Introducing SAFETY in ORGANIZATIONS
Lessons Learned
Day 1

Henrik Thane
Adj. Professor in Functional Safety, MDH
SAFETY INTEGRITY AB
2016-03-16
Dr. Henrik Thane

- **Senior Safety Assessor** and Safety Manager, Safety Integrity AB
- **Professor in Functional Safety**, Mälardalen Real Time Research Center, MDH, 2012-
- Founded Safety Integrity AB in 2009
- **Member of national standardization committees for IEC61508 and EN50128**
- Product M Manager at ENEA, Responsible for all operating systems and tools
- CEO ZealCore, co-founded ZealCore 2001, acquired by ENEA 2008
- Associate Professor (Docent) at Mälardalen Real-Time Center until 2008
- Ph.D. from the Royal Institute of technology in Stockholm, 2000
- In addition to research I have during the last 15 years worked as an expert consultant for the industry and given numerous industrial courses on design and test of software in safety-critical computer based systems.
SOFTWARE SAFETY
We provide SERVICES, EDUCATION, DOCUMENTATION TEMPLATES

We are experts on the functional safety standards:
IEC61508 and its derivatives e.g., ISO26262, EN50128/9, EN62061, EN13849

We provide SERVICES as:
- Independent SAFETY ASSESSORS (ISA)
- SAFETY MANAGERS
- SAFETY MANAGEMENT STARTUP

We offer TRAINING in
- Safety Management courses for IEC61508, EN50128/9 and ISO26262, IEC62061, EN13849.
INDEPENDENT SAFETY ASSESSOR

- Accredited TYPE A Inspection Body

QUALITY SYSTEM

- SS-EN17020:2012
  - Conformity assessment
  - Requirements for the operation of various types of bodies performing inspection
All manufacturers of safety related products

- Customers:
  - ABB Robotics, Volvo Construction Equipment, Bombardier Transportation, Atlas Copco, Trafikverket, ABB Mining, Westermo, Arcticus Systems, Öresundsbron, etc.

- Products:
  - High speed trains (400km/h), Driverless trains, Autonomous vehicles/construction equipment, Industrial Robots, Mining Elevators (2 km ride), Operating systems/tool vendors, etc.

Position

- One of a few accredited inspection bodies in Sweden
- Most customers are based in Sweden. We have however had contracts for customers in South Korea, India, China, UK, Canada, and Italy.
Independence

- Between doer and verifier
- Doer ← Verifier ← Validator ← Assessor
What is Assessment?

- “Process of analysis to determine whether software,
  which may include process, documentation, system, subsystem hardware and/or software components, meets the specified requirements and to form a judgment as to whether the software is fit for its intended purpose.

- Safety assessment is focused on but not limited to the safety properties of a system”
  EN50128:2011

- “Examination of a characteristic of an item or element”
  ISO26262-1:2011
Audit
- “Examination of an Implemented process”
  ISO26262-1:2011

Assessor
- “Entity that carries out an assessment”
  EN50128:2011
Safety Planning
- Project plan
- Safety management plan
- Validation plan
- Change management plan
- Documentation plan
- Tools and COTS qualification plan
- All plans verification report

Safety Concept Phase
- System Definition
- Hazard Analysis
- Hazard log
- Safety Function Identification
- Safety Function specification
- Safety Function Validation Test Specification
- Safety Concept verification report

Product development: System level   HW/SW
- Determine the required performance level
- Safety Function design
- Architecture selection (Single or Dual channel)
- Evaluation of achieved PL report (MTTF, DC, CCF)
- System integration test specification
- Tools and COTS qualification report
- System level verification report

Validation

After SOP: Maintenance Phase
- Impact analysis
- Maintenance & Change records
- Maintenance Validation Report
- Assessment report (for every new release)

After SOP: Deployment
- Safety Manual
- Release Notes
- Deployment verification report

Functional Safety Assessment
- Assessment
- Assessment report

Safety Function Validation Phase
- Safety Function Validation Test Records
- Safety Function Validation Test Report

