A Component-Based Model-Driven Approach with traceability of concerns: Railway RBC Handover Case Study

YRS 2015, Roma, Italy

Marc Sango
PhD candidate, University of Lille 1 and IFSTTAR, France
marc.sango@ifsttar.fr
Outline

- What Standards Require About Model Driven Engineering (MDE)?
- What is not Addressed by Railway EN-50128 Standard for MDE?
- Our Approach: A unified meta-Model and its application process
- Evaluation through the RBC-RBC Handover Case Study
- Discussion and Conclusion
What Standards Require About Model-Driven Engineering?

> All Standards for **safety-critical transportation software** acknowledge the model-driven development and V&amp;V approach.

- **Railway**: CENELEC EN 50128 Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems

- **Avionic**: RTCA DO-178B Software considerations in airborne systems and equipment certification

- **Automotive**: ISO 26262 Road vehicles - Functional safety
What Standards Require About Model-Driven Engineering?

- All Standards for safety-critical transportation software acknowledge more and less the model-driven development and V&V approach.

- **Avionic**: RTCA DO-178B Software considerations in airborne systems and equipment certification
  - The new DO-178C standard is complemented by DO-331 for Model-Based Development and Verification Supplement.

- **Automotive**: ISO 26262 Road vehicles – Functional safety:

- **Railway**: CENELEC EN 50128:2011 Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems
  - “Model-driven” is used only once in the informative annex.
What Standards Require About Model-Driven Engineering?

- All Standards for safety-critical transportation software acknowledge more and less the model-driven development and V&V approach.
What is not addressed by the Standards for MDE?

1. How are requirements **traced** in the models?
What is not addressed by the Standards for MDE?

1. How are requirements traced in the models? Instead of **requirement traceability** we prefer the name **traceability of concerns**.
What is not addressed by the Standards for MDE?

1. How are requirements traced in the models?
2. How can **temporal constraints** be **modeled** and verified?

At any time « uti » must be between « sol » and « on »
What is not addressed by the Standards for MDE?

1. How are requirements traced in the models?
2. How can **temporal constraints** be modeled and **verified**?

At any time «uti» must be between «sol» and «on».
What is not addressed by the Standards for MDE?

1. How are requirements traced in the models?
2. How can temporal constraints be modeled and verified?
3. How are requirements concretely reflected in the models?
Summary of the motivation context

- We have seen that standards require about MDE for quality reasons.
- We have also seen that they do not addressed specific questions, such as a concrete realization of solution model.
- Then, we saw that the component-based MDE is one response of this question.
- Let now introduce our component-based MDE approach.
Our approach: Meta-Model

The core of our approach is an **unified meta-model** towards a traceability of concerns but in the same UML-Based formalism.
Our approach: Application Process

Generic process that can be used to instantiate the meta-models
Evaluation: Scenario definition phase

- RBC-RBC Handover scenario in ERTMS/ETCS Systems
Evaluation: Scenario definition phase

RBC-RBC Handover scenario
Evaluation: Modeling and Verification phase
Evaluation: Tracing phase

Traceability Matrix
Evaluation: Cost Benefits Analysis

\[
\text{C&P-CostSaving} = FS_{\text{cost}} - (S_{\text{cost}} + A_{\text{cost}} + D_{\text{cost}} + Q_{\text{cost}})
\]

\[
\text{CBD-CostSaving} = FS_{\text{cost}} - (S_{\text{cost}} + R_{\text{cost}} + GD_{\text{cost}} + T_{\text{cost}} + A_{\text{cost}} + D_{\text{cost}} + Q_{\text{cost}})
\]
Evaluation: Cost Benefits Analysis

\[
\text{C&P-COSTSAVING} = FS_{\text{cost}} - (S_{\text{cost}} + A_{\text{cost}} + D_{\text{cost}} + Q_{\text{cost}})
\]

\[
\text{CBD-COSTSAVING} = FS_{\text{cost}} - (S_{\text{cost}} + R_{\text{cost}} + GD_{\text{cost}} + T_{\text{cost}} + A_{\text{cost}} + D_{\text{cost}} + Q_{\text{cost}})
\]

Total C&P vs CBD coast saving in 3 versions of LC-APS case study
Discussion & Conclusion

<table>
<thead>
<tr>
<th>Categories</th>
<th>Sub-categories</th>
<th>Approaches</th>
<th>Discussion criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Traceability</td>
<td>Interoperability</td>
</tr>
<tr>
<td>General-Purpose</td>
<td>OOP-Based</td>
<td>EJB</td>
<td>(✓)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fractal</td>
<td>(✓)</td>
</tr>
<tr>
<td></td>
<td>ADL-Based</td>
<td>AADL</td>
<td>(✓)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pin</td>
<td>(✓)</td>
</tr>
<tr>
<td>Specialized-Purpose</td>
<td>OOP-Based</td>
<td>Think</td>
<td>(✓)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CHESS</td>
<td>(✓)</td>
</tr>
<tr>
<td></td>
<td>ADL-Based</td>
<td>IEC-61499</td>
<td>(✓)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SARA</td>
<td>(✓)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AUTOSAR</td>
<td>(✓)</td>
</tr>
</tbody>
</table>

Our solution is a triple meta-models towards a traceability of concerns but in the same UML based formalism.
We formally define interoperability of our component model interface. This provides a baseline for other rules, such as component composition.
## Discussion & Conclusion

The formal model is used in the model transformation into a verification model for which we can use formal verification tool.

<table>
<thead>
<tr>
<th>Categories</th>
<th>Sub-categories</th>
<th>Approaches</th>
<th>Discussion criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Interoperability</td>
</tr>
<tr>
<td>General-Purpose</td>
<td>OOP</td>
<td></td>
<td>(√)</td>
</tr>
<tr>
<td>Specialized-Purpose</td>
<td>OOP</td>
<td></td>
<td>(√)</td>
</tr>
<tr>
<td>ADL-Based</td>
<td>ProCom</td>
<td></td>
<td>(√)</td>
</tr>
<tr>
<td></td>
<td>IEC-61499</td>
<td></td>
<td>(√)</td>
</tr>
<tr>
<td></td>
<td>SARA</td>
<td></td>
<td>(√)</td>
</tr>
<tr>
<td></td>
<td>AUTOSAR</td>
<td></td>
<td>(√)</td>
</tr>
</tbody>
</table>
As in academic component models certification support is weaker in our model. However, it is crucial to develop a solid understanding of the impact from individual components on the overall dependability of the system for certification reason.
Discussion & Conclusion

Traceability
- We have compared the most relevant work related to traceability of concerns,
- and highlight the benefits for component based model driven development.

V&V
- Model transformation is used to transform our high level model
- into a TA model for which we have used UPPAAL model checker for verification.

Interoperability
- In addition to current component models rules, such as composition and reusability,
- we have defined interoperability, by highlighting domain knowledge.

Certification
- The certification support is generally weaker in academic component models,
- mostly due to extensive cost and the need of clear industrial application.
Thanks for your attention

Marc Sango
PhD candidate,
IFSTTAR/COSYS/LEOST
marc.sango@ifsttar.fr