M. I. Rezabal, L. E. Elorza and X. E. Letona, "Reuse in Safety Critical Systems: Educational Use Case," 2013 39th Euromicro Conference on Software Engineering and Advanced Applications, 2013, pp. 402-407.

DOI: https://doi.org/10.1109/SEAA.2013.33

Reuse in Safety Critical Systems: Educational Use Case

Miren Illarramendi Rezabal, Leire Etxeberria Elorza, Xabier Elkorobarrutia Letona
Embedded Systems Research Group
Mondragon Goi Eskola Politeknikoa (MGEP)
Arrasate-Mondragon, Spain
{millarramendi, xelkorobarrutia, letxeberria}@mondragon.edu

***Abstract*— The last decades, the electromechanical control systems are being replaced by Programmable Electronic Control Systems. The challenge is that these new systems have to be at least as safe as the replaced ones. Any company that want to compete in the Safety Embedded Systems related market and have success in business, have to develop competent systems reducing the time to market and the cost of the development and certification. The reusability of SW components is one of the solutions in this way. It is clear that the industry needs new graduates with this knowledge. In this paper we are going to explain a use case that the University of Mondragon is developing in order to use it in the Master of Embedded Systems with the objective to transfer the knowledge about how to develop Safety Critical and Certifiable Systems in an efficient way.**

Keywords— Reusability SW, Safety Integrity Level, Certification of Safety Embedded Systems

I. Introduction

The University of Mondragon is a small and private university. It is a peculiar university because it is a cooperative university. Another peculiar or distinct aspect of this university is the use of active methodologies in the courses.

The University of Mondragon has several Master's degrees. One of them is the Embedded Systems Master. The main objective of this master is to form professionals able to innovate, design, develop, assess and maintain products that are based on embedded systems assuring their required safety level during all their life cycle.

The Embedded Systems Master offers a specialization on recent technologies such as:

- New paradigms of design, development and programming of embedded systems
- Emergent communication protocols
- Specialized network sensors
- High Performance Processing
- Design / development of advanced hardware systems

In the master, there are some courses that address the safety and security related standards. We consider that this aspect is very important taking into account the current market needs.

This specialization is complemented with a practical work that the students have to make in projects. These projects are real projects and the students have to do their planning and to manage the people.

As mentioned earlier, the Master is very practical. The students take their competencies in the area of embedded systems using active methodologies and each student have to take the initiative in his/her studies and decide in which aspects they want to specialize more. There are some theoretical classes (basic concepts) and then the students have to make practical exercise or real projects.

Some industrial companies (eTic, Ikerlan, Orona, Traintic, Ulma Embedded Solutions…) are also participating in the master giving some modules and/or defining real projects.

As mentioned above, we are using active methodologies and there are different reasons for it:

- to transform the studies and the educational project of the university to the new needs of the society
- take into account the European Space of Higher Education

The new educational model of the University of Mondragon is focused in the acquisition of the competencies that have to be evidenced by the learning results, the global and continuous evaluation of the learned topics, the alternating work-studies and the internationalization and the use of the active methodologies.

The teachers that designed the Embedded Systems Master of the University of Mondragon, detected that the related market needs specialized professionals on Safety Critical Embedded Systems and as consequence in the master there are some courses focused on the safety related development techniques

Part of this research was funded by the ARTEMIS Joint Undertaking, Grant Agreement number 269265 and 295373.

and standards. The educational use case that is developing the Embedded Systems research group is very interesting in order to help on the acquisition of this knowledge to the students. The theoretical part of this type of systems (standards, methods…) will be important, but we think that having the practical aspect is more important. In this way, the students will have real experiences and this type of active methodologies helps in the knowledge acquisition process.

The Embedded Systems group of the University of Mondragon is participating in different European projects. One of them is SafeCer (Safety Certification of software-intensive systems with reusable components). One of the use cases of this project is focused on the Education and Training aspects. The University of Mondragon is defining a use case for the project and the final objective is to define an appropriate use case in order to use it in the projects that the students have to elaborate in their Embedded Systems Master studies.

