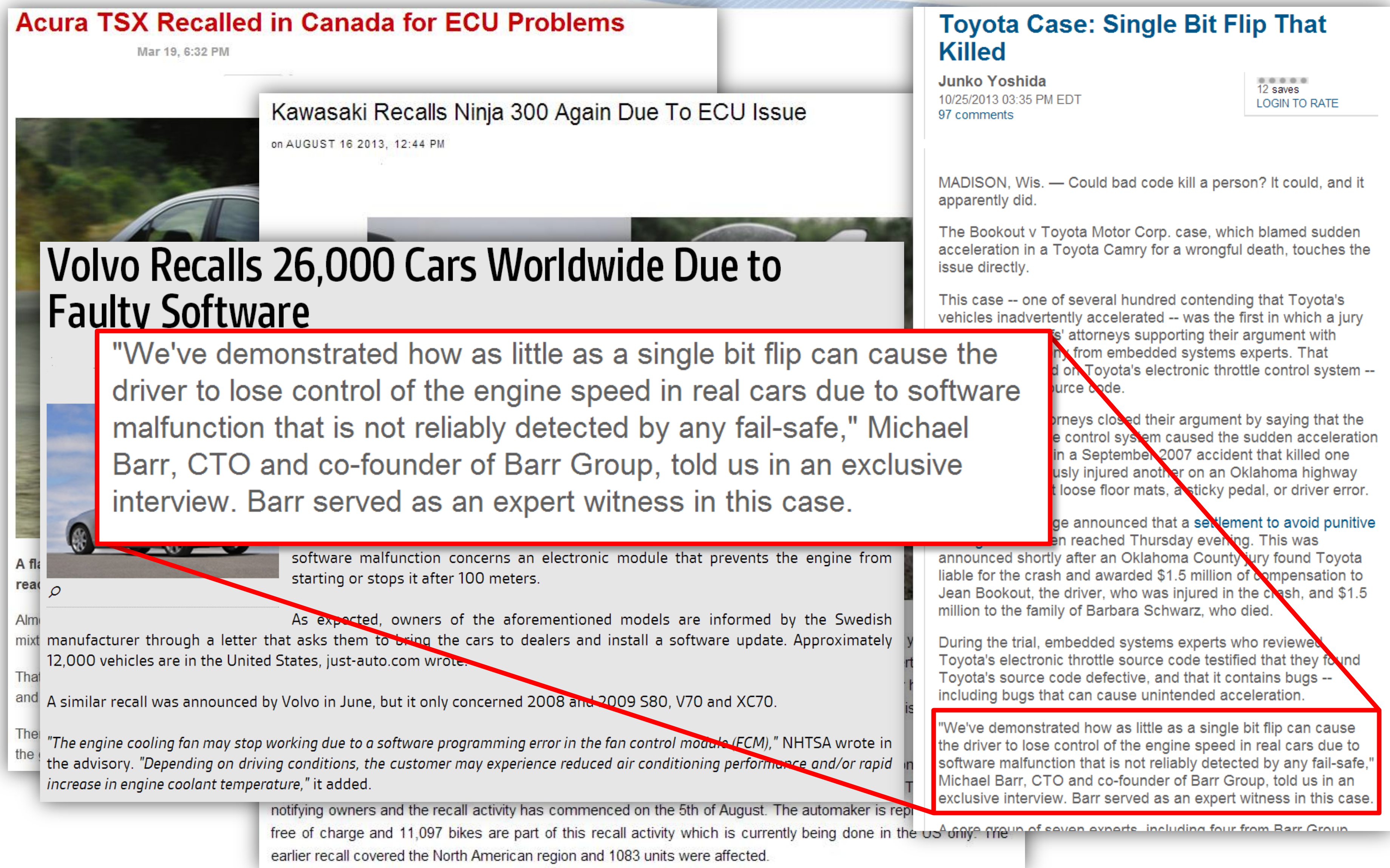
Implicit Intermittent Fault Detection in Distributed Systems

Peter Waszecki, Matthias Kauer,
Martin Lukasiewycz, Samarjit Chakraborty

TUM CREATE
Research Center for Electromobility

Motivation: Faults in Automotive Electronics



Acura TSX Recalled in Canada for ECU Problems

Mar 19, 6:32 PM

Kawasaki Recalls Ninja 300 Again Due To ECU Issue

on AUGUST 16 2013, 12:44 PM

notifying owners and the recall activity has commenced on the 5th of August. The automaker is rep... free of charge and 11,097 bikes are part of this recall activity which is currently being done in the US only. The earlier recall covered the North American region and 1083 units were affected.

Volvo Recalls 26,000 Cars Worldwide Due to Faulty Software

software malfunction concerns an electronic module that prevents the engine from starting or stops it after 100 meters.

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 (FCM)," 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,"* it added.

"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.

Toyota Case: Single Bit Flip That Killed

Junko Yoshida
10/25/2013 03:35 PM EDT
97 comments

12 saves
LOGIN TO RATE

MADISON, Wis. — Could bad code kill a person? It could, and it apparently did.

The Bookout v Toyota Motor Corp. case, which blamed sudden acceleration in a Toyota Camry for a wrongful death, touches the issue directly.

This case -- one of several hundred contending that Toyota's vehicles inadvertently accelerated -- was the first in which a jury ...s' attorneys supporting their argument with ...ny from embedded systems experts. That ...d on Toyota's electronic throttle control system -- ...urce code.

...rneys closed their argument by saying that the ...e control system caused the sudden acceleration ...in a September 2007 accident that killed one ...usly injured another on an Oklahoma highway ...t loose floor mats, a sticky pedal, or driver error.

...ge announced that a settlement to avoid punitive ...en reached Thursday evening. This was announced shortly after an Oklahoma County jury found Toyota liable for the crash and awarded $1.5 million of compensation to Jean Bookout, the driver, who was injured in the crash, and $1.5 million to the family of Barbara Schwarz, who died.

During the trial, embedded systems experts who reviewed Toyota's electronic throttle source code testified that they found Toyota's source code defective, and that it contains bugs -- including bugs that can cause unintended acceleration.

