D2.1.1 – Modelica extensions for properties modelling

Part I: Users motivation

WP2.1 – Properties modelling language
WP2 – Properties modelling and Safety

MODRIO (11004)

Version	1.0
Date	30/09/2014

Authors

Name	Affiliation
Audrey Jardin	EDF
Eric Thomas	Dassault Aviation

Executive summary

The main goal of sWP2.1, entitled “Properties modeling language”, is to extend Modelica to property modelling in order to use such property models to check system design and operation against requirements.

The objective of this document is to present the users motivation for such an approach and give a glimpse of potential industrial applications it can lead to.

This document refers to the part I of deliverable D2.1.1.

Table of contents

Executive summary **2**
Table of contents **3**
Glossary **4**
1. Users motivation **5**
2. Potential industrial applications **6**
2.1. In the energy domain 6
2.2. In the aircraft domain 7
3. References **7**

Glossary

I&C	Instrumentation & Control
WP	Work Package
sWP	sub Work Package

1. Users motivation

The main goal of sWP2.1, entitled "Properties modeling language", is to extend Modelica to property modeling in order to use such property models to check system design and operation against requirements.

However, before going into details on how such an approach can be implemented (which is documented in the other parts of deliverable D2.1.1), it is worth explaining why the concept of "property models" is appealing for an end-user and how it can open (or reinforce) a range of several applications in many industries, such as in the energy or the aircraft domains.

Need for a rigorous framework for systems validation

Facing ever increasing constraints in terms of safety, environmental or economical performances, systems become more and more complex. Therefore engineers need more powerful tools to take decisions rapidly and meet the "time-to-market" rule. Modeling and simulation tools at a system level (like Modelica environments) are now rather well adopted in the industries to assist engineers in that task. However, such tools focus until now only on efficient simulation of the behavior of the system. They do not propose any particular assistance for conducting verification tests. Usually the engineer has at his disposal one or several behavioral models that capture different aspects of the design choices for the system and runs several simulations to investigate whether the system requirements are satisfied or not. The relevance of the tests hence conducted depends on how well the models and test scenarios represent the system behavior w.r.t. the actions that may be performed on the system. The idea behind property modeling is that better model and scenario quality may be achieved when using formal requirements of the system. Experiment conducted at EDF R&D showed that formalizing requirements with property modeling indeed improves the quality of the requirements themselves by removing ambiguities, omissions or inconsistencies. It is expected that the property model of the requirements may be used as an observer to conduct the verification test automatically to detect possible violations in the requirements, and that it will be possible to generate automatically test scenarios from the property models. Automating the production of test scenarios and test runs should improve significantly the test coverage and therefore the demonstration that the system operates properly.

Expected added-value all along the system lifecycle

Formalizing the requirements into appropriate models should improve the engineering processes all along the system lifecycle from the design to the operational phase.

In particular, it is expected to:

- Improve the specification phase by providing an explicit and unambiguous list of system requirements (including assumptions on the environment of the system and designer's assertions regarding the system internal behavior). Formulating the requirements into formal statements will indeed enhance their legibility and avoid potential misunderstandings of their meanings. New static tests on the requirements model may also be imagined to automatically check the coherence of the system requirements or to point out their incompleteness;
- Ease the capitalization and the transmission of knowledge by having at a glance a functional point of view on how the system should behave (through system requirements, properties models document also operating domains and system functional constraints) whereas such expertise is rather long to develop over time especially for complex systems. As the requirements become executable under the form of property models when associated with a behavioral model, newcomers will indeed be able to virtually "play with the system" by running several simulations and then better understand the reason of each system requirement;
- Better keep track (and hence better assess the impact) of the evolutions of the system requirements (e.g. due to regulation evolutions, to changes in operational expectations …)

simply by updating the appropriate property models;

- Improve the validation phase by automating the checking procedures. Such automation will indeed give more rigor to the tests (they will be less prone to human errors, the different items being examined systematically and not by hand anymore). It will also potentially increase the test coverage (more test scenarios will be simulated);
- Enable new engineering studies by supporting advanced modeling techniques like mode switching. Property models can indeed be used to describe for instance the limits beyond which the system enters a dysfunctional mode. It can thus help to simulate models beyond normal operating conditions and make it possible to explore the full chain of consequences from an initiating event on the system. This will be very helpful in the design phase to complement the classical penalizing scenarios for the sizing of the system with new scenarios that challenge the system beyond its normal operating conditions, and in the operation phase to better diagnose the system state.