In the section II of the paper we will write about the objectives and the planning of the use case. In the section III we will explain some concepts and a tool framework related to SafeCer project. In section IV, we will define the use case and give some details of it. The last section will be the Conclusion's section and here we will explain what we expect to have as results once the use case is done.

II. Objectives and Planning of the Educational Use Case

The main technical objective of this Educational Use Case is to demonstrate that the reusability of SW components in Safety Critical Embedded Systems is possible and to demonstrate the benefits of the reusability (less cost). The use case has also some other transversal objectives.

In this way, the main transversal objective will be to transfer the knowledge of the technical objective to the students of the Embedded Systems Master. In this way, the students will learn new and innovative method, tools and processes to design, develop and certify Safety Critical Embedded Systems. In the future, these students will be in the industry and the European industrial net will be the final beneficiary.

Focusing in the technical aspect and the reusability, in this kind of systems the reusability will be used considering different point of views. The main idea is that if we have to reuse a component in a new system, the context of the new system will similar but not identical as the original one. The changes will come because of different reasons (different application domain, different complexity of the system, SIL 1level, variation on time, variation on space, different application model…). In the educational use case, we are going to consider two reasons:

- Cross domain: the regulation/standard that we have to use is different because the industrial domain has changed.

- SIL level: the new context has a different level of SIL (considering that the domain is the same and also the functionality, but the hazards have changed)

The educational use case will give us the opportunity to see how we can reuse the SW components taking into account the different changes in the context. For that, a use case is being defined and we will use there the inputs from different research projects. For this purpose, we mainly consider the recommendations provided by IEC 61508 [1] and we demonstrate the objectives of having a common reusable certification/qualification approach for the different domains – automotive, industrial and healthcare (Cross-domain component use and qualification for certification). So we will deploy SafeCer component methodology and tool framework in this case study, leading to a trainee example and E&T material and "cook book" for the SafeCer methodology and approach.

This is the planning of the Educational Use Case that we have defined in SafeCer and also this is the way that we are implementing the use case:

- Definition of requirements and assessment/evaluation criteria
- Specification of the E&T use case especially with respect to a training guideline, support material and training environment
- Implementation of the E&T use case especially with respect to a training guideline, support material and training environment
- Demonstration in practice (short university course or industrial seminar or technology transfer seminar)
- Evaluation and validation of the E&T use case (trainers and users)

At this moment we are in the two first steps of the planning: we are finishing with the definition of the requirements and the assessment criteria and starting with the specification of the use case.

III. SafeCer Process Model, Component Model and Tool Framework

The overall aim of the SafeCer project is to support efficient reuse of safety certification arguments and components prequalified according to a safety standard. The educational use case is based in some concepts that are being defined in SafeCer Project. Two concepts that are being considered in this use case are the Generic Process Model and the SafeCer Component Model.

The SafeCer project is developing several demonstrators and each of these demonstrators is a specific use case. This use

[1] Safety Integrity Level

cases are for different domains (railway, automotive, avionics…) and also the cross domain is considered. The Educational use case that we are presenting in this paper is one of them. In the first step of the project, all the partners defined the requirements for the different domains and for each specific use cases or demonstrators. The generic process model for integrated certification and development of systems built using component-based development (CBD) approach is based on the SafeCer requirements and needs and wishes of the SafeCer demonstrators; it also provides other tasks in the project with e.g. guidelines for specific development paradigms, specific safety standards and platforms of relevance to the industrial partners.

The overall objective around integrated certification and development process is to provide an overall picture of the development and certification of components and systems, in order to provide a basis for efficient development. This includes, reuse of safety arguments, design methods, and tools, as well as reusable certification for product-lines. Identification of a set of common generic activities and models for the different kinds of artifacts necessary for the certification are important requirements for this.

While developing the process and models we had the following objectives:

- The model allows mapping to a series of existing standards.
- The model is usable in Component Based Software Engineering (CBSE).
- The model provides means to perform efficient safety certification.

The process model is coupled to the individual domains in which the components are deployed. In the SafeCer project, a strong focus is placed on the automotive, aerospace and railway domains as well as cross-domain activities and the potential of deployment towards other (new) domains.