"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.

A core group of seven experts, including four from Barr Group...

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

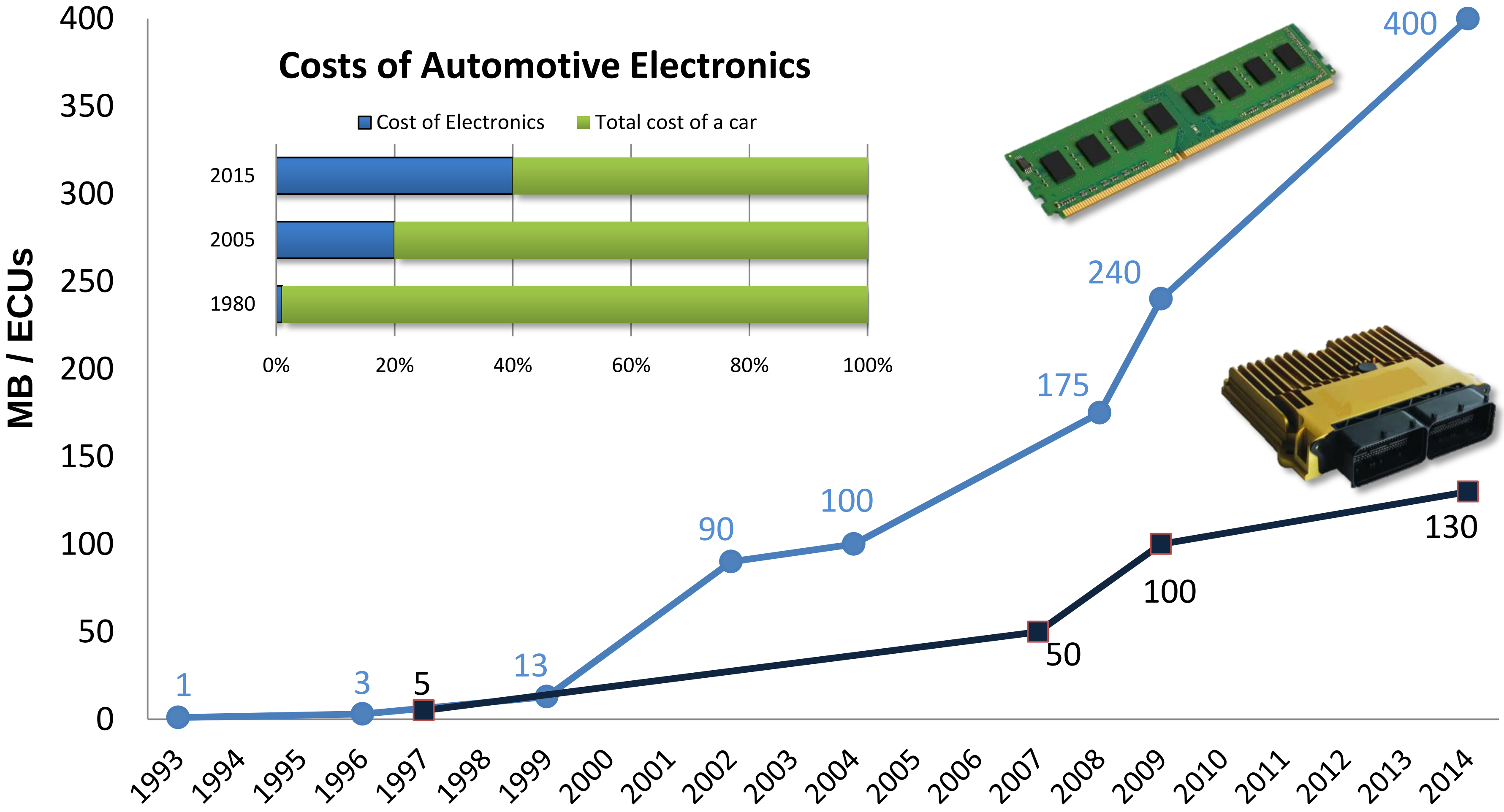
- Development of the expectation matrix
- Detection methods

