Model-Based Engineering in Real-Time Embedded Systems: Specifying Timing Constraints

Damjan Temelkovski, Ljerka Beus-Dukic

University of Westminster, United Kingdom

damjantemelkovski@gmail.com, l.beus-dukic@westminster.ac.uk

Abstract. This paper presents the results from a research project on development of Real-Time Embedded Systems (RTESs) using a Model-Based Engineering (MBE) approach. A review of the state-of-the-art modelling languages was done in order to assess their capabilities to model time. A chosen case-study, a Brake-By-Wire (BBW) system, was taken from the automotive industry. The case study focuses on the use of EAST-ADL to model the RTES and TADL to specify timing constraints. A different approach using MARTE to model the BBW system was developed within our project. This approach is used to compare MARTE (and OCL) with EAST-ADL (and TADL). The results show that MARTE can be used to model an RTES from the automotive industry but lacks some important semantic expressions for the timing constraints which are present in TADL.

Keywords: model-based engineering, real-time embedded systems, MARTE, EAST-ADL, brake-by-wire

1 Introduction

A Real-Time Embedded System (RTES) is an embedded system where the correctness of the system depends on the logical correctness of the results and on the time at which they are produced [1]. RTESs are safety-critical if a failure of the system leads to the loss of human lives. Large and complex RTESs can benefit from a development process such as Model-Based Engineering (MBE). The main benefit of MBE is that performance analysis can be done on a model of the system, in the early stages of development. This includes timing analysis – a key issue in RTESs.

Sections 2 and 3 introduce MBE and popular modelling languages. Section 4 and 5 describe the case study and our approach using MARTE. Section 6 compares EAST-ADL and MARTE, while the conclusion and further work are in Sections 7 and 8.

2 Model-Based Engineering

In MBE models are the central part of the development process. It includes creating (modelling), analysing (analysis), and executing (implementation) models.

The analysis of models can predict the system's performance and the system can be tested prior to the implementation [2]. Fig. 1 shows the flow of a model-based development of an RTES.

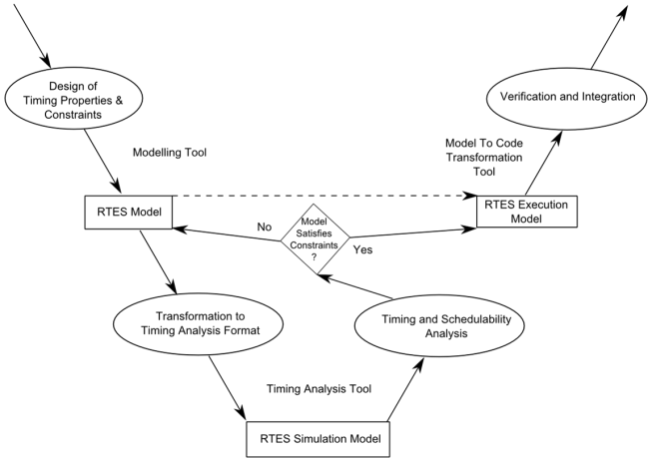

Fig. 1. A model-based engineering process

3 Review of Modelling Languages in RTESs

Timing has become an important part of UML since version 2.0 which defines the timing diagram and meta-classes such as: TimeExpressions, TimeObservations, and Durations [3].

The UML timing diagram is used to display the change in state or value in elements over time and it can be used to specify time-related behavior (Fig. 2).

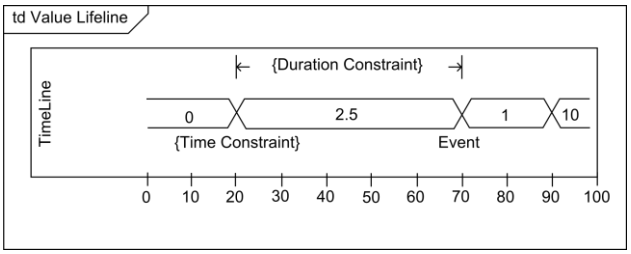

Fig. 2. The UML timing diagram

Even though timing constraints can be specified in UML, the way of modelling time in UML (known as SimpleTime) is too simple for complex RTES. This has caused Domain Specific Languages (DSLs) to become more used in the industry. DSLs are created with the help of domain experts so they include familiar concepts and syntax and are straight forward to use.