2. Potential industrial applications

As described in the previous section, modeling and simulating properties will improve many engineering processes all along the system lifecycle. It will reinforce the specification phase, ease the traceability and the impact analysis of system requirements, improve the rigor and the coverage of the testing phase and help to investigate the multiple operating modes of a system. Let us see now in practice how such technology may be applied in industries such as in the energy and the aviation domains.

2.1. In the energy domain

The major power plants projects at EDF mainly concern existing plants (e.g. lifetime extension up to 60 years, power uprate, availability improvement, …) and the construction of new plants (e.g. nuclear, renewable, …). They take place in a context where the role of Instrumentation and Control (I&C) systems become more and more important: they must satisfy numerous objectives in terms of safety, dependability and performance. Due to ever increasing safety constraints and environmental rules, the following question is hence of prime interest: will the plant systems (their physical parts together with their I&C systems), as specified and designed, guarantee the properties expected?

Currently, power plants models are used to study several physical phenomena on different time scales (e.g. robustness to transients for short time scales, and ageing for longer time scales). A difficulty of such verification is that the required properties can be found mainly in a textual manner and in paper documents intended to the engineering entities (e.g. documents used for safety evaluation, for subsystems description or for operation technical specifications). A first observation can thus be acknowledged: there is a real need to formalize and capitalize on these different properties in order to ease the transmission of knowledge on the power plant requirements (i.e. overall goals, components constraints and modeling assumptions), to keep track of the requirements evolutions, and design choices, and to remove the sources of ambiguity that could lead to misunderstandings.

Besides, although some studies already include I&C alarms that monitor key properties, many simulations rely on these alarms to determine whether the plant system is robust during transients. However, one can argue that it is inappropriate to rely on I&C to assess the robustness of a plant system, as an error in I&C, like a missing alarm or an insufficient set of sensors, could lead to a wrong conclusion. One needs to ensure that the monitoring by the I&C does reveal all properties violations. Moreover, correctness of the I&C implementation with respect to its specifications may not be sufficient, as there is a potential for the specifications to be incomplete or worse incorrect. A more appropriate approach to validate the physical system as well as its I&C system is to define properties as close to the physical system as possible.

In that context, modeling and simulating properties will:

- Enhance the demonstration of safety by validating I&C functional requirements specifications through joint modeling and simulation of physical and I&C subsystems;
- Improve documentation on plant systems which is a key issue to be faced when extending the power plant lifetime up to 60 years and when providing appropriate information to the next generations for future upgrades 30 or 40 years from now;
- Optimize power plant operation and power plant maintenance by a better monitoring of the actual operating modes and their potential evolution faced to an upcoming event.

2.2. In the aircraft domain

At Dassault Aviation, many types of energy systems must be analyzed to assess performance and nominal operation of an aircraft in the ranges of its operational uses, in relation to variability of operation (take-off, cruise, landing and induced use of systems), of environment (included loads on circuit items) and of equipment operation (natural variability of nominal actuation and potential failures that may occur during operation).

To analyze potential consequences and avoid them by adapting aircraft architecture and equipment specifications, different types of analysis are performed (such as safety analysis, functional analysis, robustness analysis, sensitivity analysis, dysfunctional analysis, etc.).

Use of properties models will help to automate the different analysis thus performed. It will ease the update of the requirements accordingly and then the communication between aircraft integrator and suppliers.

3. References

[1] Bouskela D., *MODRIO Full Project Proposal*, version 2.1, January 2013.

[2] *ITEA2 EUROSYSLIB Project*, information available at: http://www.eurosyslib.com/

[3] Jardin A., Bouskela D., Nguyen T., Ruel N., Thomas E., Chastanet L., Schoenig R., Loembé S., *Modelling of System Properties in a Modelica Framework*, in Proceedings of the 8th International Modelica Conference, Dresden, Germany, March 20-22, 2011.

[4] Jardin A., Nguyen T., Ruel N., *EUROSYSLIB Project – sWP7.1 – Properties modeling*, EDF technical report, H-P1C-2011-00913-EN, August 2011.

[5] *ITEA2 OPENPROD Project*, information available at: http://www.ida.liu.se/labs/pelab/OpenProd/

[6] Schamai W., Jardin A., Bouskela D., *Industrial Use Cases for Requirements Verification and Model Composition in ModelicaML*, 7th MODPROD Workshop on Model-Based Product Development, Linköping, Sweden, Feb. 5-6, 2013.

[7] Bruel. G, Jardin A., *OPENPROD Project – WP6 – I&C functional validation based on the modelling of requirements and properties: evaluation of ModelicaML*, EDF technical report, H-P1A-2012-03040-FR, February 2013.