Implementation of the Detection Approach

- Case study
- Experimental results

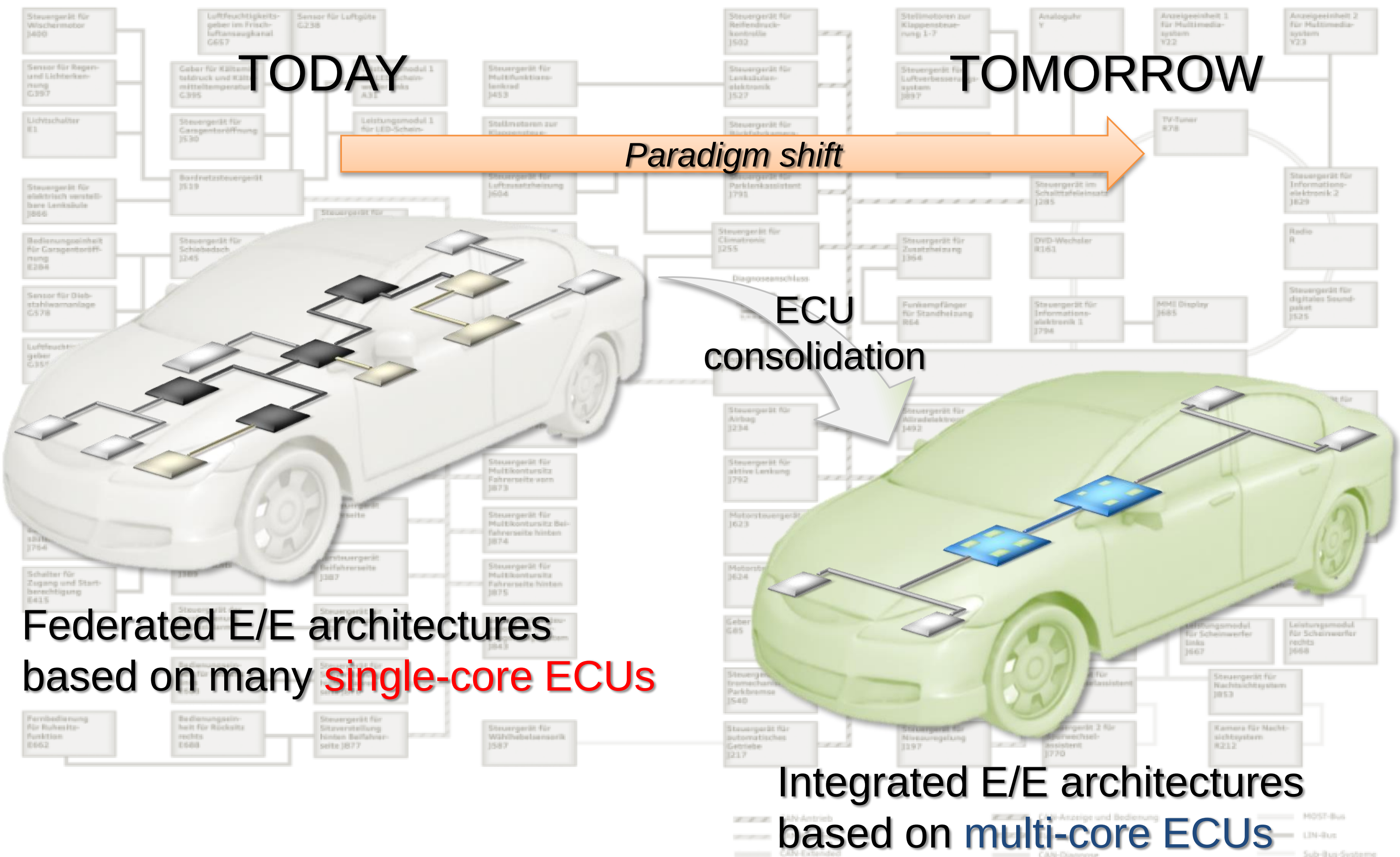
Conclusion

Increasing Significance of Automotive E/E Architectures

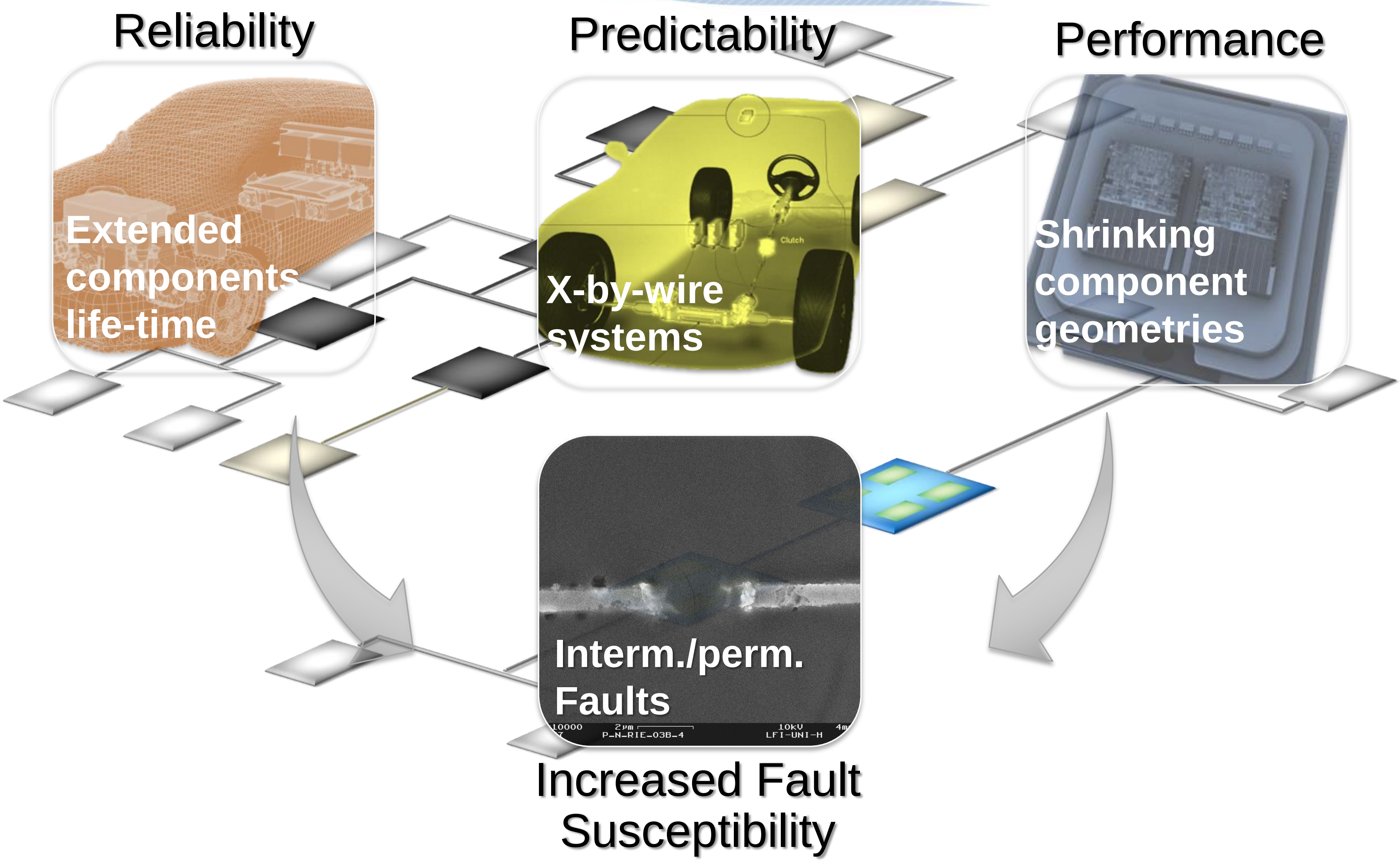


[Paul Milbredt, AUDI AG, EFTA 2010 - Switched FlexRay: Increasing the Effective Bandwidth and Safety of FlexRay Networks]
[Françoise Simonot-Lion, IEEE IES'2006 – The Design of Safe Automotive Electronic Systems]

New distributed E/E architectures ...

