New trends in medical software safety: Are you up to date?
5 October 2015, USA
Dr. Peter Havel,
Senior Vice President,
Medical & Health Services (MHS)
TÜV SÜD Product Service
phavel@tuvam.com
The more complex technology is, the harder it is prevent failure.
In 2020: 20ct – consequence?

Cost per Genome

Moore's Law

National Human Genome Research Institute
genome.gov/sequencingcosts
Market trends
Keeping up to date with the latest medical technologies

TÜV SÜD is the only Notified Body with a Scientific Advisory Board comprising of top European scientists and physicians.

TÜV SÜD and the Scientific Advisory Board

- Consequence of future treatment basis for strategic decision making
- Identifying new risks and setting safety principles
- Clinical network
- Independent scientific opinion
Market consideration - Trends

- **mHealth**
- **Moving beyond wrist wearables**
- **Micro segmentation**
- **Big data**

- **3D Bioprinting**
- **Genome & engineering**
- **Xenomorphic implants**
- **Miniaturised devices**
A missing regulatory concept is a roadblock for market access
Software is…

- Usually very complex
- Intangible - you can’t touch nor see it
- All errors are systematic
- It has already killed – and still does
Let's talk about this kind of insects - bugs
Let’s talk about bugs

- A software bug is an error, flaw, mistake, failure, or fault in a computer program that prevents it from behaving as intended (e.g., producing an incorrect or unexpected result).

- Most bugs arise from mistakes and errors made by humans during coding or in specifications.

- A few are caused by tools like compilers producing incorrect code.
How do you find bugs?
Common tactics: Banana technology

Bananas are designed to ripen in the hands of customers.
Toyota drive-by-wire bug (2009 to 2011)

How was the bug found?
- Trigged by motor accidents involving Toyota cars
- 37 alleged deaths due to bug

What was the bug?
- Sudden unintended acceleration
- Toyota admits that its runaway-car situation is serious

Cost
- Recalls covering 9 million vehicles
- Suspended sales of 8 of its best selling vehicles → $54 million/day in lost sales revenue for the company and its dealers
Can you re-use old codes that have been proven?
Re-use of proven code

Ariane Rocket (1996)

What was the bug?
- Ariane 5, Europe’s unmanned rocket, was destroyed seconds after launch on its maiden flight. Its cargo of four scientific satellites was also destroyed.

Cause of the bug
- Re-use of Ariane 4 Software. Shutdown occurred when the guidance computer tried to convert the sideways rocket velocity from 64-bits to a 16-bit format. The number was too big, and an overflow error resulted.

Cost
- $500 million
Let’s turn to medical devices

In medical devices so far…

- Having a quality system
- Working carefully?
- Really good programmers?
It does not happen in medical devices?
What was the bug?

- Radiation therapy software by Multidata Systems International miscalculated the proper dosage, exposing patients to harmful and in some cases fatal levels of radiation.
- The physicians, who were legally required to double-check the software’s calculations, were indicted for murder.

Cause of the bug

- The software calculated radiation dosage based on the order in which data was entered, sometimes delivering a double dose of radiation.

Cost

- Eight people dead, 20 critically injured.
Radiation Therapy Machine (1985)

What was the bug?
- Canada’s Therac-25 radiation therapy machine malfunctioned and delivered lethal radiation doses to patients.

Cause of the bug
- Because of a subtle bug called a race condition, a technician could accidentally configure Therac-25 so the electron beam would fire in high-power mode without the proper patient shielding.

Cost
- Three people dead, three people critically injured.
What was done in medical devices so far was perhaps not enough!

- In the US, new guidance and applicable standards were defined
- The European regulation (MDD) was also changed regarding software
2. For the purpose of this Directive, the following definitions shall apply:

(a) "medical device" means any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application intended by the manufacturer to be used for human beings for the purpose of:
Software – The landscape of EU standards

Hardware | Software in device | Stand alone software | Others
--- | --- | --- | ---

60601-1-4 – PEMS & -1
62304 - Software
60601-1-6 & 62366 – Usability
13485 - QM-System
14971 – Risk management
61508
Standards

- IEC 82304-1 - Health software – Part 1 General requirements for product safety (not harmonized)
- FDA Guidance Feb. 9th 2015
- IEC 800001-1
  - Application of risk management for IT-networks incorporating medical devices
    - Part 1: responsibilities & activities
  - Safety, effectiveness and data and system security
  - (does not set acceptance levels)
- IEC 60601
  - Incorporated PEMS (former 60601-1-4)
  - Part for network coupled devices
How do you create safe software?
Testing, testing, testing…!

The software must be tested:

- But how?
- What?
- When?
- Spec, spec, spec…..
The black box test alone is not feasible

- **Input/output combinations:**

  - ECG
  - $O_2$
  - Flow

  ➔ Small or big miracle - see M**ros*ft

  ➔ Screen output
  ➔ Diagnostic interpretation/ alarm

- **10 bit sampling:** $2^{10} \times 2^{10} \times 2^{10} = 1073741824$ (more than one billion comb.)

  ➔ Not enough time for testing
A person describes the box in her hand to another person who has never seen the box.

How can industry understand that they are not sufficiently in control of the quality?
**Specification**

- Create a box
- Create a carton box
- Create a carton box with dimensions x, y, z & thickness D

**Verification**

- Is it a box (yes/no)
- Is it made out of carton?
- Check the dimensions x, y, z, D + - 2%?
- Check the openings…?
Before you code...