System Integration Test Phase
- System Integration Test Records
- System Integration Test Report

Software
V-model. See Figure 2

Hardware
V-model. See Figure 3

ISO 13849
Product development: Software Safety Specification
- Software safety requirements Specification
- Software safety requirements Parameterization Specification
- Software Validation test specification
- Software safety requirements verification report

Product development: Software Architecture
- Software Architecture Design Specification
- Software Integration Test Specification
- Software Architecture Design Verification Report

Product development: Software Unit Design
- Software Unit Design Specification
- Software Unit Test Specification
- Software Unit Design Specifications Verification Report

Software Integration Test Phase
- Software Integration Test Record(s)
- Software Integration Test Report

Software Unit Test Phase
- Software Unit Test Records
- Software Unit Test Report

Software Validation Phase
- Software Validation Test Records
- Software Validation Test Report

Validation

ISO 13849

Figure 2
I have assessed many projects… and performed hundreds of assessments
Recent Projects

- **Safety Assessor, V300 Zefiro High speed train (400km/h), Bombardier Transportation Italy, 2011-2015**
- **Safety Assessor, TCMS C30, Bombardier Transportation Sweden, 2014-**
- **Safety Assessor/mentor, Pentronic AB, IEC61508, 2014-**
- **Safety Assessor/mentor, Atlas Copco Rock Drills, EN13849, 2013-2014**

- **Safety Assessor, Öresund Bridge, upgrade of Computer control and SCADA system for Tunnel safety and supervision, EN50129/EN50128, 2013**
- **Safety Manager ABB Robotics, Safety Controller, EN13849, 2012-**

- Safety Manager ABB Mining, regarding IEC62061, 2011-
- Safety Manager Volvo CE, project CEA2+, NEAT, RFT, regarding ISO26262, 2011-2012
- Safety Process Mentor for Data Respons, and Westermo regarding EN50129 and EN50128, 2010-2012
- **Safety Assessor Volvo CE, Process and tools, regarding IEC61508, 2010**
- **Safety Assessor, Regina SJ, intercity train project, Bombardier, 2010-**
- **Safety Assessor, Zefiro China, High speed train (400km/h), Bombardier Transportation, 2009-2013**
- **Safety Assessor, Delhi Metro project (DM2), Bombardier Transportation. 2009 -2010**
- **Safety Assessor, London underground project (SSL), Bombardier Transportation. 2008 -2011**

- Senior expert/consultant/mentor on a number of safety critical applications, within Transportation/Vehicles, and Industrial automation 1995-2011.
Experience

No project has had a streamlined organization and Development/Lifecycle Process for complying with the required safety standard.
Compliance has been fulfilled through:

- Repetitive assessments/gap analysis
- Corrective actions, i.e., changed process and updated documentation

