Cyber-Physical System and Contract-Based Design

A Three Dimensional View

Daniela Cancila
CEA, LIST
CEA Saclay - F91191
Gif-sur-Yvette Cedex
daniela.cancila@cea.fr

Hadi Zaatiti
CEA, LIST
CEA Saclay - F91191
Gif-sur-Yvette Cedex
hadi.zaatiti@cea.fr

Roberto Passerone
DISI, University of Trento
38123, Trento
roberto.passerone@unitn.it

ABSTRACT

This work reports on the experience arising from the master internship *contract-based design tailored to safety issues for cyber-physical systems (CPS)*. The main educational goal is to confront the student with realistic mixed-critical smart CPS systems, using the railway domain and autonomous trains as a case study. The results show that, for this class of systems, education should transition from a 2D to a 3D modeling design space, which is much better suited to visualizing the evolution and the underlying properties of the system. We use contract-based design to properly deal with the integration and composition of heterogeneous components, where safety aspects require special attention. The main scientific and technical results concern the implementation of contract-based design in a 3D tool. Finally, we discuss the teaching methodology underlying the internship and the competences required to address the design of a (critical) CPS by the new generation of students.

Keywords

Contract-Based Design, Railway, Cyber-Physical System, 3D tool

1. INTRODUCTION

One important and characteristic feature of CPS is the property of *autonomy*, i.e., the system's ability "of being sufficiently independent in controlling its own structural and behavioral properties" [12]. Autonomy involves intelligent CPS able to dynamically change their behavior. This property has an impact in satisfying safety-related requirements. These, in turn, play a crucial and leading role in critical CPS, where the design and the implementation must comply to strict safety norms.

This work addresses educational features tailored to safety-related issues in the design of critical CPS (Section 2). We build on a feasibility study [8] in a railway system and on pre-existing scientific results [7, 22, 15]. To improve the design of critical CPS, we adopt Contract-Based Design (CBD) [7, 22]. Several European projects highlight the added-value of contracts to address non-functional properties during the system design [2, 25, 10] and, more recently, to address modular certification and safety-related issues [21, 28]. Complex systems require collaborative engineering between teams having diverse backgrounds and different fields of expertise, and necessitate clearly defined interfaces between the different disciplines [15, 5]. Contracts are a means to structure such communications.

Although there still is not a recognized standard to specify contracts and their use, contracts are recently being introduced in the AUTOSAR standard [3, 13] and in the Polarsys project [17, 9]. These tools are mostly integrated into design environments targeting 2D modeling spaces, while others target simulation [18, 14]. In this paper we show that combining CBD with 3D modeling and design tools is valuable both in educational terms and in the ability of the designer to visualize and verify the behavior of the system (Section 3). Section 4 provides our feedback on the educational aspects and highlights some characteristics which are required to the new generation of students to address the design of a (critical) CPS.

2. EDUCATIONAL CONTRIBUTION

This work arises from a master internship on contract-based design for safety issues in cyber-physical systems (CPS) located at CEA LIST, a public French research institute specialized in digital systems design. The mission of CEA LIST is to achieve excellence in technological development on behalf of industrial partners. CEA LIST is strongly involved in industrial transfer and technological innovation based on high-level scientific results and, therefore, less involved in educational aspects, e.g., in teaching university courses. Nonetheless, education takes the form of mentoring students during their internships and thesis work, often involving hands-on experience on industrial case studies.

From a methodological viewpoint, the work is structured in three main phases with daily, weekly and monthly objectives. The first phase gathers the CBD literature, which gives the intern a better knowledge of the topic. The next phase concerns learning the tools and their usage. The last phase addresses the implementation and getting early industrial feedback. The writing of the master thesis started the first days of the internship and was carried on throughout these phases. This way, the student is able to more easily

WESE'15 October 04-09 2015, Amsterdam, Netherlands

ACM 978-1-4503-3897-4/15/10 . . . $15.00
http://dx.doi.org/10.1145/2832920.2832924

structure the related work and improve the writing along the internship.

