), s0))))))))))))
\]

**Local coverage** yields all paths in $M_W$ to $\sigma_{H_2G}$. 

Hazard-based Selection of Test Cases

Mario Gleirscher
1 Functional Safety
   System Modelling
   Property Analysis and Specification

2 Hazards
   Property Analysis and Specification
   Test Case Selection

3 Conclusion
A Strategy to select Safety-critical Test Cases

1. Capture safety goals
2. Analyse hazards
3. Build up system model
4. Specify test goals
5. Generate test cases
6. Execute test cases
7. Inspect results
8. Fix defects
A Strategy to select Safety-critical Test Cases

Capture safety goals → Analyse hazards → Build up system model → Specify test goals → Generate test cases → Execute test cases → Inspect results → Fix defects
Further Work

1. Treatment of sets of safety goals or A/G safety specifications,
2. Isolated assurance of a feature,
Contribution to Solving AST Model Problems\textsuperscript{3} . . .

. . . REQ 1&2: How to cover safety requirements by tests?

. . . INT 8: How to observe architecture to test for functional safety defects?

. . . INT 10: How to test for hazards?


References II


[MP95] Zohar Manna and Amir Pnueli.  

[PM95] David Parnas and J. Madey.  

*Zum modellbasierten, funktionalen Test reaktiver Systeme.*  
Dissertation, Technische Universität München, Faculty of Informatics, 2003.

[Rei01] Raymond Reiter.  
*Knowledge in Action: Logical Foundations for Specifying and Implementing Dynamical Systems.*  
Functional safety — wikipedia, the free encyclopedia, 2011.
[Online; accessed 15-May-2011].