Define what the device should do
Define what should be done in hard & software
Define system modules
Define the software architecture
Specify the software modules
Specify the software units

Decomposition of the problem into components

Integration of components (assembly)

Validation
System integration tests
Module integration test
Software integration tests
Module tests
Unit tests

TÜV SÜD
Specs and tests depending on risk

Software has to be classified into:
- Class A: No injury or damage to health is possible
- Class B: Non-SERIOUS INJURY is possible
- Class C: Death or SERIOUS INJURY is possible

SERIOUS INJURY: injury or illness that directly or indirectly:
- Is life threatening
- Results in permanent impairment of a body function or permanent damage to a body structure, or
- Necessitates medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure
The risk based V-model
The V-Model in IEC 62304

Boxes represent typical development lifecycle activities.
Solid Arrows indicate typical deliverables transferred into/out of activities.
Dotted arrows indicate deliverables just to the risk management file.

Key:
- Outputs from problem resolution process
- Inputs to problem resolution process

Slide 32
The structure of IEC 62304

System development / maintenance activities

Software development

Software maintenance

Software risk management

Software configuration management

Software problem resolution

Core processes

Support processes
And never forget – you should have a competent team!
Faulty altimeter contributed to Turkish Airlines crash: officials

Engine failure may have caused Turkish Airlines crash: investigator
Pilots among 9 killed in crash of Turkish flight at Amsterdam airport

Features
FAQ: Violent turbulence, what it is and why it happens
FAQ: Bird strikes - why they can bring down aircraft
IN DEPTH: Secret Skies
DATABASE: Aviation safety investigations

Severe turbulence
Missing Air France jet hit strong turbulence: officials (June 1, 2009)
15 injured by sudden drop on turbulent Air Canada flight (April 24, 2009)
At least 50 injured after Manila to Tokyo flight sends passengers 'flying' (Feb. 20, 2009)
Aspects of new technologies
Safety aspects that must be addressed

- Automated only in approved counties
- Compatibility of platforms
- Error free download
- Download at wrong time
- Overwriting of important data
- Failing usability after failed software update
- Distribution
- Not to be used without instruction for use

- App store
  - World wide accessibility
  - Download for a country where there is no approval
  - Traceability
  - Knowing who has the software knowledge & training:
- In GER & AUS – download only after training & receiving manual
- Information about new features
Wireless safety goals

- Wireless coexistence
- Wireless quality of service
- Protection from too much radiation

IT platforms

- Commercial off the shelf (COTS)
- Risk management of platform
  - E.g. Display size
  - Reliability of device

Instructions for use

- EU has problems if user is not professional
- EU directive for electronic labeling - download only for professional users
Data security

- Confidentiality
- Integrity – secure against undesired change
- Availability
  - Longevity
  - Immediateness
- Detection
  - Intrusion detection if dangerous
- Informing e.g. the admin
- Response – respond to someone who can react
- Recovery – restore intruded data
Your one stop technical solution provider

<table>
<thead>
<tr>
<th>150</th>
<th>years of experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>800</td>
<td>locations worldwide</td>
</tr>
<tr>
<td>2,060</td>
<td>million Euro in sales revenue 2014</td>
</tr>
<tr>
<td>22,000</td>
<td>employees worldwide</td>
</tr>
<tr>
<td>500</td>
<td>medical device experts across 15 countries</td>
</tr>
</tbody>
</table>

Note: Figures have been rounded off.
We are prepared to help you demonstrate the safety and effectiveness of your innovations

Establish confidence in your new technologies

- TÜV SÜD is the only Notified Body with a Scientific Advisory Board comprising of top European scientists and physicians.

- Value add services like functional safety and pre-assessments intercept issues early, saving time and money.
Specialists in worldwide regulations, we ensure that your products are tested in compliance with the latest requirements.

- **Canada**
  - CMDCAS (ISO 13485)
  - CAN/CSA C22.2 No. 60601-1 as NRTL

- **Brazil**
  - INMETRO Certification of electrical Medical Devices, including Factory Inspections

- **USA**
  - NRTL Certification
  - FDA 510(k) Third Party Review
  - FDA Third Party Inspections

- **Europe**
  - Conformity assessment procedures according to AIMDD, MDD, IVDD (notified body number 0123)

- **China**
  - CFDA Registration Agent service
  - Test Agent service
  - Clinical Trial Agent Service

- **Russia**
  - Registration Certificate by Roszdravnadzor and declaration of conformity

- **Japan**
  - Medical Device Safety Testing according to JIS
  - Certification of certain class II and class III medical devices and IVDs
  - Audits according to J-QMS requirements

- **South Korea**
  - Technical Document Review of class II medical devices
  - CB test reports

- **Malaysia**
  - Conformity Assessment Body (CAB) under the MDA
  - Technical File Review for product registration

- **Singapore**
  - CAB for medical devices in Singapore
  - GDPMDS certification
  - Product Safety Testing

- **Australia**
  - Conformity Assessment Body (CAB) under the current EU-AUS MRA

- **MDSAP (Medical Device Single Audit Program)**
  - Single regulatory audit that satisfies the needs of the following regulatory jurisdictions: Australia, Brazil, Canada, USA
Thank you!

Dr. Peter Havel
Senior Vice President
TÜV SÜD Product Service
phavel@tuvam.com
www.tuv-sud.com/medicaldevice