Safety and Security
Opportunities for Eclipse?

Presentation to the Board of Directors of the Eclipse Foundation

Santa Clara, 21 March 2011

Hans-Jürgen Kugler
Product and Service Properties vs. “Affected” Industries

- Safety
  - Aerospace
  - Transport
  - Automotive
  - Medical devices
  - …

- Security
  - Defence
  - Communications
  - Finance
  - …
  - Automotive

Compliance with regulatory frameworks needs to be demonstrated. These can be based on industry or on general standards.
The **Internet of Things** makes the situation worse ...

Safety and security requirements behave like epidemics ...

... all connected systems get “infected”
GUEST EDITORS’ INTRODUCTION:
EVOLVING CRITICAL SYSTEMS

Lorcan Coyle, Mike Hinchey, and Bashar Nuseibeh, Lero—the Irish Software Engineering Research Centre
José Luiz Fiadeiro, University of Leicester
Example:

Safety

and

Automotive Industry
The only automobiles without software.
90% of automotive innovations are realised by software

Mercedes S-Class
Infotainment Subsystem
20 Mio. LOC

50 – 100 networked ECUs
Regulatory Framework for Safety in Automotive

- ISO DIS 26262
  - Based on ISO/IEC 61508
  - Driven by the automotive industry
  - More specific to industry needs in requirements both on process and product/service
Functional Safety Development Life Cycle

Confirmation measures related to the safety lifecycle

Safety Lifecycle

Concept phase
- Project Start
- Safety plan
- Hazard analysis, risk assessment, safety goals
- Functional and technical safety requirements
- V&V-plan
- V&V test cases
- V&V tests
- Safety analyses
- V&V test cases
- V&V tests
- Safety case
- Qualification of parts and components
- Qualification of software tools
- Proven in use argument

Product Development
- Start Product Development
- Sample
- V&V test cases
- V&V tests

Production, Operation
- Sample
- SOP
- End of Decommissioning

Reviews

Audits

(1) Project independent
(2) After initiation of product development
(3) After initiation of product development at hardware level
(4) After initiation of product development at software level
(5) After a major sample
(6) At product release
(7) During production and operation
(8) Intermediate
State of method and tool support for a ISO DIS 26262-based functional safety development lifecycle

• There is **method** support for **most** of the activities in the functional safety lifecycle.
• There are **tools** for **many** of the individual activities, but not for all.
• The is **no** underlying **lifecycle support** for integration and traceability.

Everybody is expected to do their own thing … best practice:FSSC
### Integrated Functional Safety Support Centre (FSSC)

#### The project side: Develop safe products

**Planning functional safety in projects**
- Sales support
- Supplier management
- Functional safety plan including
  - Analyses, design, and test for safety
  - Confirmation measures
  - Project safety process
- Safety know-how

**Managing functional safety in projects**
- Hazard analysis and risk assessment
- Functional and technical safety concept
- Safety architecture
- Safety analyses (FTA, FMEDA, ...)
- Test support
- Reviews, audits, assessments
- Safety case

#### Establish functional safety competence

- Safety training
- Safety job aid workshop
- Design for functional safety
- Safety analyses training (H&A, FTA, FMEDA)
- Testing safety-related products
- Functional safety networking
- Functional Safety Engineer Automotive

#### Managing functional safety for the Organization

- Safety process compliance check
- Provide organizational processes for safety
- Qualification of hard- and software components
- Qualification of software tools

---

**FSSC Strategy and Control**
# Planning Functional Safety in Projects

## Task descriptions

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales support</td>
<td>The Functional Safety Manager supports the sales department during the project preparation phase. He reviews the requests for quotation and the offers and estimates the impact of safety requirements on the project.</td>
</tr>
<tr>
<td>Supplier management</td>
<td>Project Manager and Safety Engineer develop and review the development interface agreements with the suppliers. The Safety Engineer is responsible for the safety-related deliverables e.g. safety requirements, safety verification results, analysis results.</td>
</tr>
<tr>
<td>Functional safety planning</td>
<td>The Safety Engineer sets up the safety plan describing the project specific safety lifecycle and tasks. The Project Manager is responsible to assign resources to the safety-related tasks and to update the project plan accordingly.</td>
</tr>
<tr>
<td>Safety know-how planning</td>
<td>Project Safety Engineer in cooperation with a competent trainer identifies the safety-related know-how needs of the project and plans trainings for the project team or know-how transfer from outside the project.</td>
</tr>
</tbody>
</table>
## Managing Functional Safety in Projects

