Why do we need embedded software resilience?

Distributed and Secure Software (DistriNet), Bruges campus;
Associate professor Faculty of Engineering Technology;
Departmental vice chair Department of Computer Science

Jeroen Boydens
Department of Computer Science
Faculty of Engineering Technology
KU Leuven, Belgium

Jeroen.Boydens@kuleuven.be
Content

- KU Leuven
- Introduction
- Symptoms of Soft Errors
- What are Soft errors?
- Our Research
- Research Projects
- Relevant Publications
Inspiring the outstanding
KU Leuven

1425
Foundation by Papal Bull

1816
Refoundation as a state university under Dutch rule

1911
First lectures in Dutch

1970
Division of the university into KU Leuven and U.C.Louvain

2013
KU Leuven expands to include academic degree programmes hosted at university colleges within KU Leuven Association

1797
Abolition by the French authorities

1834
Restoration as a Catholic university

1965
Foundation of Kulak

2008
6 university colleges of the KU Leuven Association sign an agreement to join their educational programmes in the Associated Faculty of Engineering Technology and Bioscience Engineering
A highly ranked university

#1
in the Reuters World Ranking of Most Innovative Universities in Europe (2019)

#84
in the QS World University Ranking (2021)

#45
in the Times Higher Education World University Ranking (2021)

#5 ranked university in the European Commission Horizon 2020 programme (HEI only)

#17 ranked university in the ERC grants programme with over 110 projects (HEI only)

*Last updated: June 2020*
Europe’s most innovative university

#1 REUTERS Ranking of Most Innovative Universities in Europe
1. KU Leuven
2. University of Erlangen Nuremberg
3. Imperial College London
4. University of Cambridge
5. EPFL
6. University College London
7. Technical University of Munich
8. University of Manchester
9. University of Zürich
10. Swiss Federal Institute of Technology Zurich

#7 REUTERS Ranking of Most Innovative Universities in the world
1. Stanford
2. MIT
3. Harvard
4. University of Pennsylvania
5. University of Washington
6. University of North Carolina Chapel Hill
7. KU Leuven
8. University of Southern California
9. Cornell University
10. Imperial College London
KU Leuven in numbers

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>STAFF</td>
<td>12,680</td>
</tr>
<tr>
<td>(KU LEUVEN)</td>
<td></td>
</tr>
<tr>
<td>RESEARCHERS</td>
<td>7,637</td>
</tr>
<tr>
<td>(UNIVERSITY HOSPITALS)</td>
<td></td>
</tr>
<tr>
<td>STUDENTS</td>
<td>60,057</td>
</tr>
<tr>
<td>INTERNATIONAL STUDENTS</td>
<td>12,421</td>
</tr>
<tr>
<td>ALUMNI</td>
<td>250,000+</td>
</tr>
<tr>
<td>SPIN-OFFs</td>
<td>135</td>
</tr>
</tbody>
</table>

*Last updated: June 2020
A comprehensive university

**FACULTIES**
16

**BACHELOR DEGREES**
48 (DUTCH)
5 (ENGLISH)

**MASTER DEGREES**
137 (DUTCH)
69 (ENGLISH)
1 (FRENCH)

**ADVANCED MASTERS**
19 (DUTCH)
23 (ENGLISH)
1 (SPANISH)

*Last updated: June 2020*
In the heart of Europe

TO LONDON
UNITED KINGDOM
120 MIN BY TRAIN

TO PARIS
FRANCE
90 MIN BY TRAIN

TO AMSTERDAM
THE NETHERLANDS
110 MIN BY TRAIN

TO COLOGNE
GERMANY
110 MIN BY TRAIN
13 campuses at 10 locations

Leuven
Group T Leuven Campus
Brussels Campus
Sint-Lucas Brussels Campus
Antwerp Campus
Diepenbeek Campus
Aalst Campus
Geel Campus
Ghent Technology Campus
Sint-Lucas Ghent Campus
De Nayer (Sint-Katelijne-Waver) Campus
Brugge Campus
KULAK Kortrijk Campus
KU Leuven Association

Collaboration between KU Leuven and five partner institutions spread across Flanders