Meetings were organized between the supervisor and the intern. The goals of the meetings were to learn the scientific method, to motivate the student and to facilitate the understanding of the topic, which requires a diverse knowledge and know-how. Meetings were carried out on a daily basis, because there was no introductory course to CBD that the intern could attend. Some working sessions addressed a presentation by the student of a scientific paper. The adopted methodology leaves some personal work on the 3D technical representation of the contracts to the student to acquire autonomy. Finally, support in the technical issues has been provided by the Blender open-source and open-community via the forum and social networks.

2.1 Internship and its Results

The master internship is 6 month long and requires technical competences in computer engineering. The main goal of the internship concerns a feasibility study in applying CBD to a 3D model of a CPS. The starting points were a realistic use case based on public resources to avoid copyright conflicts; the CBD theory, compliant to the main results in this area [22, 15, 7]; and the convergence between international European projects for the specification of a CBD plug-in for SysML [10], and the adoption of LTL (Linear Temporal Logic) to specify contracts in 3D models [9]. The results include two 2D models in SysML for the railway use case; the introduction of CBD in 2D and 3D models; updating the verification tool [19] to Python 3, the underlying language of the chosen 3D modeling tool [6]; and finally a comparison between 2D and 3D to model CPS.

The main goal of the supervisor is a feasibility study in the use of new and disruptive technology to deal with CPS, where physical aspects play a crucial role. To do so, the authors in previous work envisage the idea to combine CBD and 3D models to deal with CPS [8]. The main results are a positive industrial feedback that encourages us to provide "industrial" demos and understanding if the current CBD theory should be extended (and how) to fit 3D models.

3. TECHNICAL CONTRIBUTION

We address the Communication Based Train Control system (CBTC) [24] which is a distinctive example of CPS. The high level architecture of the CBTC system comprises the Automatic Train Protection (ATP) and the Automatic Train Operation (ATO) sub-systems. Both systems have on-board and wayside equipment, which encompass software and physical systems. We model this architecture using information extracted from [27, 23] which exploit the IEEE 1474 standard. We specify two models: the first is concerned with the static block principle of train movement while the second is based on the moving block principle, a more modern version of the CBTC functionality. The latter uses high-resolution train location determination and provides better rail capacity.

The CBTC high level architecture is modeled using SysML block diagrams. The used tool is Eclipse's Papyrus. Figure 1 shows the on-board equipment diagram of the ATP block. Its main functions are: safe operation of the signaling system, imposing speed limits on trains, maintaining safe operating distance between them and complying with safety and speed requirement [1]. We specify a domain specific language tailored to CBD. We implement it as a SysML profile to apply contracts over block diagrams. Figure 1 shows a contract with its assumption and guarantee deployed over the ATP on-board equipment.

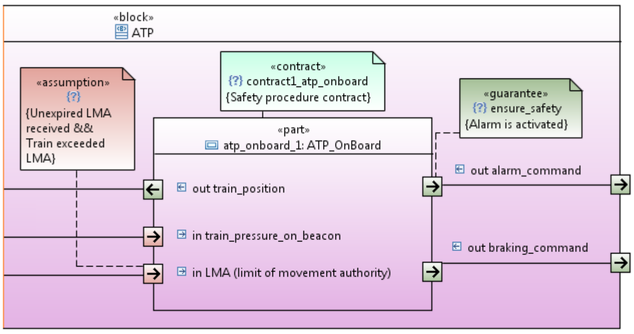

«block»
ATP
«assumption»
{?}
{Unexpired LMA received && Train exceeded LMA}
«contract»
{?} contract1_atp_onboard
{Safety procedure contract}
«guarantee»
{?} ensure_safety
{Alarm is activated}
«part»
atp_onboard_1: ATP_OnBoard
out train_position
in train_pressure_on_beacon
in LMA (limit of movement authority)
out alarm_command
out braking_command

Figure 1: ATP onboard equipment communication with contract representation using a SysML profile

In order to better visualize the behavior of the system and their respective impact on contracts, we aim at using 3D models as introduced in our previous work [8]. We expect that 3D representations can graphically simplify complicated concepts. Blender is a free and open source 3D modeling software [6]. We choose Blender as our modeling tool because it offers the flexibility we need to implement contracts in 3D models. Its internal libraries are written in Python and C++. The built-in Python console and text editor makes it simple to integrate scripts and customize the software at will.