- This is has not been cheap
- Cost factor: 3x-10x from initial estimate

Example of costly convergence

<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>Authors</th>
<th>Comments</th>
<th>Open Process Issues</th>
<th>Closed Process Issues %</th>
<th>Partially Closed Process Issues %</th>
<th>Open Product Issues (3.8)</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st draft</td>
<td>2011-11-20</td>
<td>Dr. Henrik Thane</td>
<td>Assessment plan preparation</td>
<td>390</td>
<td>0%</td>
<td>0%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit 1</td>
<td>2011-12-07</td>
<td>Dr. Henrik Thane</td>
<td>Audit regarding safety management &amp; Plans</td>
<td>366</td>
<td>(24) 6%</td>
<td>(22) 5.6%</td>
<td></td>
<td>6%</td>
</tr>
<tr>
<td>Audit 2</td>
<td>2012-04-25</td>
<td>Dr. Henrik Thane</td>
<td>Backlog plans</td>
<td>347</td>
<td>(43) 11%</td>
<td>(24) 6%</td>
<td></td>
<td>5%</td>
</tr>
<tr>
<td>Audit 3</td>
<td>2012-06-14</td>
<td>Dr. Henrik Thane</td>
<td>Backlog plans, Lifecycle documentation, product integrity checklist added</td>
<td>343</td>
<td>(47) 12%</td>
<td>(27) 7%</td>
<td>46</td>
<td>1%</td>
</tr>
<tr>
<td>Audit 4</td>
<td>2012-09-26</td>
<td>Dr. Henrik Thane</td>
<td>Backlog plans</td>
<td>325</td>
<td>(65) 17%</td>
<td>(31) 8%</td>
<td>46</td>
<td>5%</td>
</tr>
<tr>
<td>Audit 5</td>
<td>2012-11-23</td>
<td>Dr. Henrik Thane</td>
<td>Backlog and requirements</td>
<td>307</td>
<td>(83) 21%</td>
<td>(39) 10%</td>
<td>46</td>
<td>4%</td>
</tr>
<tr>
<td>Audit 6</td>
<td>2013-02-22</td>
<td>Dr. Henrik Thane</td>
<td>Backlog and requirements</td>
<td>292</td>
<td>(98) 25%</td>
<td>(42) 11%</td>
<td></td>
<td>4%</td>
</tr>
<tr>
<td>Audit 7</td>
<td>2013-04-26</td>
<td>Dr. Henrik Thane</td>
<td>Backlog and requirements</td>
<td>278</td>
<td>(113) 29%</td>
<td>(46) 12%</td>
<td></td>
<td>4%</td>
</tr>
<tr>
<td>Audit 8</td>
<td>2013-06-13</td>
<td>Dr. Henrik Thane</td>
<td>Backlog and requirements</td>
<td>254</td>
<td>(137) 35%</td>
<td>(46) 12%</td>
<td></td>
<td>4%</td>
</tr>
<tr>
<td>Audit 8b</td>
<td>2013-06-16</td>
<td>Dr. Henrik Thane</td>
<td>Backlog and requirements + missing arguments</td>
<td>243</td>
<td>(148) 38%</td>
<td>(40) 10%</td>
<td></td>
<td>9%</td>
</tr>
<tr>
<td>Audit 9</td>
<td>2013-09-26</td>
<td>Dr. Henrik Thane</td>
<td>Backlog and requirements</td>
<td>231</td>
<td>(158) 41%</td>
<td>(41) 11%</td>
<td></td>
<td>3%</td>
</tr>
<tr>
<td>Audit 10</td>
<td>2013-12-03</td>
<td>Dr. Henrik Thane</td>
<td>Backlog and test</td>
<td>213</td>
<td>(177) 45%</td>
<td>(32) 8%</td>
<td></td>
<td>4%</td>
</tr>
<tr>
<td>Audit 11</td>
<td>2014-03-17</td>
<td>Dr. Henrik Thane</td>
<td>Backlog and parameterization</td>
<td>184</td>
<td>(206) 53%</td>
<td>(32) 8%</td>
<td></td>
<td>8%</td>
</tr>
<tr>
<td>Audit 12</td>
<td>2014-04-29</td>
<td>Dr. Henrik Thane</td>
<td>Backlog</td>
<td>168</td>
<td>(224) 57%</td>
<td>(29) 7%</td>
<td></td>
<td>4%</td>
</tr>
<tr>
<td>Audit 13</td>
<td>2014-05-28</td>
<td>Dr. Henrik Thane</td>
<td>Backlog + deployment</td>
<td>134</td>
<td>(256) 66%</td>
<td>(22) 6%</td>
<td></td>
<td>9%</td>
</tr>
<tr>
<td>Audit 14</td>
<td>2014-06-26</td>
<td>Dr. Henrik Thane</td>
<td>Backlog</td>
<td>113</td>
<td>(277) 71%</td>
<td>(23) 6%</td>
<td></td>
<td>5%</td>
</tr>
<tr>
<td>Audit 15</td>
<td>2014-08-22</td>
<td>Dr. Henrik Thane</td>
<td>Backlog</td>
<td>102</td>
<td>(288) 74%</td>
<td>(23) 6%</td>
<td></td>
<td>3%</td>
</tr>
</tbody>
</table>
Observed Manufacturer Challenges