MORE THAN 100,000 STUDENTS
LARGEST ASSOCIATION IN FLANDERS
43% OF THE STUDENT POPULATION IN FLANDERS
A global reach

12,421 INTERNATIONAL STUDENTS

1,788 INCOMING EXCHANGE STUDENTS

2,257 OUTGOING EXCHANGE STUDENTS

61 UNIVERSITY-WIDE AGREEMENTS

>2,200 FACULTY AGREEMENTS

>50 PROGRAMME AGREEMENTS

*Last updated: June 2020
Incoming students

Number of incoming degree seeking students 2014-2018
- > 1000
- 1000 - 500
- 500 - 250
- 250 - 100
- 100 - 50
- 50 - 10
- 10 - 1

Created with mapchart.net ©
Member of many acclaimed (inter)national networks
Hub of (inter)national networks

U21

1997

FOUNDED

27

MEMBERS

KEY CHARACTERISTICS

• Pioneer in educational innovation

• Strong research engagement by supporting the development of new international opportunities for emerging researchers

• Deliver internationally-focused opportunities for enhanced student engagement, both actual and virtual
Innovative research
RESEARCH EXPENSES
522 (MILLION EUROS)

HORIZON 2020 FUNDING
291 (IN MILLION EURO)

HORIZON 2020 PROJECTS
514

HORIZON 2020 PROGRAMME
#5 (HEI ONLY)

PHD DEGREES AWARDED
2 EVERY WORKING DAY
Research excellence

• KU Leuven: a leading European research university

TOP 10 HIGHER EDUCATION INSTITUTIONS based on number of Horizon 2020 projects

<table>
<thead>
<tr>
<th>Institution</th>
<th>Participations, June 30, 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIVERSITY OF CAMBRIDGE</td>
<td>403</td>
</tr>
<tr>
<td>UNIVERSITY OF OXFORD</td>
<td>435</td>
</tr>
<tr>
<td>KOBENHAVNS UNIVERSITET</td>
<td>302</td>
</tr>
<tr>
<td>UNIVERSITY COLLEGE LONDON</td>
<td>357</td>
</tr>
<tr>
<td>KU LEUVEN</td>
<td>291</td>
</tr>
<tr>
<td>IMPERIAL COLLEGE</td>
<td>279</td>
</tr>
<tr>
<td>ETH ZURICH</td>
<td>233</td>
</tr>
<tr>
<td>TECHNISCHE UNIVERSITEIT DELFT</td>
<td>257</td>
</tr>
<tr>
<td>EPFL LAUSANNE</td>
<td>297</td>
</tr>
<tr>
<td>TECHNICAL UNIVERSITY OF DENMARK</td>
<td>232</td>
</tr>
</tbody>
</table>

LABEL = BUDGET IN MILLION €
Research Partnerships

IMEC
- Started as a spin-off
- Leading research and innovation hub for nanoelectronics and digital technologies
- Hosts 4,000 brilliant minds from over 85 countries
- Headquartered in Leuven
- Host research institute for collaborative PhD and postdoc research

VIB
- Center for Cancer Biology (11 groups)
- 1,717 collaborators in 86 research groups
- VIB-KU Leuven: 593 scientists in 3 research centres
- Center for Brain & Disease Research (16 groups)
- Center for Microbiology (5 groups)
Research Partnerships

Energy Ville, knowledge centre for industry and public authorities on energy-efficient buildings and intelligent networks for a sustainable urban environment.

Flanders Make is the strategic research centre for the manufacturing industry. More than 500 specialised researchers work together with companies and knowledge institutions to develop new technologies for improving products and productions processes.
16 faculties

HUMANITIES & SOCIAL SCIENCES
- Institute of Philosophy
- Theology and Religious Studies
- Law
- Economics and Business
- Social Sciences
- Arts
- Psychology and Educational Sciences
- The Arts

SCIENCE, ENGINEERING & TECHNOLOGY
- Science
- Engineering Science
- Bioscience Engineering
- Engineering Technology
- Architecture

BIOMEDICAL SCIENCES
- Medicine
- Pharmaceutical Sciences
- Movement and Rehabilitation Sciences
KU Leuven takes great pride in its University Hospitals and the acclaim they have received in the pursuit of outstanding medicine.