We construct a 3D model of a train station of an automatic metro, where the platform and the train doors have to align and open synchronously (see Figure 2). We focus on two CBTC functionality: the *passenger exchange* function of the ATO and the *train speed supervision* of the ATP. We then define an animated scenario describing the train coming into the station, the automatic train doors and platform doors opening, passengers being exchanged, the same doors closing and finally the train departing from the station. This scenario, simple to describe, involves complex safety procedures that are not visible to the eye. Mixed criticality resides in, but is not limited to, the communication between ATP and ATO which holds different *safety integrity level* (SIL).

Using Blender, we implement an interface for temporal constraints verification in an animated 3D model (Figure 3). We proceed by first defining properties over the 3D model that express some of the system specifications (see Figure 3.A). Then, we construct temporal constraints using these defined properties (see Figure 3.B). The constraints are expressed in Linear Temporal Logic (LTL). We adopt LTL because it is widely used in contract based tools [9, 17] and the related literature. We expect that interfacing with such tools would be made easier in future work. For example, the following constraints expressed in natural language:

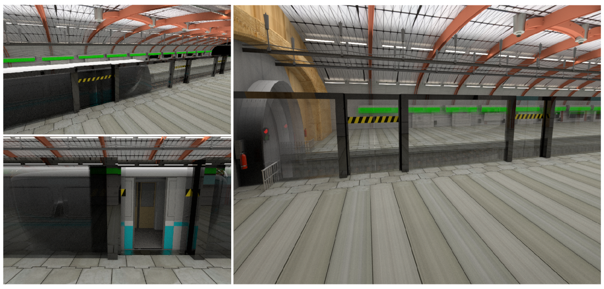
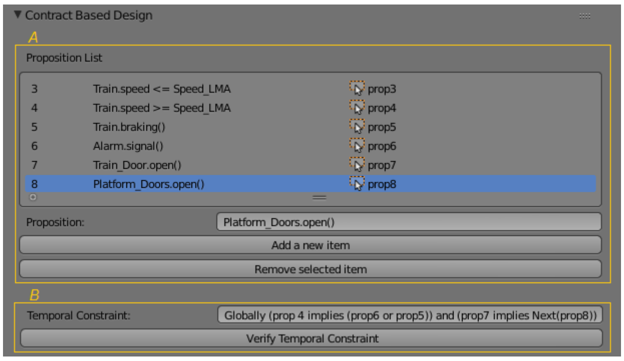


Figure 2: Constructed 3D model with a defined scenario



3	Train.speed <= Speed_LMA	prop3
4	Train.speed >= Speed_LMA	prop4
5	Train.braking()	prop5
6	Alarm.signal()	prop6
7	Train_Door.open()	prop7
8	Platform_Doors.open()	prop8

Proposition: Platform_Doors.open()

Temporal Constraint: Globally (prop 4 implies (prop6 or prop5)) and (prop7 implies Next(prop8))

Figure 3: Blender interface for property verification over a 3D model

- At all states, whenever the train speed exceeds the speed authorized by the Limit of Movement Authority (LMA), then train brakes or an alarm is activated
- At all states, if the Train Doors open then the Platform Door open in the following state

can be equivalently expressed using LTL and the system properties as

$$\begin{gathered}\Box(prop4 \rightarrow (prop6 \vee prop5)) \\ \Box(prop7 \rightarrow (\bigcirc prop8))\end{gathered} \tag{1}$$

where $\Box$ is the *Global* operator and $\bigcirc$ is the *Next* operator. This constraint is shown in Figure 3.B.

3.1 The verification process

In the animation field, a scenario is a set of *frames* together with *keys* which represent the set of values of all parameters involved within the model at a specific frame: objects location, physical (or logical) constraints, computation assignment to an object, value of a signal, and so on. We start from and update previous work [19] in temporal verification of animations. The verification of the temporal constraints is based on assigning states to *frames*. For example: $\Box\Phi$ is true if Φ is true in every frame. As a result, the notion of time is lifted to frames: we can choose which time unit to assign for each frame by manipulating the FPS (frames per second).

