Towards Declarative Safety Rules for Perception Specification Architectures

Johann Thor Mogensen Ingibergsson
MMMI, University of Southern Denmark

joint work with Ulrik Pagh Schultz and Dirk Kraft
Field Robots

• Why field robots?
  – Dangerous work.
  – Decreasing workforce.
  – Ecological Concerns.

• SAFE Project.
Context:
Safety Certification within Agriculture

• Why certification? Liability!
  – Robot causes damage due to manufacturing defects.
  – Robot causes damage simply by acting or reacting.
How to Certify Field Robots?

- No standard is available.
- Other Industries? Avionics?
- Interpretation for agriculture and field robots.
How is Certification Done within Software for Field Robots?

Issues with current standards.

- **Issue**: Research is solution driven.
- **Issue**: 20 papers in non-development-related, suggesting approaches are investigated.

[Source: Ingibergsson, Kuhrmann & Schultz, PROFES2015]
How to Certify Field Robots?

- **Issues with current standards.**
  - **Issue:** Use of standards is limited.
  - **Issue:** Loose connection between development practices and standards.

<table>
<thead>
<tr>
<th>Simulation</th>
<th>Formal implementation verification</th>
<th>Mathematical modeling and algorithms</th>
<th>System architecture and reuse</th>
<th>Misc</th>
<th>Behavior modeling</th>
<th>Formal specification deriving implementation</th>
<th>Not SW dev-related</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>1</td>
<td>0</td>
<td><strong>2</strong></td>
<td><strong>1</strong></td>
<td><strong>9</strong></td>
<td><strong>2</strong></td>
<td><strong>15</strong></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Certifying Field Robots

Based on Interpretation

• ISO 13482
  Risk assessment

• ISO 13849
  Functional safety Mechanics.

• ISO/DIS 18497
  Performance

• ISO 25119
  Functional safety electronics.

• IEC 61496
  Electro-Sensitive Protective Equipment (EPSE).
Implications of Standards on Development of Field Robots in Practice?
**ISO 26262-1:2011**

Road vehicles -- Functional safety -- Part 1: Vocabulary

**ISO 25119-4:2010(en)** Tractors and machinery for agriculture and forestry

**Introduction**

ISO 25119 sets out an approach to the design and assessment, for all safety life cycle activities, of safety-relevant systems comprising electrical and/or electronic and/or programmable electronic components (E/E/PES) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It is also applicable to municipal equipment. It covers the possible hazards caused by the functional behaviour of E/E/PES safety-related systems, as distinct from hazards arising from the E/E/PES equipment itself (electric shock, fire, nominal performance level of E/E/PES dedicated to active and passive safety, etc.).

---

**Functional Safety vs Performance**

- **Functional Safety**
  - Verification of input
  - Test of computations
  - Periodic testing
  - Verification of design
  - Verification of system
  - Heartbeat signals

- **Performance**
  - Detection Accuracy
  - Detection Classification
  - Algorithm capabilities

**Correct Split ... ?**
Example: Simple Vision Pipeline

1. Rectify and minimize distortion
2. Dense Disparity Image
3. Vision Algorithm
4. Smoothing / filtering
5. Segmenting Objects
Vision Pipeline Described with RPSL

Camera_Left: SensorComponent
- ImageType: Raw
- Color: Mono_Bayer
- Size: 480x752
- SystemType: Hardware

Bayer2Mono_Left: ProcessingComponent
- Algorithm: Bayer2Mono
  - Complexity: Low
  - SystemType: Software

Rectify_Undistort_Left: ProcessingComponent
- Algorithm: Remap
  - Complexity: Low
  - Region: full
  - SystemType: Software

Dense Disparity Image

Camera_Right: SensorComponent
- ImageType: Raw
- Color: Mono_Bayer
- Size: 480x752
- SystemType: Hardware

Bayer2Mono_Right: ProcessingComponent
- Algorithm: Bayer2Mono
  - Complexity: Low
  - Region: full
  - SystemType: Software

Rectify_Undistort_Right: ProcessingComponent
- Algorithm: Remap
  - Complexity: Low
  - Region: full
  - SystemType: Software

DisparityMap: ProcessingComponent
- Algorithm: DisparityMap
  - Complexity: Medium
  - Region: full
  - SystemType: Software

PointCloud_3D: ProcessingComponent
- Algorithm: DisparityMapTo3D
  - Complexity: Low
  - Region: full
  - SystemType: Software

[Source: Hochgeschwender, Schneider, Voos & Kraetzschmar, SIMPAR2014]
How to Introduce Functional Safety

Based on Interpretation

**ISO 25119** – Functional safety electronics.
- Develop software and hardware according to the standard.
- Software could be subjected to Misra, to create a foundation across standards.

**IEC 61496** – Electro-Sensitive Protective Equipment (EPSE).
- **Fault**: Shall force the system to a safe-state, i.e. full stop.
- **Multiple Faults**: Shall not influence the above reaction.
- **Periodic tests**: Ascertain functionality.

**ERROR**: Go to safe state.
DSL Proposal

\[ h = \text{Bayer2Mono\_Left\_output\_histogram}; \]

\[ \text{length (nonempty (h.bins))}/\text{length (h.bins)}>0.1; \]
\[ \text{max (h)} - \text{min (h)}>1000p; \]

\[ \text{length (PointCloud\_3D\_output\_inArea (Camera\_Left\_Landmark))}>900 \text{ 3D points}; \]
DSL Test images

(a) Left lens, covered.  (b) right lens, overexposed.
(c) Left lens, partial cover  (d) right lens, partial cover
Conclusion

Contributions

• Analysis of safety standards in the agricultural domain.
• Language concept for extending RPSL with safety annotations.

Future work

• Code generation for safety-critical hardware.
• Systematic evaluation of language design for the safety domain.
• Evaluation by safety experts.