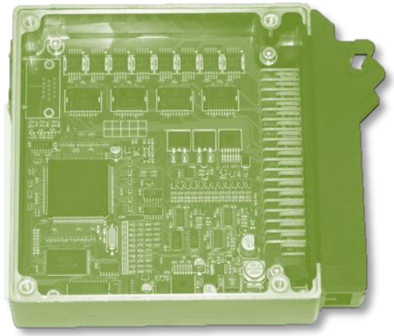


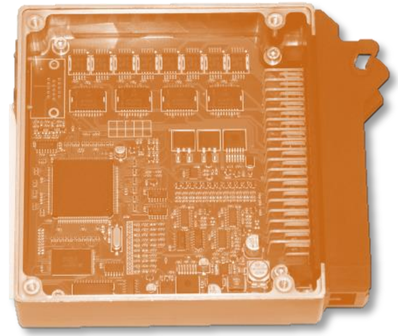
... come along with new challenges!

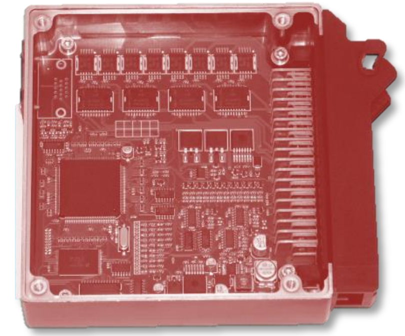


Types and Causes of Faults

Transient	Intermittent	Permanent



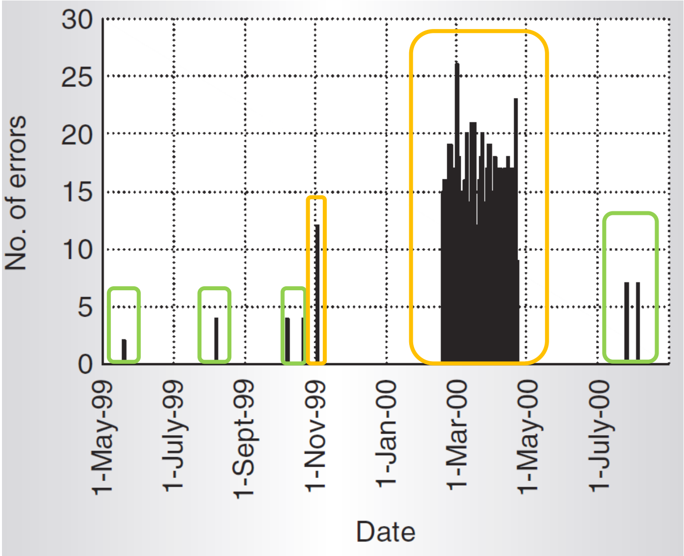




Temporal conditions
- strong radiation
- EM interference

Marginal hardware
- process variation
- electromigration

Irreversible changes