Using a similar GUI, we construct contracts over the model using the pre-defined temporal constraint(s). Then we establish links between the contracts and the dependent 3D *entities* (objects, constraints and others). Throughout the verification during the specified scenario, we check for any contract violation.

4. DISCUSSION AND CONCLUSION

This internship provides us an example of reasoning, modeling and implementing a critical CPS. It also constitutes a benchmark for discussions, analysis and to find new challenges to be solved. The work required a large spectrum of competences from the student, which are not necessarily learned during the university courses. For this reason, we strongly suggest coupling theory with the implementation and modeling of a real or, if not possible, a realistic CPS. This reinforces the view put forward in [4]: "laboratory exercises should provide the breadth and depth needed to build systems in practice, rather that reinforcing the theoretical concepts, introduced during the university courses". At the same time, after a first use of the 3D tool, the student became aware of the need to define a mathematical framework to advance in his development and knowledge. Hence, discussions, analysis and the use of mathematical frameworks were used in-depth during the second phase.

This work pursuits the feasibility study in [8] and is the first internship that studies these topics. Certain concepts and ideas cannot easily be represented in illustrations or 2D representations, and if they were, time and effort are needed to understand the complex representation. The student gave positive feedback on the use of 3D tools and CPS visualization, supporting the result carried out in other teaching courses [26]. Indeed, 3D representations can help the teacher transfer complex concepts of CPS design to the student.

During the internship we presented our work to industrial railway experts which responded positively to our approach. This positive feedback had a motivating impact on the student. It is important for the student who studies CPS to be in contact with both the scientific and industrial environment, because applying theoretical concepts to the real world often holds unexpected difficulties that can be overcome through advice from both industrial and scientific experts.

It is essential to note the general importance of open communities in supporting projects. In our case, the open source community of Blender benefited our work by accelerating the implementation process, through constant feedback from Blender experts. This cooperation was a key factor for the intern to accomplish his work within the given time. Since Blender is an open source software, the student had access to its internal libraries and functions, so that establishing a 3D representation for both CPS and CBD became less troublesome.

Mixed criticality is crucial in CPS [20, 11, 16]. It is important to show and discuss such issue with students because we believe that new challenges will arise and its up to the new generation to face them. Mixed criticality has been partially studied at the component level (ATO and ATP have different levels of severity - SIL) in order to better understand the railway CPS taken under consideration in the internship. The investigation in mixed criticality requires a large knowledge which equally encompasses 3D design, execution platform components, and safety norms. These latter could be not accessible to the intern.

The overall feedback on our work leads us to the following suggestion, which we promote as a conclusion: a teaching university course could consider the design and the development of a realistic CPS, the use of fragments of videos of real CPS (mostly accessible on YouTube) and the study of CPS by adopting different viewpoints (e.g., design methodologies and processes, safety, including mixed criticality, modular per-certification, mathematics frameworks). Among the main characteristics of the new generation of engineers, we point out staying updated on new emerging concepts joint with technical knowledge and scientific method. Finally, we suggest that the new generation of engineers should be able to root theory in facts and to always get the proper feedback from the facts.

5. ACKNOWLEDGMENTS

We thank Andreu Cabre for helping us throughout the 3D modeling and the Blender open-community.

6. REFERENCES

[1] Ansaldo-STS. Glossary. http://www.ansaldo-sts.com/en/glossary. Accessed: 2015-04-20.

[2] ASSERT FP6 Project. Automated proof-based System and Software Engineering for Real-Time systems project. http://www.assert-project.net.

[3] AUTOSAR. Automotive Open System Architecture. www.autosar.org.

[4] S. Behere and M. Törngren. Educating Embedded Systems Hackers: A practitioner's perspective. In *Proceedings of WESE workshop*, 2014.

[5] L. Benvenuti, A. Ferrari, L. Mangeruca, E. Mazzi, R. Passerone, and C. Sofronis. A contract-based formalism for the specification of heterogeneous systems. In *Proceedings of the Forum on Specification, Verification and Design Languages*, FDL08, pages 142–147, Stuttgart, Germany, September 23–25, 2008.

