DOI: https://doi.org/10.1109/SEAA.2014.40

Reuse in Safety Critical Systems: Educational Use Case First Experiences

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

***Abstract*—In order to maintain Europe as world leader in development of safety relevant systems one of the keys would be to join together the European industrial, academic and scientific communities. One of the main industrial challenges is that any company that wants to compete in the safety-related embedded systems 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. The technical aspects are worked out in the ARTEMIS nSafeCer project and industrial, academic and scientific communities are working together generating new methods and tools and applying them in use cases. One of the use cases of the project is an educational one and the University of Mondragon is developing it in order to use it in the Master of Embedded Systems Courses with the objective to transfer the knowledge about how to develop safety critical and certifiable systems in an efficient way.**

Keywords: Reusability of 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 the required safety level during all their life cycle.

The Master Course is very practical. The students take their competencies in the area of embedded systems using active methodologies and each student has 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 exercises or real projects.

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

In this way, the master course joins industrial and academic communities and the students have the option to contribute to the industry and also have the opportunity to work with real problems.

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 application in order to use it in the projects that the students have to elaborate in their Embedded Systems Master studies.

This educational use case 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,etc.) will be important, but having the practical aspect is also very important. In this way, the students will have real experiences and this type of active methodologies helps in the knowledge acquisition process.

The planning of this use case was explained in a previous publication [4] where the objectives and the related technical concepts and the tool framework of the SafeCer project were defined. The Educational Use case was also defined. In this paper, we are going to explain the usage of the use case in the master.

In section II of the paper objectives and the definition of the use case are presented. In section III we will explain the subjects/courses where the use case has been applied and their objectives. In section IV, the tool framework used in the use case is presented and in section V we will explain the results obtained in the use case. The last section will be the Conclusion's section and here we will conclude about the first

Part of this research was funded by the ARTEMIS Joint Undertaking, Grant Agreement number 269265 and 295373 (p+n) SafeCer.

year's results and explain what we expect to have as results in the future (once the use case is finished).

II. Objectives and definition of the Educational Use Case

The main technical objectives of this Educational Use Case are to demonstrate that the reusability of SW components in Safety Critical Embedded Systems is possible and also to demonstrate the benefits of reusability (less cost, safer, reduced time to market,etc.).

The use case has also another transversal and educational important objective. This objective is to transfer the knowledge of the technical objective to the students of the Embedded Systems Master. The students will learn new and innovative methods, tools and processes to design, develop and certify Safety Critical Embedded Systems. In the future, these students will work in industry and the European industrial net will be the final beneficiary.

In order to reach the technical and educational objectives a teacher group of the University of Mondragon have designed and developed the first example of this education use case in the SafeCer project and they are documenting all the guidelines. In this case, the application/example will be the automatic control of the roof of a sport stadium. This automatic roof will be controlled by 2 to 4 distributed engines and the applied safety functional standard will be the IEC 61508 [2].

As mentioned in [4], the use case is going to have two main milestones scheduled in the two years of the Master of Embedded Systems. For the first milestone, during the Master's first year, the students have to design and develop a system that controls an automatic roof with at least 2 distributed engines and the applied safety functional standard has to be the IEC 61508 [2].

In the second milestone (planned for the Master's second year), some safety requirements/contracts of the system the students have designed and developed in the first course will be changed. They will have to redesign and redevelop the system considering the reusability. The modifications of the system's requirements will entail one of the following changes:

- Change the SIL level of the system.
- Change the application of the control system and use it to control an automatic roof of a car (Cross Domain: a specific domain standard will be considered).

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.

In the first year experiment the students have defined a Process Model and they have used a tool to automatize the process. Furthermore they have defined the requirements and they have done a Hazard and Risk Analysis in order to analyze the context of the system and calculate the SIL level of the system.This work is related with one of the courses called Reliability and Performance Analysis.

After these steps they have defined the safety related Requirements and Contracts and they have started with the design of the system. They have used SysML as modeling language and a Contract Based Design approach have been followed. In this case, they have also used tools that help on that. The use of contracts is useful for verification purposes at early stages of the development (the design in this case). All this work has been done in another course called Life cycles of Embedded Systems.