- preceded by intermittent faults



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

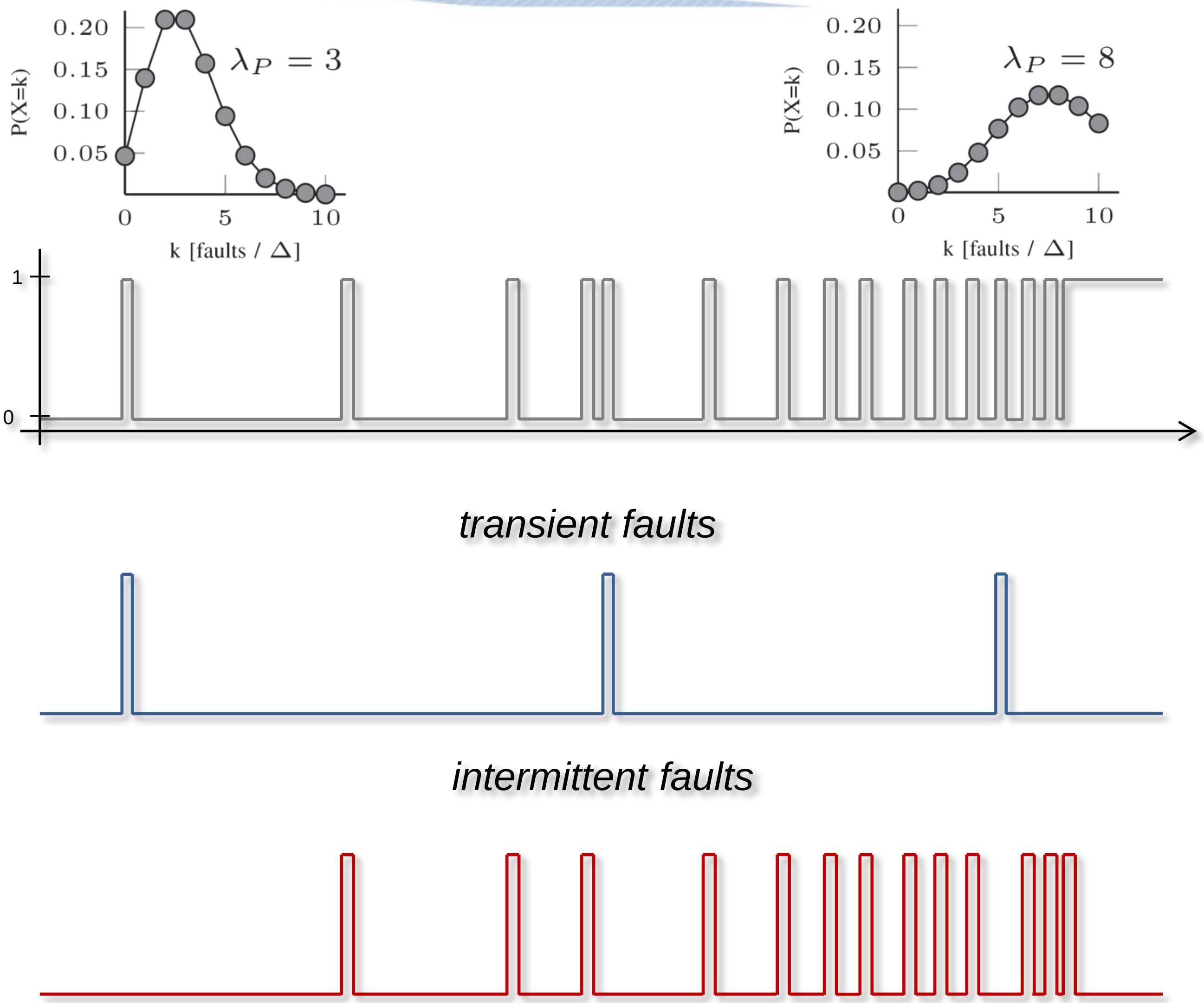
Fault Rate Development

Distribution

Observation

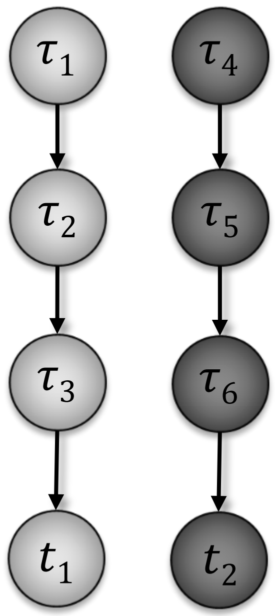
Expectation

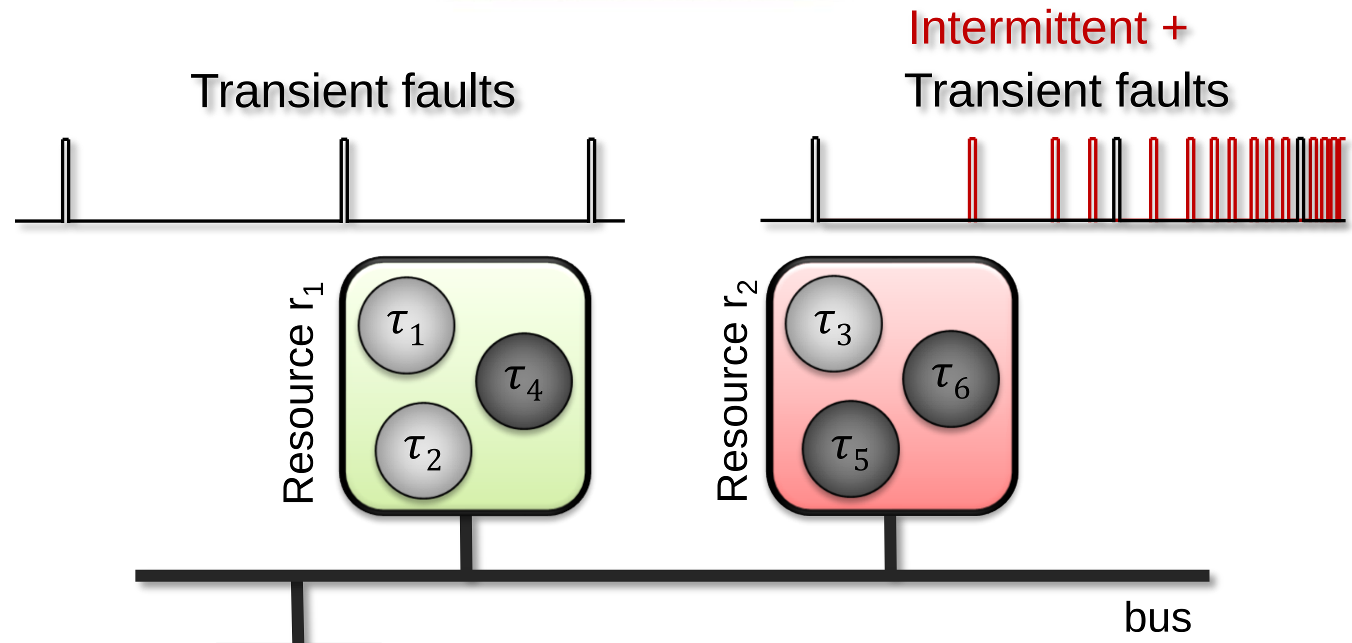
Detection

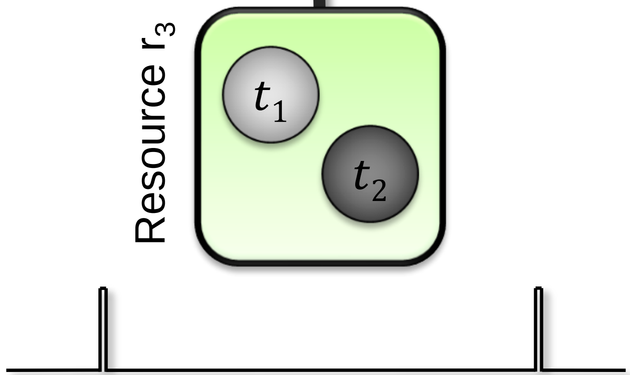


Principle of the Implicit Fault Detection

Task dependency graph:



