Towards an Automated Verification Process for Industrial Safety Applications

Kleanthis Thrampoulidis\textsuperscript{2,1}, Doaa Soliman\textsuperscript{1}, and Georg Frey\textsuperscript{1}
\textsuperscript{1Saarland University, Saarbrücken, Germany, \textsuperscript{2}University of Patras, Greece}

IEEE Conference on Automation Science and Engineering (IEEE CASE 2011)
August 24-27, Trieste, Italy.

What is this presentation about?

- Integration of the traditional Mechatronics development process with safety engineering
  - A big challenge in Automation systems Engineering
- Mechatronic systems
  - Software implements the most significant and challenging part of their functionality.
  - Software is used to realize their most competitive advantages.
- Safety Engineering
  - is to assure that the system will behave as needed even when it fails.
Outline

• The 3+1 SysML-view Model
  – A solution to the integration problem in Industrial Automation Systems Engineering
  – Integration with Safety Engineering

• An approach to upgrade legacy systems to conform to safety standards
  – Case study: The XY coordinated table

• Automating the verification process
• Concluding remarks

The 3 discipline views model

Cross cutting Aspects
- functionality
- safety
- security

©K.Thramboulidis CASE 2011
The Integration Problem

The Integration Problem (Safety considered)
The 3+1 SysML-view model

Integration with existing tools

Source: K. Thramboulidis, "The 3+1 SysML View-Model in Model Integrated Mechatronics", Journal of Software Engineering and Applications (JSEA)
The MTS V-model

MTS requirements
MTS architecture
MTC requirements

repeat for each
composite MTC

MTC architecture
MTC verification

repeat for each
composite MTC

MTC Integration
MTC Integration test

software
electronics
mechanics

Primitive MTC construction

©K.Thramboulidis CASE 2011

The SysML4MIM profile - The MTC

Traditional Approach

The MIM approach

©K.Thramboulidis CASE 2011
Safety and IEC 61131

- consistency with **industry safety standards** is mandatory
  - general purpose, such as the IEC 61508,
  - domain specific such as the IEC 62061 for the machinery sector, IEC 61511 for the process industry sector and IEC 62227 for the railway domain.

- **IEC61131**
  - The use of verified safety libraries (e.g. PLCOpen) even though considered suitable to meet SIL 3 does not guaranty the safety level of the system.
  - Safety analysis should be performed ...

Safety Eng. in 3 discipline view model

[Diagram showing the relationship between Safety Engineer, Mechanical Engineer, and Software/Platform Engineer, with Modelica and CANOpen Magic tools and databases interconnected.]
Safety Eng. in 3+1 SysML-view model

MTS V-model and Safety
Key concepts of the integration

- Define the proper system behavior that is required to prevent hazards.
- Enables an operator to handle during operation-time a system state that may lead to a hazard or accident.

Legacy systems - The XY coordinated Table
Main challenges

1. Define safety requirements for the upgraded system.
2. Define requirements of the safety system.
3. Design the safety system.
4. Verify of the safety application.
5. Integration with the legacy system.
6. Verify the upgraded system.

Define Safety System’s Requirements
Safety Requirements

General safety requirements introduced by IEC 62061
R.1. to provide complementary protective measures, e.g. emergency stop;
R.2. to provide information for safe use, e.g. warning signals;
R.3. to reduce risk under conditions of failure or misuse e.g. automatic monitoring.

Project Specific safety requirements
R.3. Cell’s doors should be released for opening under safe conditions.
R.4. Cell’s doors should be locked before the system enters the “Automatic mode” of operation mode.
R.5. Motor’s speed should not exceed a given safe speed when in “Manual mode” of operation.

SysML4Safety profile
Legacy system behavior – Essential use case

Automatic mode of operation

<table>
<thead>
<tr>
<th>Operator</th>
<th>System Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close doors and select</td>
<td>Move the drawing table with the defined speed settings and</td>
</tr>
<tr>
<td>automatic mode</td>
<td>according to the selected task until the drawing table reaches the end position.</td>
</tr>
</tbody>
</table>

Hazard: “Protective cell door is open”
Cause: “Actor Misbehavior”
+ “Operator access the machine with his hand”
+ “High operating speed”
Consequence: Operator injury
Risk associated to this hazard: Probability x Severity → Not acceptable
Safety Measures: Guarded doors

Legacy system behavior – Upgraded use case

Select automatic mode.
Close the doors.
Give unlock command.
Check the status of doors.
Wait for doors to be closed.
Move the drawing table… end position.
Stop the motors safely.
Wait for the doors unlock request.
Unlock the doors.

Select automatic mode.
Check the status of doors.
If doors are open, then move drawing table with Low Safety Limited Speed … end position.
If doors are closed but not locked, then move drawing table with Medium Safety Limited Speed … end position.
If doors are locked, then move drawing table with Normal operating Speed … end position.
Stop the motors safely.
If doors are locked and there is an unlock request while performing the task, then reduce the speed to Medium Safety Limited Speed and unlock doors.

©K.Thamboulidis CASE 2011

21

©K.Thamboulidis CASE 2011

22
Sequence diagram to split behavior

Safety system: Hardware part
Safety system: Software part

PLC tool: SafeProg from KW software

Verification of the safety application
Transformation process

Transformation rules

1. Declaration Rule
   - Result: All external variables are globally declared.

2. SFB Rule
   - Result: All SFBs TA templates are defined.

3. Connections Rule
   - Result: All connections TA templates are defined.

4. Execution Flow Rule
   - Result: Execution priorities are defined.
Concluding Remarks

- Current practices for safety engineering are inappropriate for the development of Industrial Automation Systems
- The integration of the 3+1 SysML-view model with safety engineering provides a promising solution
- This methodology was adapted to upgrade legacy systems
- The verification of the safety application is automated using model transformations and the UPPAAL model checker.

Thank you for your attention!