**2 MAIN CAMPUSES**

- **Gasthuisberg Campus** for acute care
- **Pellenberg Campus** for rehabilitation

**University Hospitals in 2019**

<table>
<thead>
<tr>
<th>Service</th>
<th>Annual Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laboratory tests</td>
<td>17,001,609</td>
</tr>
<tr>
<td>Consultations</td>
<td>735,156</td>
</tr>
<tr>
<td>Radiological examinations</td>
<td>413,764</td>
</tr>
<tr>
<td>Emergencies</td>
<td>65,245</td>
</tr>
<tr>
<td>Hospital admissions</td>
<td>58,756</td>
</tr>
<tr>
<td>Surgical procedures</td>
<td>57,346</td>
</tr>
<tr>
<td>Kidney dialyses</td>
<td>30,907</td>
</tr>
<tr>
<td>Radiological examinations</td>
<td>287</td>
</tr>
<tr>
<td>Staff members</td>
<td>9,760</td>
</tr>
<tr>
<td>Physicians</td>
<td>1,752</td>
</tr>
</tbody>
</table>
The search for a coronavirus vaccine

- Research at Rega Institute
- Based on the Yellow Fever vaccine
- Simultaneous work on antiviral medicines
FACULTY OF ENGINEERING TECHNOLOGY

Bruges Campus | Ghent & Aalst Technology Campus | Group T Leuven Campus | De Nayer Campus Sint-Katelijne-Waver | Geel Campus | Diepenbeek Campus
SCIENCE, ENGINEERING & TECHNOLOGY (SET) GROUP
### 5 Faculties
- Science
- Engineering Science
- Bioscience Engineering
- Engineering Technology
- Architecture

### 14 Research departments
- Architecture
- Biology
- Biosystems
- Chemical Engineering
- Chemistry
- Civil Engineering
- Computer Science
- Earth and Environmental Sciences
- Electrical Engineering (ESAT)
- Mathematics
- Mechanical Engineering
- Materials Engineering
- Microbial and Molecular Systems
- Physics and Astronomy

---

**Arenberg Doctoral School**
SET Group in numbers

+20,000 students

- Science
- Engineering Science
- Bioscience Engineering
- Engineering Technology
- Architecture

870x11 to 949x40
**SET Group**

**Spin-offs**

2019

128 spin-off companies

+7000 direct jobs

Cumulative number of spin-offs created

KU Leuven  SET Group
FET at KU Leuven
Faculty of Engineering Technology
Multicampus faculty

7 CAMPUSES IN FLANDERS,

+6000 STUDENTS

+12% INTERNATIONAL STUDENTS

+800 STAFF

+10% INTERNATIONAL STAFF
Faculty of Engineering Technology

Education and research at KU Leuven outside Leuven

Bruges Campus
www.iiw.kuleuven.be/brugge

Ghent Technology Campus
www.iiw.kuleuven.be/gent

Aalst Campus
www.iiw.kuleuven.be/aalst

De Nayer Campus
Sint-Katelijne-Waver
www.iiw.kuleuven.be/denayer

Campus Groep T
Leuven
www.iiw.kuleuven.be/groept

Geel Campus
www.iiw.kuleuven.be/geel

Diepenbeek Campus
in collaboration with UHasselt
www.iiw.kuleuven.be/diepenbeek
Introduction
Why do we need embedded software resilience?

When looking at embedded systems they are being used ever more in a plethora of different environments.

Ranging from infotainment systems, over healthcare support systems, medical safety critical systems, autonomous vehicles and even systems going into space!
Introduction

One challenge all these systems have in common is that they can be disturbed either by radiated or by conducted interference.

On top of that, as their microcontrollers operate on lower voltages to spare battery time, these microcontrollers are becoming more vulnerable to soft-errors.
Introduction

What are soft errors?
Why are they transient & difficult to simulate?
Experience of our research group
Symptoms of Soft Errors
If the automotive community genuinely cares about road safety, dedicated short-range communications (DSRC)-based V2X (both vehicle-to-vehicle and vehicle-to-infrastructure) communication should be the backbone of the sexy technologies widely deemed necessary to the next generation of electric, connected, and autonomous vehicles.

However, it isn’t. At least Mobileye, one of the most respected computer vision technology companies, didn’t think that DSRC was necessary.

When an Intel/Mobileye team decided to offer the media a public demo of their autonomous vehicles on the road in Jerusalem last month, the team went ahead to equip traffic lights — on the route where the AVs were supposed to drive — with LTE-based modems as “an extra safety measure.” Ironically, one of the Intel/Mobileye AVs got caught by a local TV station’s video camera running a red light. (Fast-forward the video to 4:28 for said scene.)