### Task descriptions

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard analysis and risk assessment</td>
<td>Hazard analysis and risk assessment is performed by a team of experts once in the concept phase of the customer project and at any change of the safety-related system as part of impact analysis. Results are safety goals, top level safety requirements, and safety integrity levels required.</td>
</tr>
<tr>
<td>Functional and technical safety concept</td>
<td>During the concept phase hardware and software architects derive the functional safety requirements from the top level safety requirements. In a next step during product development they create the specification of the technical safety requirements.</td>
</tr>
<tr>
<td>Safety analyses (FTA, FMEDA)</td>
<td>Safety analyses are performed by a team of experts during system design to identify causes and effects of systematic failures and to initiate design improvements. Quantitative analyses are performed to estimate failure rates and to support safety validation.</td>
</tr>
</tbody>
</table>
## Managing Functional Safety in Projects

### Task descriptions

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testing</td>
<td>Testers supported by the Project Safety Engineer apply the test methods prescribed by the safety standard to verify that the product and its components comply with the safety requirements.</td>
</tr>
<tr>
<td>Reviews</td>
<td>Reviewers supported by the Project Safety Engineer examine work products to provide evidence that they meet safety requirements.</td>
</tr>
<tr>
<td>Audits</td>
<td>Auditors examine processes applied in the project to provide evidence that their implementation meets the process-related requirements of the safety standard.</td>
</tr>
<tr>
<td>Compiling safety case</td>
<td>The Project Safety Engineer progressively compiles the argument that the safety goals are complete and satisfied.</td>
</tr>
<tr>
<td>Safety assessments</td>
<td>The Safety Assessor assess the functional safety achieved by the item. Assessments include the product, the work products, the processes required for functional safety, and a general review of safety measures.</td>
</tr>
</tbody>
</table>
### Managing Functional Safety for the Organization

#### Task descriptions

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check process assets for safety compliance</td>
<td>The Safety Assessor checks process assets of the organization to identify gaps with respect to the process-related requirements of the safety standard.</td>
</tr>
<tr>
<td>Provide organizational processes for safety</td>
<td>The Functional Safety Manager is responsible to close the identified process gaps by providing organizational processes (e.g. safety analysis process) that comply with process requirements of the safety standard and can be applied in safety-related projects.</td>
</tr>
<tr>
<td>Qualification of hardware and software components</td>
<td>The Functional Safety Manager ensures that only qualified hardware and software components are used in safety-related projects. He is responsible to manage qualification testing and to provide qualification reports for components.</td>
</tr>
<tr>
<td>Qualification of software tools</td>
<td>The Functional Safety Manager ensures that software tools applied in safety-related development are qualified according to requirements of the safety standard.</td>
</tr>
</tbody>
</table>
## Establish Functional Safety Competence

### Task descriptions

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety training including</td>
<td>Safety trainings are planned and performed according to the qualification needs of the projects staff. A competent safety trainer moderates the workshops.</td>
</tr>
<tr>
<td>• Job-aid workshop</td>
<td></td>
</tr>
<tr>
<td>• Design for safety</td>
<td></td>
</tr>
<tr>
<td>• Safety analyses</td>
<td></td>
</tr>
<tr>
<td>• Testing</td>
<td></td>
</tr>
<tr>
<td>Functional safety networking</td>
<td>Networking supports the exchange of information and experiences related to functional safety. Practitioners learn from practitioners.</td>
</tr>
</tbody>
</table>
Where is the opportunity for Eclipse?

- Solve the support deficiencies by providing a “Functional Safety Lifecycle Support” platform

- Automotive Functional Safety Platform on Eclipse
  - Integration
  - Traceability
  - New tools

- Why Eclipse and Open Source?
  - Functional safety should be the hallmark of an industry, and not the competitive advantage of a few leading companies.
EAIWG

2008 Automotive Interest Group
  15 interested companies

2011 EAIWG - - key automotive players
  BMW
  Bosch
  Continental
EAIWG

Holy Grail \(\rightarrow\) Common Automotive Tool Chain
Realistic \(\rightarrow\) Integration to improve Traceability

Current Key Topics

- CDT
- Large Models
- *Functional Safety*
  - *E.g. collate topic related practices and tools from other domains.*

Related

Sphinx (ARTOP), TOPCASED, Opees, OpenETCS, …
Generalise the Functional Safety Considerations as “plugins”

• Safety
  • Aerospace
  • Transport
  • Automotive
  • Medical devices
  • …

• Security
  • Defence
  • Communications
  • Finance
  • …
  • Automotive

Different standards and different practices
Similar approach
What comes after safety and security?

• Reliability and robustness (ruggedness)
• Accessibility

And the pattern of spread will be equally explosive!
Contact

• Hans-Jürgen Kugler,
  Principal and Chief Scientist
  KUGLER MAAG CIE GmbH
  Leibnizstr. 11
  D-70806 Kornwestheim
  Germany

• +49 7154 1796 450

• hansjuergen.kugler@kuglermaag.com