AADL (Architecture Analysis & Design Language) is a component-based modelling language mainly used in the avionics and aerospace industries. Each component can have timing properties that describe the timing information; subsequently, timing analysis can be done on AADL models [4].

AUTOSAR (AUTomotive Open System ARchitecture) is a software architecture standard for the automotive industry. AUTOSAR's timing extensions use two main concepts: Timing Event and Timing Event Chain [5].

EAST-ADL (Electronics Architecture and Software Technology - Architecture Description Language) is a modelling language that provides an abstraction of AUTOSAR divided into several levels: vehicle, analysis, design, and implementation. The vehicle level defines what features the vehicle should provide. The analysis level provides functional abstractions about the system's behaviour. The design level provides a hardware-oriented view of the RTES, and the implementation level is the AUTOSAR-compliant code. EAST-ADL defines: event constraints (set on an event), offset constraints (set on several events), and delay constraints (set on an event chain). Delay constraints can be: age, reaction or input/output synchronization constraints [6].

MARTE (Modeling and Analysis of Real-Time Embedded systems) is a UML profile for RTESs based on the UML profile for Schedulability, Performance, and Time (SPT) and the Systems Modeling Language (SysML), an extension of UML for systems engineering. MARTE is used to model any kind of RTESs [7, 8]. Most of the time concepts are in the Time and the NFP (Non-Functional Properties) packages. MARTE includes customizable clocks and elements explicitly bound to them [9].

Table 1 shows a summary of these modelling languages; the first column (Timing Model) shows the name of the model or mechanism for handling time in the language.

	Timing Model	Originally Used In	Currently Used In
UML	SimpleTime	Software Modelling	System Modelling
AADL	Timing Properties	Avionics	RTES Modelling
AUTOSAR	Timing Extensions	Automotive Modelling	Automotive Modelling
EAST-ADL	TADL Concepts	Automotive Modelling	Automotive Modelling
SPT	Time Domain Model	Analysis in Software Modelling	(Deprecated)
MARTE	Time Package	RTES Modelling	RTES Modelling

Table 1. Summary of the review of modelling languages for RTESs

4 Case Study

ITEA2's [10] project TIMMO-2-USE defined the language TADL which is used on top of EAST-ADL to specify timing constraints. One of the examples described in the project is a Brake-By-Wire (BBW) system in an automobile [11]. A BBW system is a

braking system with no mechanical connection between the brake pedal and the wheels. Instead, the braking force is applied by actuators controlled by an RTES. Sensors on the brake pedal measure its angle and alert a central controller when it has been pressed. The wheels' speed is also measured by sensors and sent to a controller. It calculates the necessary torque that needs to be applied to the wheels and triggers the actuators. This BBW system also uses the antilock braking system (ABS).

4.1 Timing Constraints

Multiform timing constraints are constraints where simultaneity and precedence between events give the only notion of time [12]. The case study includes multiform timing constraints such as TC1: "*The vehicle shall start to brake within 5 meters after the brake pedal is pressed*". This timing constraint is set on an event chain starting with the brake pedal event and ending with the wheel actuator event. On the vehicle level it is an EAST-ADL «reactionConstraint» with the property "upper" set to 5m.

On the analysis level the model is refined. The mentioned timing constraint (TC1) is split into four reaction constraints. Each constraint is attached to a separate event chain between the brake pedal event and one of four actuator reaction events.