Finally, the students have had to implement the model they have designed and test the system assuring that the real implementation fits with the contracts defined in the model level and also all the requirements defined initially. The third subject that participates on this experiment is Real Time Systems.

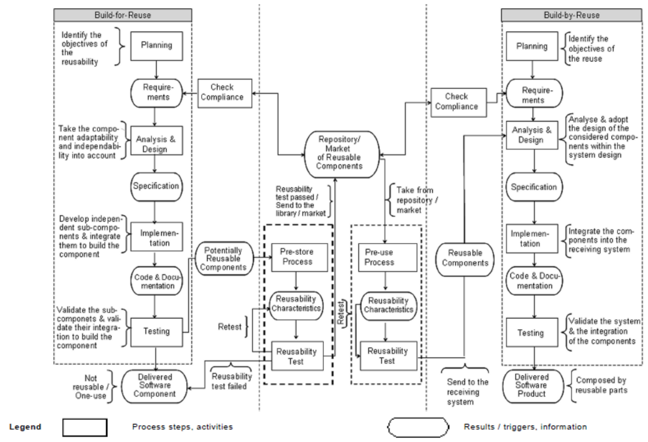
So, the first year experience has been focused on designing and developing a distributed engines control for an automatic roof but in one specific context and taking into account reusability concepts. A test suite has been generated, based on the contracts and requirements of the system and the idea is to repeat the experiment with the same students next year (2nd Year of the Master) but changing the context (change the requirements/contracts of the designed system) and checking the benefits of the reusability in Safety Critical Systems.

III. Objectives and Specifications of the Related Courses

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 on 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 Generic Process Model, is based on Component Based Development (CBD) and has to map a series of existing standards (automotive, aerospace, railway, generic) to provide an overall picture of the development and certification of components and systems for efficient development. The SafeCer Component Model, has to provide a common high-level unification of the various existing approaches to component-based development and architectural modeling in the considered domains .

The Generic Process Model has been studied in the subject called Reliability and Performance Analysis. In this subject, there is a theme related to the Safety Development Life-cycle. The objective of the theme is to learn the differences between a regular/standard SW life-cycle and the safety related one. The students analyze different life-cycles that are defined in different standards (IEC 61508 [2], ISO 26262[6], CENELEC 50126[1]) and the SafeCer Process Model [7] and they have to define a generic process that can be used in the most domains. This year, they have also learned the Activity Patterns concept. Activity Patterns represent dedicated activities that need to be performed as part of the development process. The students have defined the Activity Patterns they were going to use in the development of the automatic roof control system. They have also studied the IEC/PAS 68214 [3] and see the life cycle or the process model that this guideline defines taking into account the reusability and safety critical SW components. The IEC/PAS 68214 [3] proposes two development processes to develop this systems: For Reuse and By Reuse. All these aspects have been considered in the course.

This course also introduces Hazard and Risk Analysis techniques. The objective is to see which are the most used techniques and also to know how to calculate the SIL level of a system they have to develop. This year, they have done this exercise using as example the automatic roof control system and they have also define the safety requirement of the system.



Build-for-Reuse
Identify the objectives of the reusability
Planning
Require-ments
Check Compliance
Take the compo-nent adaptability and independabi-lity into account
Analysis & Design
Specification
Develop indepen-dent sub-compo-nents & integrate them to build the component
Implemen-tation
Code & Docu-mentation
Validate the sub-componets & vali-date their integra-tion to build the component
Testing
Not reusable / One-use
Delivered Software Component
Potentially Reusable Components
Retest
Reusability test failed
Repository/ Market of Reusable Components
Reusability test passed / Send to the library / market
Pre-store Process
Reusability Characteristics
Reusability Test
Retest
Take from repository / market
Pre-use Process
Reusability Characteristics
Reusability Test
Check Compliance
Reusable Components
Send to the receiving system
Build-by-Reuse
Planning
Identify the objectives of the reuse
Require-ments
Analysis & Design
Analyse & adopt the design of the considered compo-nents within the system design
Specification
Implemen-tation
Integrate the com-ponents into the receiving system
Code & Docu-mentation
Testing
Validate the system & the integration of the components
Delivered Software Product
Composed by reusable parts
Legend
Process steps, activities
Results / triggers, information

Fig. 1. Combining build-for-reuse and build-by-reuse from [3].