The other important concept of SafeCer project is the Component Model. The SafeCer component meta-model is based on the requirements defined in SafeCer. The role of the SafeCer component meta-model is to provide a common high-level unification of the various existing approaches to component-based development and architectural modeling in the considered domains. This common meta-model will act as a basis for the work on safety contracts and safety argumentation, allowing new principles and mechanisms to be formulated in general terms and later instantiated to the various concrete domain specific formalisms. The SafeCer component meta-model is defined in a stand-alone way and not as an extended version of other meta-model

One key feature of the SafeCer component meta-model is the separation of component modeling and system modeling. In order to facilitate the specification of reusable information, the primary focus is the modeling of component type, i.e. those aspects that are common to all occurrences of the component in various systems. These include the component interface, defining the means by which the component interacts with its surroundings, but also component contracts and argument fragments. A component contract represents an abstraction of a particular functional or nonfunctional aspect of the component (functional behavior, resource usage, fault propagation, etc.), often represented in the form of assumptions that the component makes about its surroundings and characteristics that are guaranteed whenever these requirements are fulfilled. Each contract can also have argument fragments, which are structured representations of different evidence that the contract is valid as well as the reasoning why these pieces of evidence together provide the desired level of confidence in the contract.

When these reusable component types are used in the construction of a system, they are referred to as component instances. These instances inherit the contracts and argument fragments from their respective type, but the particular context of an instance can be used to refine the contracts before they are used in analysis and system safety argumentation.

As described on [7], the Certification Tool Framework (CTF) is a framework collecting all the SafeCer consortium partners' tools producing evidence within the process of certification. Each tool, able to produce or manage artifact and needed to provide certification evidence, will return one or more artifact as output. Some of these tools are going to be used in this educational use case.

WEFACT is a tool developed by AIT (Austrian Institute of Technology) and it is one of the CTF's tools that is going to be used in the use case in order to use the General Process Model defined in the SafeCer ARTEMIS project.

As defined in [6], the Workflow Engine for Analysis, Certification and Testing (WEFACT; formerly called "Generic Test Bench", developed in the project DECOS) has the goal to facilitate validation, verification and certification of DECOS-based systems in a modular (component based) manner, making use of properties of the DECOS architecture elements (e.g. core services, high-level services). WEFACT consists of two parts, the Test Bench framework which provides a flexible infrastructure for defining and executing the V&V process and the external resources–external processes, tools and standards – which are integrated into the Test Bench framework by well-defined interfaces. Additionally, an extensive on-line user guide ("help file") including the DECOS v-plan cook book ("How to develop a v-plan") is available. This tool is one of the tools that are being extended in the SafeCer project taking into account the SafeCer Generic Process Model and the properties of the SafeCer System's.

Other tool that will be used in this use case is the extended version of CHESS tool developed in the SafeCer project. The main functionality of this tool is:

- Component based modeling environment with dependability analysis, real time analysis and code generation support

The CHESS Development Environment belongs to the following categories:

- Requirements management: modeling of requirements
- It is possible to model the following:
    - Software, by using dedicated component based approach,
    - Hardware platform,
    - Software to hardware deployment,
    - Functional and extra functional (i.e. dependability, predictability) concerns.
- Software development: automatic code generation for functional and real time concerns starting from modeled software (ADA, C++, and Java).
- Verifications available starting from the modeled software and hardware
- Traceability management: requirements traceability

The extended version of the tool uses the Component Model defined in the SafeCer project. In the use case, all the modeling and the development of the use case will be done using this tool.

The design and development of the control system will be based on contracts. In order to assure that the system fix the contracts, a contract base modeling will be considered in both versions of the use case and a tool called NuSMV3/ OCRA will be used to demonstrate that the modeled system fits the contracts.

NuSMV3 is a verification tool for finite and infinite-state systems. The tool provides different functionalities for functional verification, requirements validation, and safety analysis. The validation and verification of OTHELLO contracts is development on top of NuSMV3, in particular in a package called OCRA (Othello Contract Refinement Analysis). The tool is able of reading an architecture description with a contract specification and checking that the contracts refinement is correct. The tool also allows specifying the architecture description with a simple component-based textual language containing the essential modeling elements, the component input/output event and data ports, the interconnections among the sub-components, and the contracts specification. The tool allows specifying the contracts in the Othello specification language. Finally, the tool shall verify that the contracts of the sub-components of a component refine the contract of the component itself.