Local Device Managers (LDMs), that act as the software interface for the sensors and actuators, have been defined on the design level. A 5-ECU (Electronic Control Unit) system has been designed, using an Ethernet ring topology. Each wheel has its own ECU and there is an additional main controller ECU. Each of the four reaction timing constraints for TC1 has been remodelled as three different mode-dependant constraints, resulting in 12 constraints. The three modes that have been defined are depending on the vehicle's speed [13]:

- mode 1: 0 m/s $\leq v <$ 30 km/h (8.333 m/s) $\rightarrow$ 0.0 s $\leq t <$ 600 ms (0.6 s)
- mode 2: 8.333 m/s $\leq v <$ 90 km/h (25m/s) $\rightarrow$ 0.6 s $\leq t <$ 200 ms (0.2 s)
- mode 3: 25 m/s $\leq v <$ 130 km/h (36,111 m/s) $\rightarrow$ 0.2 s $\leq t <$ 138 ms (0.138s)

In the worst case scenario the car would start braking exactly 5m after hitting the break. Therefore, $s = 5$m, v being the speed, the time (t) can be calculated.

The case study showed how the timing constraints can be specified in the model of the system in the early stages of development. It has shown how the EAST-ADL timing constraints such as: Reaction, Age, ExecutionTime, PeriodicEvent, Input and Output Synchronization Constraints can be used.

Tools used for modelling included Papyrus and SystemDesk. Tools used for implementation (code-generation) included: Simulink, TargetLink, and ArcticStudio. The timing analysis tools used were: aiT, TCNAnalyzer, SymTA/S, and INCHRON.

The large number of tools in the example shows that model-based development with EAST-ADL cannot be done with a single tool. For instance, the model in Papyrus describes the timing constraints, but it has not been directly used to generate code. Instead the timing information from this model has been manually added to a Simulink model used for code generation. An approach which would avoid the remodelling of the system in different tools would be preferred.

5 Model of the BBW System in MARTE

Our model of the BBW in MARTE uses the EAST-ADL levels: vehicle, analysis, and design [13].

5.1 Vehicle Level

Use-Case Diagram. Since use-case diagrams are used to describe the behaviour of a system i.e. what the system would do without specifying the detail of how it would be done, they are very suitable for the vehicle level (Fig. 3).

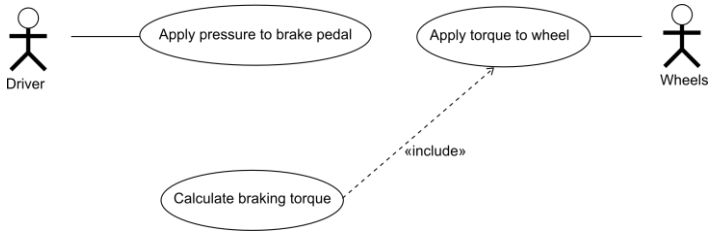

Fig. 3. MARTE use-case diagram on vehicle level

Class Diagram. The class diagram on the vehicle level hides the details of the system and presents it as a black box (Fig. 4). The timing constraint "*The vehicle shall start to brake within 5 meters after the brake pedal is pressed"* is modelled using a SysML Requirement. SysML's «refine» stereotype couldn't be used in Papyrus, so a «requirementRelated» edge was defined. Two events, a BrakePedalPressure_Event and an ActuatorReaction_Event, have an «nfp» property that is specifying when they have occurred. This «nfp» property is of the «NfpType» DistanceUnit, so it is expressed in "unusual" units (distance units).

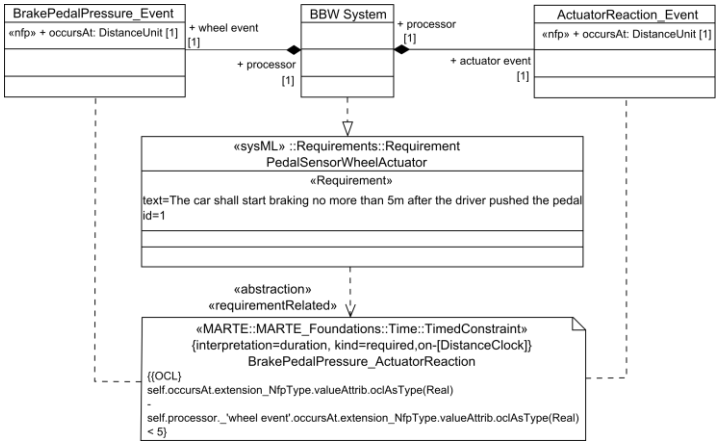

Fig. 4. Excerpt from the MARTE class diagram on vehicle level

The timing constraint is connected to a new type of MARTE clock. The unit of this clock is *metre* and it ticks on each 1mm (resolution = 1mm). The timing constraint is a MARTE «timedConstraint» and an OCL rule specifies that the difference between the occurrences of the brake pedal and actuator events needs to be less than 5. This shows MARTE's capability to model multiform time.

