Reliability in Embedded Applications

Klaus-Peter Zauner

COMP2215: Computer Systems II
Embedded Systems

Typical:

- Harsh Environment
  - Thermal
  - Electromagnetic
  - Electrostatic
  - Radiation (e.g., at high altitude)
  - Mechanical (shock, vibration)
  - Adversarial Attacks
Embedded Systems

Typical:

- Critical System failure results in:
  - Loss of life
  - Loss of vehicle
  - Irreversible damage

There is also a legal dimension: Embedded software is typically part of a product and liability can not be dodged by excluding it in the license.
Embedded Systems

Typical:

- Critical System failure results in:
  - Loss of life
  - Loss of vehicle
  - Irreversible damage

There is also a legal dimension: Embedded software is typically part of a product and liability can not be dodged by excluding it in the license.
Common Issues

Hardware

- Glitches
  - Power
  - Clock
  - Signals
- Wear-out
  - Flash
  - EEPROM

Software

- Timing
  - Real Time
  - Race conditions
- Difficult code
  - Parallelism
  - Optimisation
Common Issues

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ Glitches</td>
<td>▶ Timing</td>
</tr>
<tr>
<td>▶ Power</td>
<td>▶ Real Time</td>
</tr>
<tr>
<td>▶ Clock</td>
<td>▶ Race conditions</td>
</tr>
<tr>
<td>▶ Signals</td>
<td>▶ Difficult code</td>
</tr>
<tr>
<td>▶ Wear-out</td>
<td>▶ Parallelism</td>
</tr>
<tr>
<td>▶ Flash</td>
<td>▶ Optimisation</td>
</tr>
<tr>
<td>▶ EEPROM</td>
<td></td>
</tr>
</tbody>
</table>
What can happen?

▶ Erroneous signal detection
  ▶ E.g., Interrupts
▶ Wrong instruction executed
▶ Memory state changed
  ▶ Temporarily or permanent
▶ CPU state changes
▶ CPU resets
What can happen?

- Erroneous signal detection
  - E.g., Interrupts
- Wrong instruction executed
- Memory state changed
  - Temporarily or permanently
- CPU state changes
- CPU resets

Anything may happen...
What can be done?

The Situation:

- Critical System
- Anything can happen

⇒ Reduce probability that something bad happens

Do not underestimate the failure probabilities for a mass market product that is on 24h.
What can be done?

The Situation:
- Critical System
- Anything can happen

⇒ Reduce probability that something bad happens

Do not underestimate the failure probabilities for a mass market product that is on 24h.
What can be done?

The Situation:

- Critical System
- Anything can happen

⇒ Reduce probability that something bad happens

Do not underestimate the failure probabilities for a mass market product that is on 24h.
Mitigation Measures

- Physical protection
- Target Application Specific Failure Modes
- Redundancy
- Protection Circuits
- Defensive Programming
Mitigation Measures

- Physical protection
- Target Application Specific Failure Modes
  - Redundancy
  - Protection Circuits
  - Defensive Programming
Mitigation Measures

- Physical protection
- Target Application Specific Failure Modes
- Redundancy
- Protection Circuits
- Defensive Programming
Mitigation Measures

- Physical protection
- Target Application Specific Failure Modes
- Redundancy
- Protection Circuits
- Defensive Programming
Mitigation Measures

- Physical protection
- Target Application Specific Failure Modes
- Redundancy
- Protection Circuits
- Defensive Programming
Application Specific Failure Modes

- Ubiquitous use of embedded systems
- Diverse requirements
  - including cost

Example

Power glitches have different effects depending on their timing relative to the clock.

- Engine controller → probability may be acceptably low
- ATM machine → hit in vulnerable period very likely (intentional attack)
How to respond?

- Shut down
  - Temporarily or Permanently
  - Requires redundancy
    (other machine or human operator)

- Try to recover
  - Reset (e.g. watchdog timer)
  - Real-time requirements?
How to respond?

- **Shut down**
  - Temporarily or Permanently
  - Requires redundancy
    (other machine or human operator)

- **Try to recover**
  - Reset (e.g. watchdog timer)
  - Real-time requirements?
How to respond?

- **Shut down**
  - Temporarily or Permanently
  - Requires redundancy (other machine or human operator)

- **Try to recover**
  - Reset (e.g. watchdog timer)
  - Real-time requirements?

Failed system not identified? (requires redundancy):

- Use simplest system
- Vote
How to respond?

- **Shut down**
  - Temporarily or Permanently
  - Requires redundancy
    (other machine or human operator)

- **Try to recover**
  - Reset (e.g. watchdog timer)
  - Real-time requirements?

Failed system not identified? (requires redundancy):

- Use simplest system
- Vote
Triple Redundancy with Voting

Lufthansa A321 on 05.11.2014, loss of 4000 feet of altitude

Airbus analysed the data and stated: ”all three sensors worked normally until about 8 minutes into the flight[...]. At that point, at an ambient temperature of -35 degrees C, AoA sensors 1 and 2 froze up at a position of approximately 4.5 degrees nose up [...]. Within 15 seconds the first officer made increasing nose up input until reaching 75% of the maximum travel of the side stick, the attitude however changed from 4.5 degrees to -3.5 degrees against this input. The system disregarded/turned off the AoA 3 sensor because it disagreed more than the permitted value with the other 2 sensors.
Triple Redundancy with Voting

Lufthansa A321 on 05.11.2014, loss of 4000 feet of altitude

Airbus analysed the data and stated: ”all three sensors worked normally until about 8 minutes into the flight[...] At that point, at an ambient temperature of -35 degrees C, AoA sensors 1 and 2 froze up at a position of approximately 4.5 degrees nose up [...]. Within 15 seconds the first officer made increasing nose up input until reaching 75% of the maximum travel of the side stick, the attitude however changed from 4.5 degrees to -3.5 degrees against this input. The system disregarded/turned off the AoA 3 sensor because it disagreed more than the permitted value with the other 2 sensors.
Triple Redundancy with Voting

When Alpha Prot is activated due to blocked AOA probes, the flight control laws order a continuous nose down pitch rate that, in a worst case scenario, cannot be stopped with backward sidestick inputs, even in the full backward position.

If the Mach number increases during a nose down order, the AOA value of the Alpha Prot will continue to decrease. As a result, the flight control laws will continue to order a nose down pitch rate, even if the speed is above minimum selectable speed, known as VLS.

This condition, if not corrected, could result in loss of control of the aeroplane.
Protection Circuits

- Recognise Adverse Situation
  - radiation sensors
  - temperature sensors

- Recognise Failure
  - Watchdog (timing integrity)
  - Hardware Check sums (data integrity)

- Fallback Systems
  - Recognise large deviations of a refined system
  - Use as “second chance” if refined system fails
Defensive Programming

- **Self-stabilising protocols**
  - Any random data inserted in the message stream will be dissipated after some rounds

- **Initialise unused resources**
  - E.g., Write a jump instruction to a reset vector to all unused program memory cells

- **Coding rules**
  - Avoid the well known traps of low-level C-coding
  - E.g. MISRA C (Motor Industry Software Reliability Association)

- **Automated tools for compliance and model checking**
  - see G. J. Holzman: “Mars Code”