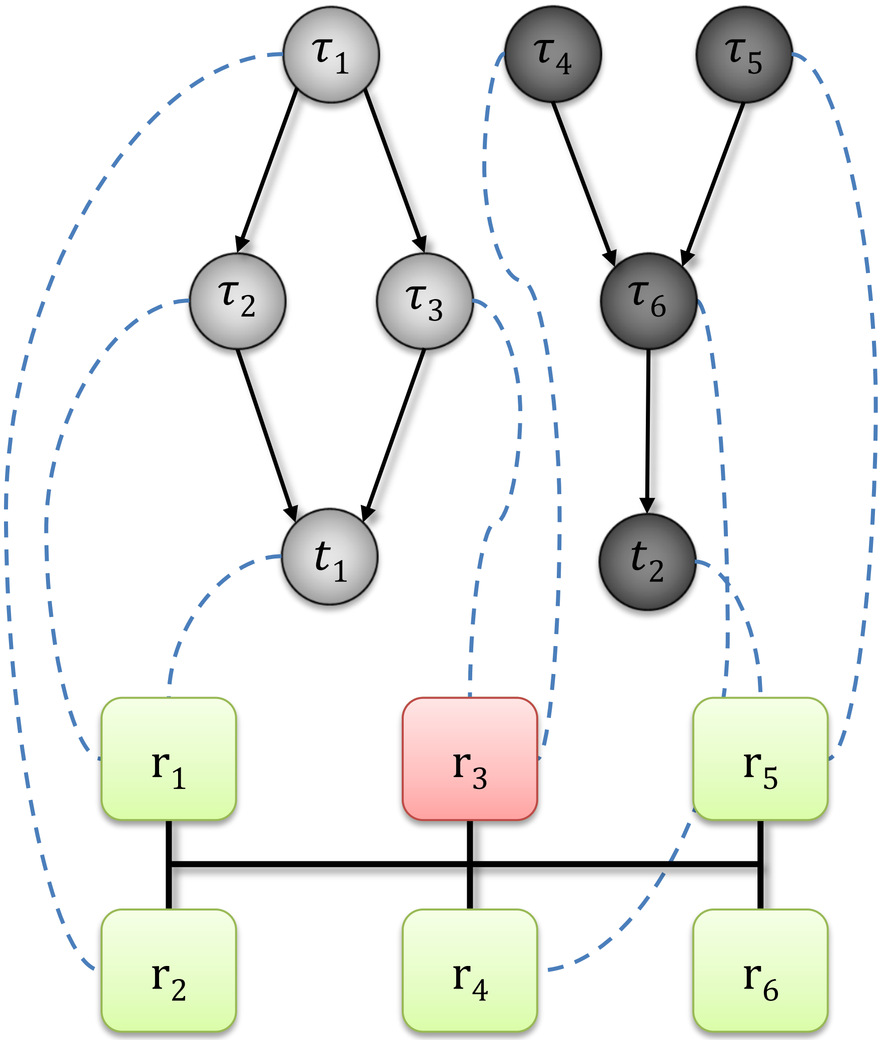




Failure rate of plausibility tests in t_1 and t_2 :

Failure ratio $\frac{t_1}{t_2}$	0.5	2	1
Faulty resource	r_2	r_1	r_3

Expectation Matrix



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

$$\lambda(t,r) = \sum_{\tau \in \mathrm{T}_r \cap pred(t)} \frac{e_\tau}{h_\tau} \mathrm{E}[X_r]$$

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:

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

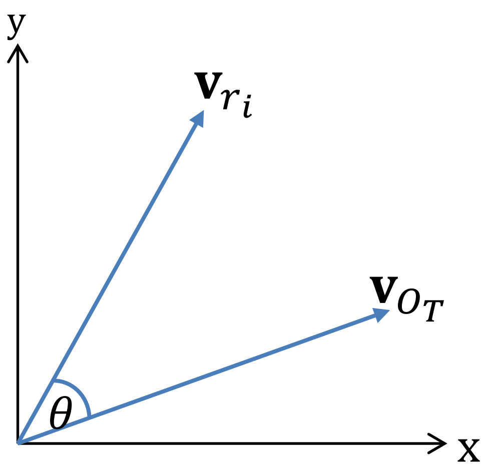
expectation vector:

$$\mathbf{v}_{r_i} = \begin{pmatrix} \lambda_{t_1,r_i} \\ \vdots \\ \lambda_{t_T,r_i} \end{pmatrix}$$

observation vector:

$$\mathbf{v}_{O_T} = \begin{pmatrix} O_{t_1} \\ \vdots \\ O_{t_T} \end{pmatrix}$$

Cosine Similarity



$$\boldsymbol{similarity} = \mathbf{cos}(\boldsymbol{\theta})$$

$similarity = 1?$ ⇨ **r_i is faulty**

Singular Value Decomposition

$$\Lambda_s{}^{|T|\times 2} = \begin{pmatrix} \lambda_{t_1,r_i} & O_{t_1} \\ \vdots & \vdots \\ \lambda_{t_T,r_i} & O_{t_T} \end{pmatrix}$$

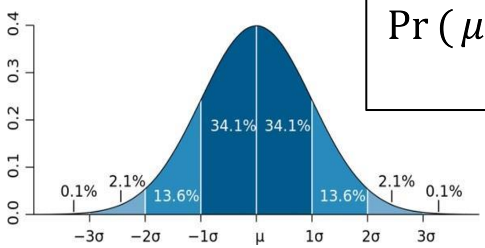
$$\boldsymbol{\Lambda_s = U\Sigma V^T} \longrightarrow \boldsymbol{\Sigma} = \begin{pmatrix} \boldsymbol{\sigma_1} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{\sigma_2} \end{pmatrix}$$

$rank(\Sigma) < 2?$ ⇨ **r_i is faulty**

Tolerance intervals $\epsilon_{\cos}$ and ϵ_{svd} used to consider ‘noise’ from transient faults.

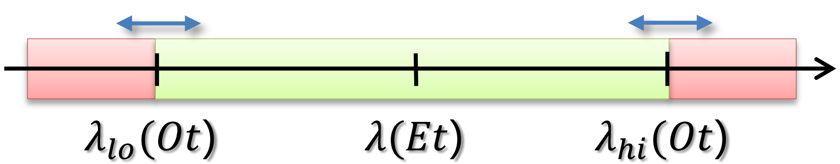
ILP-based Detection Methods

Confidence Interval



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

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



$$\underset{y_r \in \{0,1\}}{\textit{minimize}} \quad \sum_{r \in R} y_r \qquad (13a)$$

subject to:

$$\forall t \in T: \quad \lambda_{lo}(O_t) \le \frac{E_t}{\Delta} \le \lambda_h$$

$$\forall t \in T: \quad E_t = \sum_{r \in R} x_r \cdot \lambda(t, r$$

$$\forall r \in R: \quad x_r \ge x_{\text{var}} \cdot y_r$$

$$\forall r \in R: \quad x_r \le x_{\text{var}} + 10^{10} \cdot y$$

Pearson's χ2 -Test

statistical hypothesis test

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

null hypothesis: $H_0: Et \rightarrow Ot$

"All observed test failures result from the expected test failures."

