Implicit Intermittent Fault Detection in Distributed Systems

Peter Waszeckii, Matthias Kauer, Martin Lukasiewycz, Samarjit Chakraborty
Motivation: Faults in Automotive Electronics

Acura TSX Recalled in Canada for ECU Problems
Mar 19, 8:32 PM

Kawasaki Recalls Ninja 300 Again Due To ECU Issue
on AUGUST 16 2013, 12:44 PM

Volvo Recalls 26,000 Cars Worldwide Due to Faulty Software

"We've demonstrated how as little as a single bit flip can cause the driver to lose control of the engine speed in real cars due to software malfunction that is not reliably detected by any fail-safe," Michael Barr, CTO and co-founder of Barr Group, told us in an exclusive interview. Barr served as an expert witness in this case.

As expected, owners of the aforementioned models are informed by the Swedish manufacturer through a letter that asks them to bring the cars to dealers and install a software update. Approximately 12,000 vehicles are in the United States, just-auto.com wrote.

A similar recall was announced by Volvo in June, but it only concerned 2008 and 2009 S80, V70 and XC70.

"The engine cooling fan may stop working due to a software programming error in the fan control module (ECM)," NHTSA wrote in the advisory. "Depending on driving conditions, the customer may experience reduced air conditioning performance and/or rapid increase in engine coolant temperature."

"We've demonstrated how as little as a single bit flip can cause the driver to lose control of the engine speed in real cars due to software malfunction that is not reliably detected by any fail-safe," Michael Barr, CTO and co-founder of Barr Group, told us in an exclusive interview. Barr served as an expert witness in this case.
Outline

Introduction
• Automotive electrical/electronic architectures
• Importance of reliable distributed systems

Faults in Semiconductor Devices
• Types and causes of faults
• Fault-rate development

Implicit Detection of Intermittent Faults
• Development of the expectation matrix
• Detection methods

Implementation of the Detection Approach
• Case study
• Experimental results

Conclusion
Increasing Significance of Automotive E/E Architectures

Costs of Automotive Electronics

Cost of Electronics vs. Total cost of a car

- 1980
- 2005
- 2015

Costs of Electronics:
- 0%
- 20%
- 40%
- 60%
- 80%
- 100%

Total cost of a car:
- 0%
- 20%
- 40%
- 60%
- 80%
- 100%

[Paul Milbredt, AUDI AG, EFTA 2010 - Switched FlexRay: Increasing the Effective Bandwidth and Safety of FlexRay Networks]
[Françoise Simonot-Lion, IEEE IES'2006 – The Design of Safe Automotive Electronic Systems]
New distributed E/E architectures ...

**TODAY**
Federated E/E architectures based on many single-core ECUs

**TOMORROW**
Integrated E/E architectures based on multi-core ECUs

Paradigm shift

ECU consolidation
... come along with new challenges!

- **Reliability**
  - Extended component life-time

- **Predictability**
  - X-by-wire systems

- **Performance**
  - Shrinking component geometries

- **Interm./perm. Faults**
  - Increased Fault Susceptibility
Types and Causes of Faults

**Transient**
- Strong radiation
- EM interference

**Intermittent**
- Process variation
- Electromigration

**Permanent**
- Irreversible changes
  - Preceded by intermittent faults

[Constantinescu, Trends and Challenges in VLSI Circuit Reliability, 2003]
Fault Rate Development

Distribution

Observation

Expectation

Detection

transient faults

intermittent faults
Principle of the Implicit Fault Detection

Task dependency graph:

- \( \tau_1 \rightarrow \tau_4 \)
- \( \tau_2 \rightarrow \tau_5 \)
- \( \tau_3 \rightarrow \tau_6 \)
- \( t_1 \rightarrow t_2 \)

Transient faults

Resource \( r_1 \):
- \( \tau_1 \)
- \( \tau_2 \)
- \( \tau_4 \)
- \( \tau_6 \)

Resource \( r_2 \):
- \( \tau_3 \)
- \( \tau_5 \)
- \( \tau_6 \)