Sequence Diagram. The sequence diagram focuses on showing the dynamic side of the system. It uses MARTE's «timedObservation» to annotate the starting of the calculation of the torque and its application to the wheel. These two timedObservations are connected to a DistanceClock. A «timedConstraint», also connected to the DistanceClock, is added to specify that their difference needs to be less than 5 (Fig. 5).

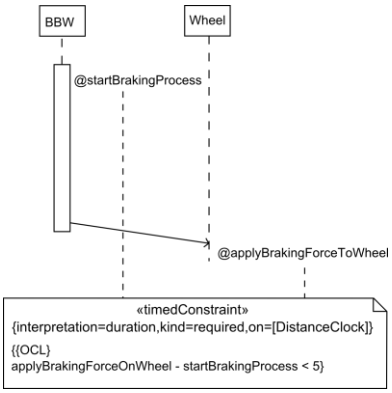

Fig. 5. Excerpt from the MARTE sequence diagram on vehicle level

5.2 Analysis Level

Use-Case Diagram. The use-case diagram at the analysis level shows a more detailed view of the system with all the BBW components displayed as actors (Fig. 6). It can be noted that the ABS seems to be the most involved actor.

Class Diagram. At the more detailed analysis level, the clock based on multiform time is still used for some constraints. The BBW system is decomposed to: brake torque calculator, brake controller, ABS, vehicle speed estimator, wheel speed sensor, and actuator. The pedal and actuator have two events, brake pedal pressure event and actuator reaction event.

These events have an «nfp» property of the distance unit type (their values are shown in metres) and they are constrained by a «timedConstraint». An OCL rule is again responsible for showing that the difference between the actuator event and the brake pedal occurrence should be less than 5 metres. Fig. 7 shows an excerpt from the class diagram on the analysis level, focusing on this timing constraint.