Mobileye blamed this embarrassment on electromagnetic interference (EMI) between the TV crew’s wireless camera and the traffic light’s wireless transponder. Crossed signals from the two sources befuddled the car.

[...]
Symptoms of Soft Errors

INSIDE EVS

Mark Kane https://insideevs.com/ June 26th, 2021

CHINA: TESLA ‘RECALLS’ MODEL 3 AND MODEL Y

According to the latest reports from China, there is a safety issue related to Tesla's assisted driving feature. As we understand, the cruise control can be activated accidentally, "causing sudden acceleration."

The Chinese regulators require Tesla to 'recall' nearly 300,000 Made-in-China (MIC) and imported Model 3 and Model Y cars, although it's expected that an over-the-air software update will solve the issue. This is why it's not an ordinary recall that would require a visit to a service center, but it's also not a voluntary software update either.

"The cars’ autopilot systems can be activated automatically, potentially leading to crashes from sudden acceleration, the Chinese agency said.” - Bloomberg

Reuters and Bloomberg say that the number of affected cars stand at about 285,000 including:

- 249,855 MIC Model 3/Model Y - 211,256 Model 3 and 38,599 Model Y
- 35,665 imported Model 3.

That gives us some clue about how many Tesla Model 3 and Model Y were sold in China so far.

[...]
Effects of EMI

- Whole range of effects, including but not limited to:
  - Bit flips
  - Program crashes
  - Data corruption
  - Voltage spikes (and downtime)
  - Annoying buzzes (radios, microphones, …)
  - …

⇒ Sometimes very hard to diagnose that they’re EMC related …
Example:

- On May 26th, 1991
- Boeing 767-3Z9ER
  - Uncommanded deployment of the thrust reverser in-flight
  - One of the first Fly-by-Wire examples

One of the investigators stated:

“had that Boeing 767 been of an earlier version of the type, fitted with engines that were controlled mechanically rather than electronically, then that accident could not have happened” – Job Macarthur
# Symptoms of Soft Errors

<table>
<thead>
<tr>
<th>Domain</th>
<th>Application</th>
<th>Symptoms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avionics</td>
<td>Fly-by-wire</td>
<td>System restart</td>
</tr>
<tr>
<td>Automotive</td>
<td>Brake-by-wire</td>
<td>Unexpected braking action / no braking action</td>
</tr>
<tr>
<td>Supercomputers</td>
<td>Calculations</td>
<td>Wrong or unrecognisable calculations</td>
</tr>
<tr>
<td>Networking</td>
<td>Router</td>
<td>Change of addresses / reboot</td>
</tr>
<tr>
<td>Personal appliances</td>
<td>Smartphone</td>
<td>System hangs</td>
</tr>
</tbody>
</table>
What are soft errors?
What are soft errors?

Diagram showing an embedded system with layers of application, OS, hardware, and I/O. The diagram includes an example of bit-flip caused by an external electric and magnetic field, with memory before and after the flip.
What are soft errors?

![Diagram of computer architecture](image)

- Memory
- Instructions decoding
- Register bank
- ALU
- Data memory management
- Code memory management
- Memory
Why are soft errors transient?

Soft errors *don’t affect the program memory*

Corrupted execution → reset → Normal execution

**but…**
Why are soft errors dangerous?

Corrupted data might be written to **non-volatile memory**

and

A corrupted cyber-physical system might result in **damaged hardware**
Why are soft errors dangerous?

<table>
<thead>
<tr>
<th>Industry</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical</td>
<td>[IEC 62304]</td>
</tr>
<tr>
<td>Process industry</td>
<td>[IEC 61511]</td>
</tr>
<tr>
<td>Transportation</td>
<td>[EN 50126] [EN 50128] [EN 50129]</td>
</tr>
<tr>
<td>Agriculture</td>
<td>[ISO 25119]</td>
</tr>
<tr>
<td>Nuclear</td>
<td>[IEC 60880] [IEC 60987] [IEC 61226]</td>
</tr>
<tr>
<td>Automotive</td>
<td>[ISO 26262]</td>
</tr>
</tbody>
</table>
Why are soft errors dangerous?