[6] Blender Foundation. Home of the blender project. Free and open 3D creation software. https://www.blender.org.

[7] D. Cancila, R. Passerone, T. Vardanega, and M. Panunzio. Toward correctness in the specification and handling of non-functional attributes of high-integrity real-time embedded systems. *IEEE Transactions on Industrial Informatics*, 6(2):181–194, May 2010.

[8] D. Cancila, E. Soubiran, and R. Passerone. Feasibility study in the use of contract-based approaches to deal with safety-related properties in CPS. *Ada User Journal*, 35(4):272–277, December 2014.

[9] A. Cimatti, M. Dorigatti, and S. Tonetta. Ocra: A tool for checking the refinement of temporal contracts. *ACM/IEEE 28th International Conference*, Nov 2013.

[10] CONCERTO Project. Guaranteed Component Assembly with Roud Trip Analysis for Energy High-integrity Multi-core Systems. http://www.concerto-project.org/.

[11] CONTREX FP7 Project. Design of embedded mixed-criticality CONTRol systems under consideration of EXtra-functional properties. http://www.assert-project.net.

[12] CyPhERS FP7 Project. CPS: State of the Art. http://www.cyphers.eu/sites/default/files/D5.1.pdf.

[13] W. Damm, H. Hungar, B. Josko, T. Peikenkamp, and I. Stierand. Using Contract-based Component Specifications for Virtual Integration Testing and Architecture Design. In *Proceedings of DATE conference*, pages 109–120, 2011.

[14] A. Davare, D. Densmore, L. Guo, R. Passerone, A. L. Sangiovanni-Vincentelli, A. Simalatsar, and Q. Zhu. METROII: A design environment for cyber-physical systems. *ACM Transactions on Embedded Computing Systems*, 12(1s):49:1–49:31, March 2013.

[15] P. Derler, E. A. Lee, M. Torngren, and S. Tripakis. Cyber-physical system design contracts. In *International Conference on Cyber-Physical Systems (ICCPS 2013*, Philadelphia , USA, 2013.

[16] DREAMS FP7 Project. Distributed REal-time Architecture for Mixed Criticality Systems. http://www.assert-project.net.

[17] Eclipse. Open Source Tools for Embedded Systems (PolarSys). https://www.polarsys.org/projects/polarsys.chess.

[18] L. Guo, Q. Zhu, P. Nuzzo, R. Passerone, A. L. Sangiovanni-Vincentelli, and E. A. Lee. Metronomy: a function-architecture co-simulation framework for timing verification of cyber-physical systems. In *Proceedings of the International Conference on Hardware/Software Codesign and System Synthesis*, CODES14, New Delhi, India, October 12–17, 2014.

[19] Hamed Zaghaghi. Animation Temporal Verification. http://www.foro3d.com/f230/animation-temporal-verification-77370.html.

[20] PROXIMA FP7 Project. Probabilistic real-time control of mixed-criticality multicore and manycore systems. http://www.proxima-project.eu/.

[21] SAFECER Project. Safety Certification of Software-Intensive Systems with Reusable Components. http://www.safecer.eu/.

[22] A. Sangiovanni-Vincentelli, W. Damm, and R. Passerone. Taming Dr. Frankenstein: Contract-based design for cyber-physical systems. *European Journal of Control*, 18(3):217–238, 2012.

[23] Siemens. How does a driverless metro system work? April 2012. FactSheet.

[24] Siemens. Trainguard Sirius CBTC. 2013.

[25] SPEEDS FP6 Project. SPEculative and Exploratory Design in Systems Engineering. http://www.speeds.eu.com/.

[26] W. Taha, R. Cartwright, R. Philippsen, and Y. Zeng. Experiences with A First Course on Cyber-Physical Systems. In *Proceedings of WESE workshop*, 2013.

[27] R. Technical. Automatic train operation. http://www.railway-technical.com/sigtxt4.shtml\#ATO-ATP-Multi-Home-Signalling, December 2014. Accessed: 2015-04-25.

[28] The GSN Working Group Online. Goal Structuring Notation (GSN). http://www.goalstructuringnotation.info/.