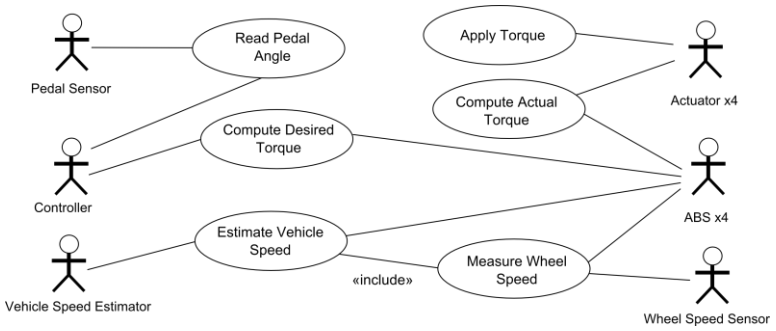

Fig. 6. The use-case diagram on the analysis level

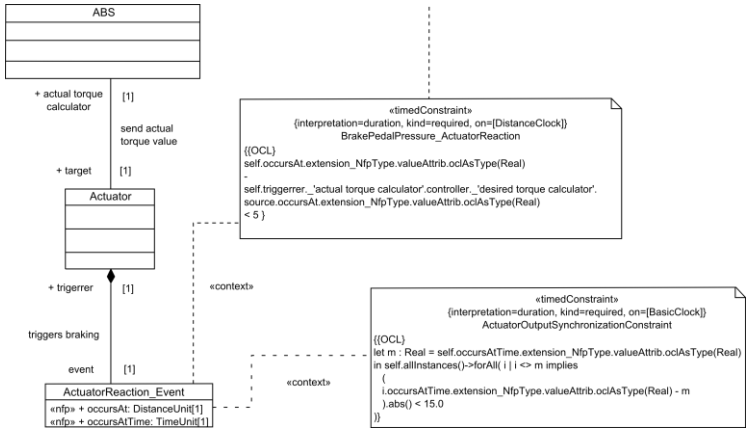

Fig. 7. Excerpt from the MARTE class diagram on analysis level

Sequence Diagram. The sequence diagram on the analysis level shows a better dynamic view of the system by describing the way that the message passing would go. The controller alerts the wheel speed sensor to measure and send the speed of the wheel to the vehicle speed estimator and the ABS. What the sequence diagram does not show that well is that there are in fact four ABSs and four wheel speed sensors, and they all need to be informed separately.

5.3 Design Level

Use-Case Diagram. The design level has a use-case diagram of the hardware components. This helps understand the mapping of the software components to the hardware elements (the ECUs). It shows what specific set of actions each ECU needs to do.

Class Diagram. The class diagram on the design level shows the most detailed view of the system. A global controller acts as a central unit for managing the data from the

wheel sensors and the brake pedal sensor. It is connected to the four wheels and the four ABSs.

A mode dependant timing constraint has been modelled by using three different constraints depending on the vehicle speed (Fig. 8). OCL rules are used to compare the time when the pedal pressure event occurred and the time when the actuator events occurred.

At this abstraction level multiform time clocks are not used and all the timing constraints are represented in time units (*ms*). Therefore all «nfp» properties of the brake pedal pressure event and the actuator event have time units.

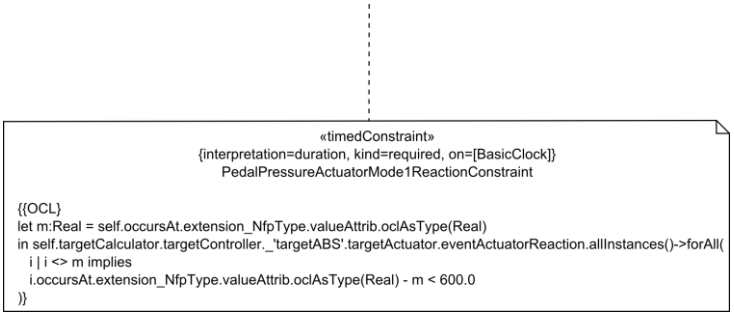

Fig. 8. The timing constraint TC1 in mode 1 in the MARTE class diagram on design level

5.4 Summary

The MARTE model is split in vehicle, design, and analysis levels, similarly to the EAST-ADL model, and it uses use-case, sequence, and class diagrams. The vehicle and design levels contain timing constraints that refer to a multiform clock defined as DistanceClock, which shows the use of multiform time in MARTE. It also shows how the timing constraints can be included in sequence diagrams.

The timing constraints were specified using OCL and its shortcomings were overcome by using MARTE's «nfp» properties.

Due to the lack of specific semantics for the kinds of timing constraints (age, reaction, execution, etc.) in MARTE, new class properties had to be used. In EAST-ADL this is done more formally using the properties of the timing constraints (e.g. *upper*).

6 EAST-ADL Versus MARTE

EAST-ADL has been developed specifically for the automotive industry. Its main goal is to provide higher levels of abstraction for AUTOSAR. Research comparing EAST-ADL to MARTE [14] provides mapping of the EAST-ADL properties into respective MARTE properties.

Proactive performance engineering methods can be easily done on an EAST-ADL model due to the layered architecture. The EAST-ADL timing constraints from the case study are compared with the MARTE constraints used in our model (Table 2).

	EAST-ADL Timing Constraint (value)	MARTE Timing Constraint (value)
1	Reaction (upper)	TimedConstraint («nfp» class property:TimeUnit)
2	Execution (upper)	TimedConstraint (class property:Real)
3	Periodic (period)	TimedConstraint (class property:Real)
4	InputSynchronization (upper)	TimedConstraint («nfp» class property:TimeUnit)
5	OutputSynchronization (upper)	TimedConstraint («nfp» class property:TimeUnit)

Table 2. Comparison of the EAST-ADL timing constraints and the timing constraints used in the MARTE model

MARTE is not focusing on a specific kind of RTES and this universal character is one of its benefits. It is a UML profile, therefore an experienced UML modeller will find it intuitive and straight forward to use.