Regarding to the SafeCer Component Model, in the ”Life cycles of Embedded Systems” course of the first year of the Master of Embedded Systems the modeling of the system of the educational use case has been one of the assignments of the students. The students have designed the overall system and its components using the CHESS tool and the related Component Model.

In this course, model based system engineering methodologies are explained with special focus on requirement analysis and design of systems using SysML models.

The students have performed the design of the system using models for addressing several views:

- Structural modeling using Block Definition Diagrams (BDD), Internal Block Diagrams (IBD) and component interconnection (ports).

- Dynamic behavior modeling for describing the internal behavior of the components using state machines.

- External behavior modeling (communication and collaboration) for describing the possible interaction scenarios using sequence diagrams.

- Algorithm behavior modeling using activity diagrams for describing algorithms and functional aspects.

The Contract Based design concept has also been introduced in order to have the benefit of the reusability. The students have analyzed different authors’ studies about the Contract Based design [5], [10]. When reusable components 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. Although these benefits have not seen in this first iteration of the use case, next year we will have the results of having modeled the system using the contracts.

Finally, there is a third course that has been collaborating in the use case: Real Time Systems. In this course, the students have implemented the system taking into account the requirements and the design they have defined in the other courses. For doing this implementation, the students have used techniques and programming languages that are appropriate to the SIL level required by the system. For each of the phases or steps of the identified activity patterns, they have defined the tools and techniques to be used based on the Requirements and Hazard and Risk Analysis results and the generic safety standard IEC 61508 [2].

The final results has been two Lego cranes mock-ups that have distributed control of two engines . This physical system is used as a simulator of the automatic roof control system.

IV. Tool Framework Used in the Educational Use Case

As described in [8] and [9], 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 or have been used in this educational use case.

Workflow Engine For Analysis, Certification and Test (WEFACT) is a tool developed by AIT (Austrian Institute of Technology) and it is one of the tools that is going to be used in the use case in order to use the Generic Process Model. The tutors of the courses have used the tool and they have defined the requirements and contracts of the use case, the activities involved in the use case (based on the Activity Patterns) and the input and output artifacts of each of these activities.

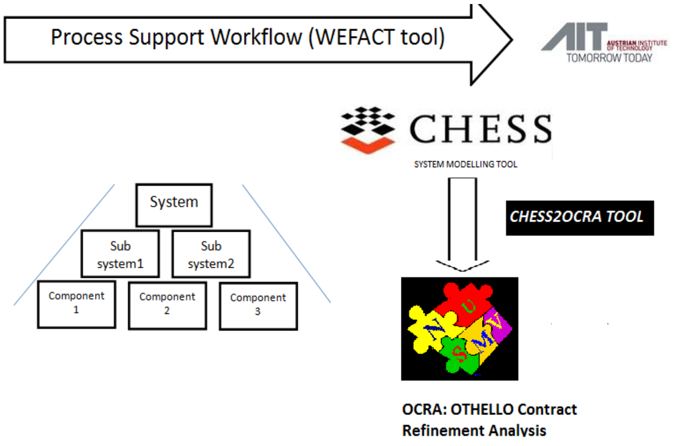


Fig. 2. Tools used in the educational use case.

Other tool that has been considered to be used in the educational use case is the extended version of Composition with Guarantees for High-integrity Embedded Software Components Assembly (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

In the use case, all the modeling and defining the contracts of the use case has been done using this tool. This tool has the option to define contracts for the system and it is possible to use a Contract Based Design approach.

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 then it is translated from CHESS to OCRA using the CHESS2OCRA tool.

As we explained earlier, the design of the control system has been based on contracts. In order to assure that the system fits the contracts, a contract base design has been applied and the tool called NuSMV3/OCRA has been used to verify the contracts. In this case, the students have had support and help for defining the contracts. The time they had to work on these concepts was not very long so they have had help. The final idea or objective was to see that this type of technology exists and how it helps on the development of the safety critical systems doing it more efficient.