Resource \( r_3 \):
- \( t_1 \)
- \( t_2 \)

Intermittent + Transient faults

Failure rate of plausibility tests in \( t_1 \) and \( t_2 \):

<table>
<thead>
<tr>
<th>Failure ratio ( \frac{t_1}{t_2} )</th>
<th>0.5</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faulty resource ( r_2 )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( r_1 )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( r_3 )</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Expectation Matrix

\[ \lambda(t, r) = \sum_{\tau \in T_r \cap \text{pred}(t)} \frac{e_\tau}{h_\tau} \mathbb{E}[X_r] \]

Frequency of a test \( t \in T \) failing due to a fault on resource \( r \in R \)

Expectation Matrix \( \Lambda = (\lambda(t, r))_{t,r} \)

\[
\begin{pmatrix}
\lambda_{t_1,r_1} & \lambda_{t_1,r_2} & \lambda_{t_1,r_3} & 0 & \lambda_{t_1,r_5} & 0 \\
0 & 0 & \lambda_{t_2,r_3} & \lambda_{t_2,r_4} & \lambda_{t_2,r_5} & 0
\end{pmatrix}
\]

\[
O_t \gg E_t = \Delta \sum_{r \in R} \lambda(t, r)
\]
Vector-based Detection Methods

**Expectation Matrix:**

\[
\Lambda^{[T \times |R|]} = \begin{pmatrix}
\lambda_{t_1, r_1} & \lambda_{t_1, r_2} & \cdots & \lambda_{t_1, r_{R-1}} & \lambda_{t_1, r_R} \\
\lambda_{t_2, r_1} & \lambda_{t_2, r_2} & \cdots & \lambda_{t_2, r_{R-1}} & \lambda_{t_2, r_R} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
\lambda_{t_{T-1}, r_1} & \lambda_{t_{T-1}, r_2} & \cdots & \lambda_{t_{T-1}, r_{R-1}} & \lambda_{t_{T-1}, r_R} \\
\lambda_{t_T, r_1} & \lambda_{t_T, r_2} & \cdots & \lambda_{t_T, r_{R-1}} & \lambda_{t_T, r_R}
\end{pmatrix}
\]

**Observation Vector:**

\[
v_{r_i} = \begin{pmatrix}
\lambda_{t_1, r_i} \\
\vdots \\
\lambda_{t_{T-1}, r_i} \\
\lambda_{t_T, r_i}
\end{pmatrix}
\]

**Observation Vector:**

\[
v_{oT} = \begin{pmatrix}
0_{t_1} \\
\vdots \\
0_{t_T}
\end{pmatrix}
\]

**Cosine Similarity**

\[
similarity = \cos(\theta)
\]

**Singular Value Decomposition**

\[
\Lambda_s^{[T \times 2]} = \begin{pmatrix}
\lambda_{t_1, r_i} & 0_{t_1} \\
\vdots & \vdots \\
\lambda_{t_T, r_i} & 0_{t_T}
\end{pmatrix}
\]

\[
\Lambda_s = U \Sigma V^T \quad \Sigma = \begin{pmatrix}
\sigma_1 & 0 \\
0 & \sigma_2
\end{pmatrix}
\]

**Similarity**

\[
similarity = 1? \quad r_i \text{ is faulty}
\]

\[
\text{rank}(\Sigma) < 2? \quad r_i \text{ is faulty}
\]

Tolerance intervals \(\epsilon_{\cos}\) and \(\epsilon_{\text{svd}}\) used to consider 'noise' from transient faults.
**ILP-based Detection Methods**

### Confidence Interval

The three-sigma rule defines the limits of the confidence interval $[\lambda_{lo}(Ot), \lambda_{hi}(Ot)]$.

- $Pr(\mu - 3\sigma \leq x \leq \mu + 3\sigma) \approx 0.9973$

### Pearson’s $\chi^2$-Test

Statistical hypothesis test

- **null hypothesis:** $H_0: Et \rightarrow Ot$

  “All observed test failures result from the expected test failures.”