However, modellers that don't use UML may prefer another DSL. EAST-ADL's main benefit is that it is closer to the modeller experienced with automotive RTESs, especially with AUTOSAR. Furthermore, EAST-ADL offers specific semantics for different types of timing constraints used in the automotive RTESs.

A disadvantage of EAST-ADL was shown in the case study, where several tools were needed in order to produce code and to perform timing analysis. There is a possibility to use Acceleo (to generate code) and Cheddar (for timing analysis) directly on the MARTE model, which would be an advantage for MARTE.

7 Conclusion

The MARTE model proved that MARTE can be used to model systems from the automobile industry. However, it cannot be said that it would be the best approach since the only benefits over EAST-ADL are its universality and the potentially simpler tools. The main drawback is the lack of semantic support for specific kinds of timing constraints.

8 Further Work

The Eclipse plug-in Acceleo can transform the MARTE model from Papyrus into code, but specific transformation templates to MARTE are necessary.

Mappings of the MARTE concepts for the timing analysis tool Cheddar have already been developed. However, they need to be compatible with the latest version of MARTE. Further work on these tools will make MBE with MARTE simpler.

Acknowledgements. This research has been supported by the EUROWEB Project funded by the Erasmus Mundus Action II programme of the European Commission.

References

1. Stankovic, J. A: Misconceptions about real-time computing: a serious problem for next-generation systems. Computer, vol. 21, no. 10 (1988)
2. Feiler, P. H., Gluch, D. P: Model-Based Engineering with AADL; An Introduction to the SAE Architecture Analysis & Design Language. Addison-Wesley (2013)
3. Bennett, S., Skelton, J., Lunn, K: Schaum's Outline of UML, 2nd ed. McGraw-Hill International (2004)
4. Ma, Y., et al: Toward polychronous analysis and validation for timed software architectures in AADL. In Proceedings of the Conference on Design, Automation and Test in Europe, pp. 1173-1178. (2013)
5. AUTOSAR Timing Extensions 411. http://www.autosar.org/download/R4.0/AUTOSAR_TPS_TimingExtensions.pdf
6. EAST-ADL Domain Model Specification. http://www.east-adl.info/Specification/V2.1.11/EAST-ADL-Specification_V2.1.11.pdf
7. Iqbal, M. Z., Ali, S., Yue, T., Briand, L: Experiences of Applying UML/MARTE on Three Industrial Projects. In MODELS 2012, LNCS 7590, pp. 642 – 658 (2012)
8. Briand, L., et al: Research-Based Innovation: A Tale of Three Projects in Model-Driven Engineering. In MODELS 2012, LNCS 7590, pp. 793 – 809 (2012)
9. André, C., Mallet, F., De Simone, R: Time modeling in MARTE. In ECSI Forum on specification & Design Languages (FDL), pp. 268-273 (2007)
10. ITEA2 Official Web Site. http://www.itea2.org/
11. Schliecker, S., et al: TIMMO-2-USE Brake-By-Wire Validator. ITEA2
12. André, C., Mallet, C., Peraldi-Frati, M-A: A multiform time approach to real-time system modeling; application to an automotive system. In Industrial Embedded Systems. SIES'07. International Symposium on, pp. 234-241. IEEE (2007)
13. Temelkovski, D., Beus-Dukic, L: Model-Based Engineering in Real-Time Embedded Systems: Specifying Timing Constraints, University of Westminster (2014)
14. Espinoza, H., Gérard, S., Lönn, H., Kolagari, R.T: Harmonizing MARTE, EAST-ADL2, and AUTOSAR to Improve the Modelling of Automotive Systems. In The Workshop STANDRT, AUTOSAR (2009)