	H_0 is true	H_0 is false
H_0 rejected	false positive	correct
H_0 accepted	correct	false negative

$$\underset{y_r \in \{0,1\}}{\textit{minimize}} \quad \sum_{r \in R} y_r \qquad (17a)$$

subject to:

$$\forall t \in T: \quad \chi^2 = \sum_{t \in T} O_t^2 \cdot R_t - 2 \cdot O_t + E_t \qquad (17b)$$

$$\forall t \in T: \quad E_t \cdot R_t = 1 \qquad (17c)$$

$$\forall t \in T: \quad E_t = \sum_{r \in R} x_r \cdot \lambda(t, r) \cdot \Delta \qquad (17d)$$

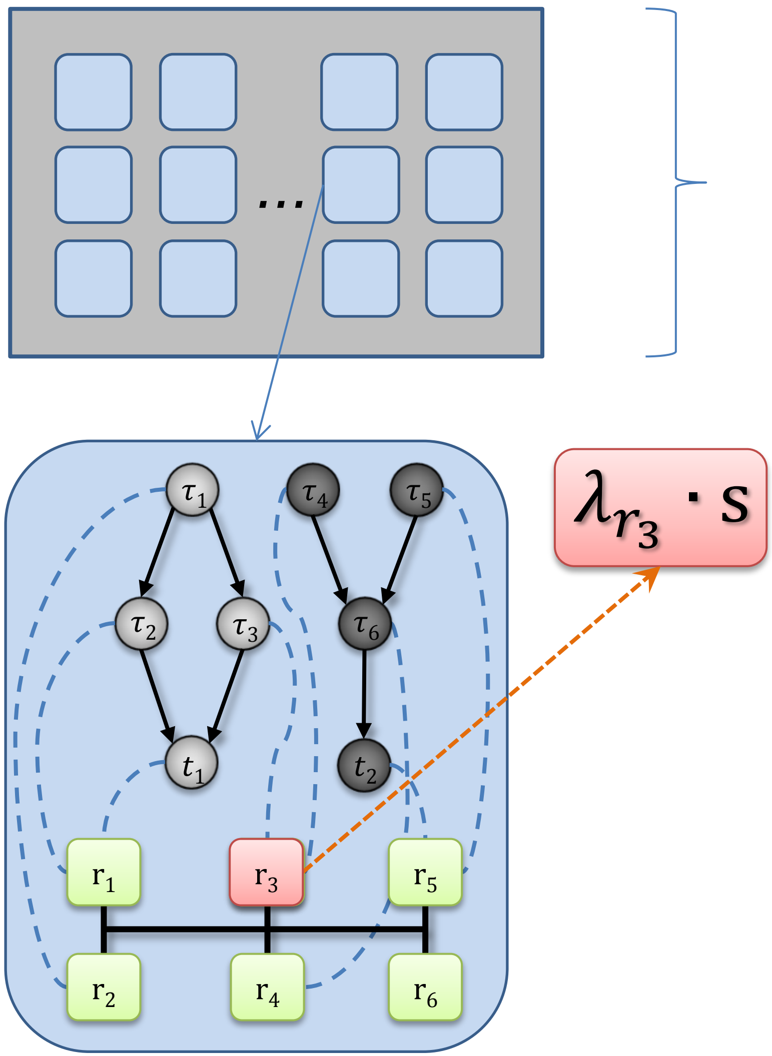
$$\forall r \in R: \quad x_r \ge x_{\text{var}} \cdot y_r \qquad (17e)$$

$$\forall r \in R: \quad x_r \le x_{\text{var}} + 10^{10} \cdot y_r \qquad (17f)$$

x_r indicates faulty resource r

Case study

test case model:



test cases	240
resources	10 ... 100
tasks / resource	3 ... 10
tests / resources	1 ... 4
stressed / unstressed	50%

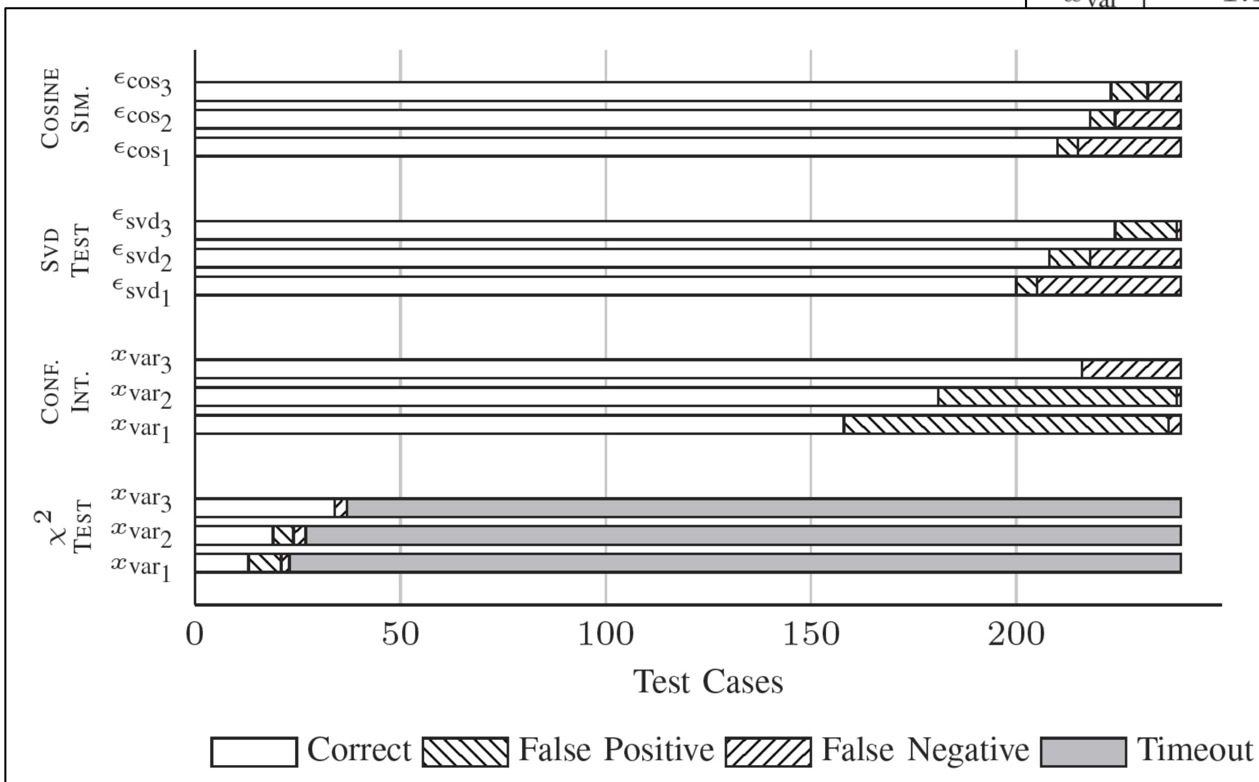
results	
correct	proper detection of stressed/unstressed system
false positive	unstressed resource detected as stressed
false negative	stressed resource not detected
timeout	test run aborted after 60s