There is also a tool called CHESS2OCRA that translates the model of the system defined on CHESS to the OCRA tool (contract based modeling). So in the use case, first the system is modeled using CHESS and there will be translated from CHESS to OCRA using the CHESS2OCRA tool.

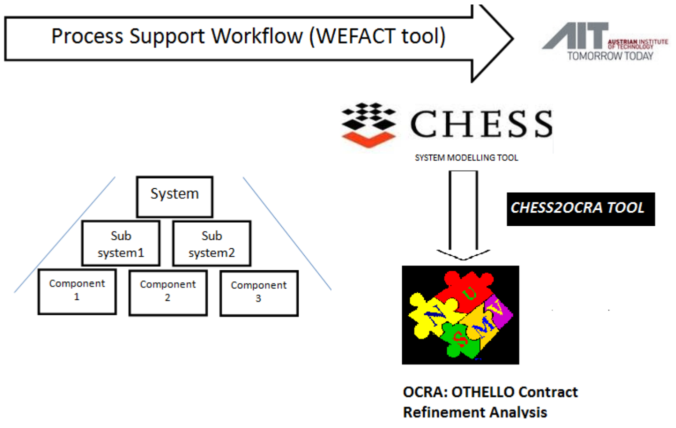
Process Support Workflow (WEFACT tool)
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY
CHESS
SYSTEM MODELLING TOOL
System
Sub system1
Sub system2
Component 1
Component 2
Component 3
CHESS2OCRA TOOL
OCRA: OTHELLO Contract Refinement Analysis

Fig. 1: Tools used in the educational use case

Using the defined Process Model, Component Model and these tools of the CTF of SafeCer, the educational use case will demonstrate the benefits of reusing components in Safety Critical Systems.

IV. Description of the Use Case

The Educational Use Case of the University of Mondragon in SafeCer project will be a generic use case that has to control from 2 to 4 distributed engines. The final application will be defined by the students and the minimum requirement will be that they have to control 4 distributed engines.

The use case will have different milestones and the first one will be to design and develop the use case taking into account the requirements of the application. One of the requirements of the system will be that the system has to be a Safety Critical System that they have to certify using the IEC 61508 [1] and the methods and tools defined in the SafeCer project.
Once they have developed the system, the external expert assessment group (teachers of the master) will assess their system and they will define a new context for the system.

In this new context, one of the two changing items will be different (domain or SIL level) and the students have to redevelop the system using the methods and tools of SafeCer. In this case, they have to demonstrate that using these methods and tools they will benefit of the reusability and that the costs of the second version is less than the original one or at least it is not as high as developing the system from scratch.

For doing this use case, some important concepts will be explained to the students. In some regulations/standards there are defined concepts like Proven in Use or Safety Element out Of Context. Also, there is a reusability related standard that they have to take into account: IEC/PAS 62814:2012 ed 1.0.

[2]. All these information and the different standards (IEC61508 [1], ISO26262 [8], CENELEC 50126 [5], CENELEC 50128 [4], CENELEC 50129 [3]) will be the basis of the use case.

As first milestone, the teachers of the University of Mondragon will design and develop the first example of this education use case in the SafeCer project and they will document all the guidelines. In this case, the application will be the automatic control of the roof of a sport stadium.

This automatic roof will be controlled by 4 distributed engines and the applied safety functional standard will be the IEC 61508 [1]. In this case, we will consider that a Hazard Analysis of the system is done (our research is not centered in this part) and taking into account the material of the roof and the HW that we are using the result of the SIL allocation for the Programmable Electronic System is SIL2.

Once we have developed this control system, in the second milestone, the teacher group of the University of Mondragon will have two choices for the second iteration:

- Change the SIL level of the system and redevelop the control system (SIL 4)
- Change the application of the control system and use it to control an automatic roof of a car.