Preventing and/or detecting soft errors is a key aspect of safety-critical and mission-critical systems.
Tolerable Risk and Residual Risk

- Residual Risk
- Tolerable Risk
- EUC Risk

Determined by society

Necessary Risk Reduction
What you need to do, no compromises!

Actual Risk Reduction

Zero Risk does not exist. This would require infinite time and money!
Our Research
Our Research

Software Implemented
Soft Error Detection

Error-free execution
Our Research

Software Implemented
Soft Error Detection

Unprotected Code

lift is stuck due to soft error

Soft error in unprotected code
Our Research

Software Implemented Soft Error Detection

soft error in protected code

Protected Code

factory continues without issues

soft error is detected

system is reset

Unprotected Code

Soft error in protected code
The Ultimate Factory
The Problem: Control Flow Error

No corruption, z will be 43

Unwanted Jump z will be 11

x = 5;
a = 3;
y = x + a;
\underline{y = y \times x};
z = y + a;

Bit-Flip
Solution: Software-Implemented CFE Detection Techniques

1) Add extra control variable S

2) Add extra control variable update instructions
   S = S + 1

3) Add extra control variable comparison instruction
   if S != 5 then

4) Add call to error handler in case of mismatch
   errorHandler()

---

```plaintext
S = 0;
x = 5;
S = S + 1;
a = 3;
S = S + 1;
y = x + a;
S = S + 1;
y = y * x;
S = S + 1;
z = y + a;
S = S + 1;
If S != 5 then
   errorHandler();
```

---

No corruption, z will be 43

Bit-Flip

1 0 1 1 ...

Control Flow Error detected and errorHandler called
Problem with implementing CFE detection techniques in high-level code

Job of the compiler:
- Translate the human-readable code into machine code for the target embedded system
- Optimize the code, e.g.
  - Remove code will never be executed
  - Reduce execution time or memory usage
Problem with implementing CFE detection techniques in high-level code

• The compiler optimizes the CFE detection technique instructions away
• To achieve their maximum error detection ratio, CFE detection techniques must be implemented in low-level code
• To implement CFE detection techniques in low-level code
  • The low-level version of the program must be understood
  • A low-level version of the CFE detection technique must be created.
  • Doing this manually:
    • Time-Consuming; Difficult; and Error-Prone!
Ease the implementation CFE detection techniques
Based on literature, three criteria to characterize CFE detection techniques were selected:

- **Error Detection Ratio**
  - Indicates which percentage of CFEs a technique detects.

- **Execution Time Overhead**
  - Indicates how much more time the protected program needs to execute, compared to the unprotected program.

- **Code Size Overhead**
  - Indicates how much more memory the protected program needs to be stored, compared to the unprotected program.
Measuring the Error Detection Ratio

To measure the error detection ratio, CFEs have to occur in the target embedded system

Option 1: Ad Hoc

Option 2: Fault Injection
Fault Injection:
The hardware setup
Research Projects started +/- 2008
Research Projects - European Collaborations
Research Projects - European Collaborations

AUTOBarge
European training and research network on Autonomous Barges for Smart Inland Shipping
Research Projects - recent projects

- **Safety Assurance 4.0** *(VLAIO TETRA)*
  Management of Safety Risks in Industry 4.0
  4yr PhD + 3yr PostDoc

- **SAFETEE** *(C2 Intern KU Leuven)*
  Towards a method and platform for trustworthy autonomous systems
  20yr PhD + 4yr PostDoc

- **FIRES** *(C3 Intern KU Leuven)*
  A Framework to Increase the Resilience of Embedded Systems
  4yr PhD + 2.5yr Postdoc
Relevant Publications


Relevant Publications


Relevant Publications


Relevant Publications

  Instruction Level Duplication and Comparison for Data Error Detection: a First Experiment.  

  Software-Implemented Fault Injection for Physical and Simulated Embedded CPUs.  


  An Improved Data Error Detection Technique for Dependable Embedded Software.  
Relevant Publications


M-Group | Fast Growing Team!

Department of Mechanical Engineering
Department of Electrical Engineering
Department of Computer Science

“True to the mechatronic approach”
M-Group | Fast Growing Team!

- Currently 4 professors (at least 8 within a few years)
- 1 research manager
- 1 project office manager
- 4 post-doc
- About 20 junior researchers
- 2 technical support
- >10 lecturers
140

5 PhDs successfully completed in 2020-2021