Experimental Results I

parameter values:

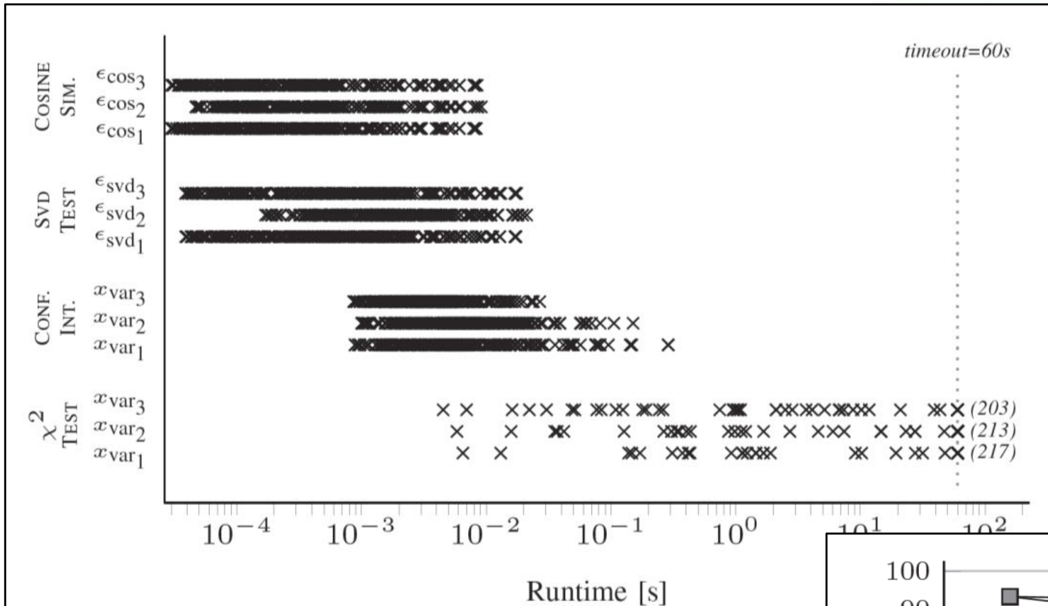
	Value 1	*Value 2*	*Value 3*
ϵ_{cos}	$3.0 \cdot 10^{-3}$	$6.0 \cdot 10^{-3}$	$1.2 \cdot 10^{-2}$
ϵ_{svd}	$4.3 \cdot 10^{-5}$	$8.50 \cdot 10^{-5}$	$1.70 \cdot 10^{-4}$
x_{var}	1.1	1.5	1000

overall detection rate:



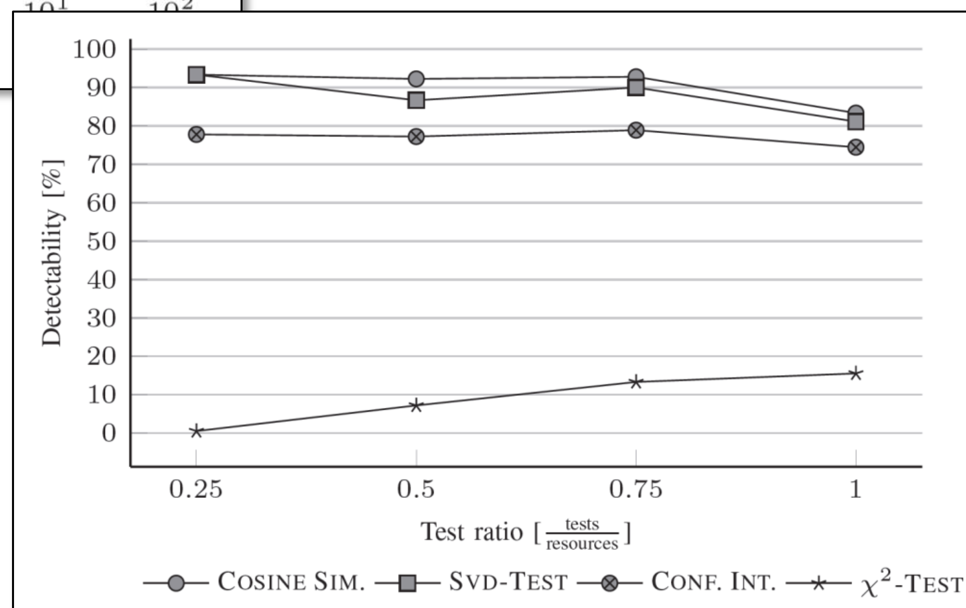
- evidence of feasibility of our approach
- good overall detection rate for methods I, II and III
- best results for vector-based methods
- χ2 –Test promising when disregarding timeout

Experimental Results II



- Vector-based approaches in millisecond range
- Conf. Int. method in sub-second range
- Runtime for χ2 –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
- χ2 –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!"