At this moment we are working with the first choice and we have considered that the system have to be redeveloped based on the results of a new Hazard Analysis of the system. In this case, the material of the roof and the HW used in the system are not as safe as in the first one. The results of the Hazard Analysis and the SIL allocation for the new system say that the Programmable Electronic System that we have to develop for the second iteration will be SIL4. The reusability will be considered and as result we expect that the second development will be much more efficient because of using the tools and processes defined in SafeCer project. Once this option is done, the teacher group will consider also the second choice as future work.

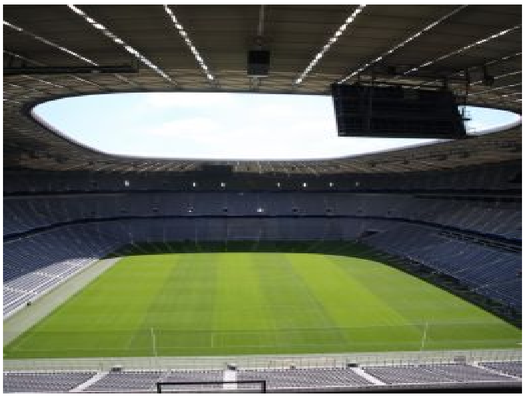

Fig. 2: Sport Stadium with automatic roof

After this demonstrator, the University of Mondragon will have elaborated a platform, framework and guidelines to use in the Master of Embedded Systems.

As mentioned earlier in this paper, the University of Mondragon uses active methodologies in its studies so the educational use case proposed in this paper and in SafeCer project fits very well in this methodology. Each student group will redefine the application that they want to develop but the basis will be always the same and they will do the research in an active way and doing the two iterations of the use case. In this way, they will research on reusability aspects on Safety Critical Embedded Systems and also they will learn the main aspects of the main regulations in Safety Functional Systems.

V. CONCLUSIONS

The main conclusions of this work will come after finishing the realization of the Educational Use Case. Here, we have presented the planning and how we are working in the Educational Use Case. Once the both planned steps are concluded, we will have the results of the use case documented and we will use all this information as guidelines in the Embedded System Master. The final result we hope to obtain it is a useful demonstrator based on reusability to develop Component based Safety Critical Systems which can be used in the Embedded Systems Master and in the other training courses.

At this point, the conclusions will be that using the active methodologies that use the university and the development of this use case will generate very well prepared new professionals in the area of Safety Critical Embedded Systems. They will have very good competences and knowledge in this area (standards and regulations, safety critical systems' development methods…) and also they will be able to minimize the efforts in new developments of this kind of systems taking into account the reusability.

As last conclusion, we also want to talk about the importance of the automation of the Certification Process. Having a tool framework that will help in the Certification Process is a very important point and the possibility that this framework gives to us when we want to reuse SW components gives us very powerful benefits. The process of Certification will be much more agile if we use this type of automated systems that helps us during the process. The result will be that the Certification Process will be reduced in time and costs and this is the final objective of the research project. We think that it will be a very important result to have an educational use case able to demonstrate the benefits of reusing and automation

ACKNOWLEDGMENT

The research leading to these results has received funding from the ARTEMIS JU under grant agreement n° 269265 and 295373 (pSafeCer and nSafeCer projects) and from National funding (Ministerio de industria, energía y turismo). The project has been developed by the embedded system group supported by the Department of Education, Universities and Research of the Basque Government.

References

[1] U. 61508, «Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad,» Marzo 2011.

[2] I. P. 62814, « Dependability of software products containing reusable components – Guidance for functionality and tests - Edition 1.0,» 2012.

[3] AENOR, UNE-EN 50129: Aplicaciones Ferroviarias. Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos relacionados con la seguridad pra la señalización, 2005.

[4] AENOR, UNE-EN 50128: Aplicaciones Ferroviarias. Sistemas de comunicación, señalización y procesamiento Software para sistemas de control y protección de ferrocarril, 2002.

[5] AENOR, UNE-EN 50126: Aplicaciones Ferroviarias: Especficación y demostración de la fiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS), 2005.

[6] S. Project, «D3.1.1: Survey of available tools,» 2011.

[7] pSafeCer, «D3.1.3: CTF Platform Prototype: Software Description Overview,» 2012.

[8] ISO, «ISO26262- Road vehicles- Functional Safety,» 2011.