- **Separated processes and organizations**
  - One for development
  - One for safety management
    - Similar to HW development and SW development processes and organizations
• Fragile (one-off mentality)
  – After first release change management is not harmonized
  – Development documentation and artifacts diverge from safety documentation

• Safety anxiety
  – Organization change takes time
  – Safety culture implementation takes time
  – Harmonized safety and development process takes time
 Lessons learned

• **Reuse is very important**
  – Reuse documentation from previous projects
    • Plans, templates, verification checklists, etc.
    • Preferable have a certified safety management system
      – That can be instantiated for every new project
    • Continuous improvement

• **Continuous Training**
  – Role centric training
    • Project Manager, Safety Manager, Requirements Manager
    • Architect, Implementer,
    • Test manager, Verification manager
    • Validator
    • Assessor
    • Configuration Manager
  – Mentors (with experience from previous projects)
  – **New people** who are introduced late in a project often think the process is over ambitions and require way too much work. They need to be trained and mentored.
• **When the deadline approaches**
  – Often all ambitious safety goals are washed out
  – All kinds of shortcuts are sought.
  – Extremely important to keep to the process then and that there are sufficient resources.

• **Regard the safety standards with respect but not fear. They are there to help.**
• Embedded Systems Safety
  – IEC 61508 (2001) and (2010 2nd ed.)

• Industry specific
  – Software for Machines
    • ISO13849-1
    • ISO 62061
  – Transportation
    • EN 50128 – railway software
    • ISO 26262 – Automotive/Trucks/Construction Equip.

• Industry specific
  – Aerospace and aviation
    • DO-178B, Aviation, USA
    • NASA-STD-8719-13, NASA, USA
    • ESA PSS-05-0, Space, European
  – Military
    • MIL-STD-882D, DoD, USA
    • 00-55/00-56, MoD, UK
    • MIL-STD-498, DoD, USA
Current situation

– It is about a 10 year turn-around time for new functional safety standards
Safety

Integrity

Functional Safety Challenges

- **High complexity**
  - The complexity of computer controlled systems increase exponentially
  - Current standards do not deal with high complexity systems

- **Multiple concerns: Safety and security jointly**
  - More and more systems are connected to the Internet: IoT, Cars, Trains, …
  - Functional safety deals with dangerous faults stemming from the system itself
  - Security deals with intentional sabotage of systems, this is not covered by current functional safety standards to any extent.

- **Multiple domains**
  - Need to be able to deal with many functional safety standards concurrently in a cost efficient manner
    - For example OEMs who target Automotive, Construction Equipment, and railway at the same time
    - Tool vendors, who want to certify their tools for many different safety standards in order to increase customer value and market share
Summary: Safety Assessment

SS-EN-IEC 61508
2001 & 2010

Compliance by fulfillment of all Product and Process Requirements:

- Plans & Process
- Requirements
- Verification for each phase
  - Static (reviews)
  - Dynamic (tests)
- Independence
  - Between doer and verifier
  - Doer – Verifier – Validator - Assessor

- Reports for each phase
- Change management
- A complete documentation trail
- Assessment

EN 50126
EN 50129
EN 50128
Railroad
1999/2001/2011

IEC 61513
Nuclear Power
2001

IEC 61511
Process Industry
2003

IEC 62061
Safety of Machinery
2003

IEC 26262
Automotive
2012
Important to integrate safety process & development process

Assessment

Documentation/Tests

Issue List

Update Process/Update Product

Zero Issues

Compliant Process

Certificate/report on Compliance

Compliant Product

Processes, Methods & Measures:

Qualified Tools:

Model

Code

Test

Project Actual State

Project Target State
Figure 1. Allegedly the first computer bug - found by Grace Hopper’s Team in 1945. Exhibited at the Museum History of American Technology/Smithsonian

henrik.thane@safetyintegrity.se