- $\chi^2 = \sum_{t \in T} \frac{(O_t - Et)^2}{Et}$

#### Type I errors

<table>
<thead>
<tr>
<th>$H_0$ is true</th>
<th>$H_0$ is false</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>$H_0$ rejected</strong></td>
<td>false positive</td>
</tr>
<tr>
<td><strong>$H_0$ accepted</strong></td>
<td>correct</td>
</tr>
</tbody>
</table>

**$x_r$ indicates faulty resource $r$**

### Constraints

**minimize:** $\sum_{y_r \in \{0, 1\}} \sum_{r \in R} y_r$

subject to:

- $\forall t \in T : \lambda_{lo}(Ot) \leq \frac{E_t}{\Delta} \leq \lambda_{hi}(Ot)$
- $\forall t \in T : E_t = \sum_{r \in R} x_r \cdot \lambda(t, r)$
- $\forall r \in R : x_r \geq x_{var} \cdot y_r$
- $\forall r \in R : x_r \leq x_{var} + 10^{10} \cdot y_r$

**minimize:** $\sum_{y_r \in \{0, 1\}} \sum_{r \in R} y_r$

subject to:

- $\forall t \in T : x^2 = \sum_{t \in T} O_t^2 \cdot R_t - 2 \cdot O_t + E_t$
- $\forall t \in T : E_t \cdot R_t = 1$
- $\forall t \in T : E_t = \sum_{r \in R} x_r \cdot \lambda(t, r) \cdot \Delta$
- $\forall r \in R : x_r \geq x_{var} \cdot y_r$
- $\forall r \in R : x_r \leq x_{var} + 10^{10} \cdot y_r$
Case study

test case model:

<table>
<thead>
<tr>
<th>test cases</th>
<th>240</th>
</tr>
</thead>
<tbody>
<tr>
<td>resources</td>
<td>10 ... 100</td>
</tr>
<tr>
<td>tasks / resource</td>
<td>3 ... 10</td>
</tr>
<tr>
<td>tests / resources</td>
<td>1 ... 4</td>
</tr>
<tr>
<td>stressed / unstressed</td>
<td>50%</td>
</tr>
</tbody>
</table>

results

| correct | proper detection of stressed/unstressed system |
| false positive | unstressed resource detected as stressed |
| false negative | stressed resource not detected |
| timeout | test run aborted after 60s |
Experimental Results I

**Overall detection rate:**

- Evidence of feasibility of our approach
- Good overall detection rate for methods I, II and III
- Best results for vector-based methods
- $\chi^2$-Test promising when disregarding timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value 1</th>
<th>Value 2</th>
<th>Value 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\epsilon_{\text{cos}}$</td>
<td>$3.0 \cdot 10^{-3}$</td>
<td>$6.0 \cdot 10^{-3}$</td>
<td>$1.2 \cdot 10^{-2}$</td>
</tr>
<tr>
<td>$\epsilon_{\text{svd}}$</td>
<td>$4.3 \cdot 10^{-5}$</td>
<td>$8.50 \cdot 10^{-5}$</td>
<td>$1.70 \cdot 10^{-4}$</td>
</tr>
<tr>
<td>$x_{\text{var}}$</td>
<td>1.1</td>
<td>1.5</td>
<td>1000</td>
</tr>
</tbody>
</table>
Experimental Results II

- Vector-based approaches in millisecond range
- Conf. Int. method in sub-second range
- Runtime for $\chi^2$ -Test might be reduced by non-linear solver

- Good detection rate for methods I, II and III
- Slight decline due to false positives when test-number is high
- $\chi^2$ -Test distorted due to limited number of test results
Growing importance of distributed architectures
   • fault-detection is inevitable

Detection approach proposed
   • early and implicit diagnosis of intermittent faults
   • vector-based and ILP-based implementations

Experimental results prove feasibility
   • based on 240 test cases
   • good results for the first three methods

Future work
   • simultaneous detection of multiple faulty resources
   • different fault rates and fault propagation models
Thank you for your attention!

“Questions are guaranteed in life; answers aren't!”