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.

Using the defined Generic Process Model, Component Model and these tools of SafeCer, the educational use case will demonstrate the benefits of reusing components in Safety Critical Systems. In the second milestone, in the first phases or activities, the requirements and contracts will be redefined and a new Hazard and Risk Analysis of the new system will be done. Taking into account these results, the SW components that are affected by the changes will be identified and this components will be redesigned using the suitable techniques according to the SIL level and the industrial domain. Finally, the new system will be verified and it must meet the new contracts. During this process, there will be parts of the system that are not affected by the requirements' changes and they would be reused without any changes. So we can conclude that in this way the new development process will be more efficient because of the reusability. Next figure shows the relation of the Activity Patterns used in the use case and the tools to be used in each activity.

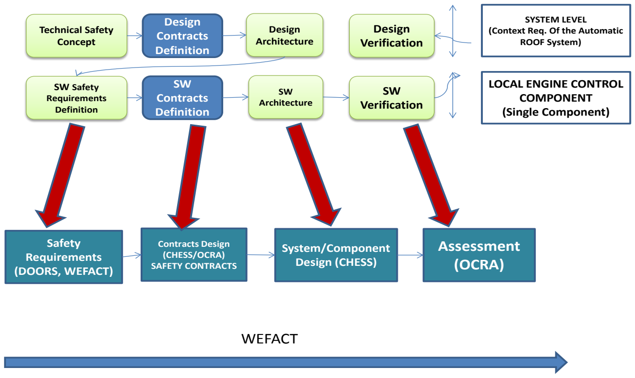
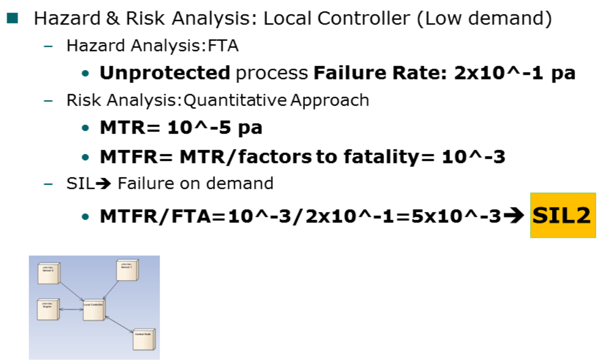

Technical Safety Concept
Design Contracts Definition
Design Architecture
Design Verification
SYSTEM LEVEL (Context Req. Of the Automatic ROOF System)
SW Safety Requirements Definition
SW Contracts Definition
SW Architecture
SW Verification
LOCAL ENGINE CONTROL COMPONENT (Single Component)
Safety Requirements (DOORS, WEFACT)
Contracts Design (CHESS/OCRA) SAFETY CONTRACTS
System/Component Design (CHESS)
Assessment (OCRA)
WEFACT

Fig. 3. Activities Patterns and related tools used in the educational use case.

V. First Experiences of the Educational Use Case

In this section we will see the results we have obtained in the different courses of the Master after doing the different practices we have defined in section III.

In the case of the Reliability and Performance Analysis course, the students have defined the safety requirements for the automatic roof control system and they have done a Hazard and Risk Analysis of the system reaching to the conclusion that in the context of a Sport Stadium, the Local Engine Controlling SW component has to be a SIL 2. In this case, the teacher gave the students some basic examples and then the students did the final analysis. In most cases the result has been that the Local Engine Controlling SW Component has to reach SIL2



- Hazard & Risk Analysis: Local Controller (Low demand)
  - Hazard Analysis:FTA
    - **Unprotected** process **Failure Rate: 2x10^-1 pa**
  - Risk Analysis:Quantitative Approach
    - **MTR= 10^-5 pa**
    - **MTFR= MTR/factors to fatality= 10^-3**
  - SIL➔ Failure on demand
    - **MTFR/FTA=10^-3/2x10^-1=5x10^-3➔ SIL2**

Fig. 4. Results obtained from the Hazard and Risk Analysis.

In the case of ”Life cycles of Embedded Systems”, the students have design and modeled the control system using the SysML language and they have defined contracts. In the next figure we can see some of the obtained results.

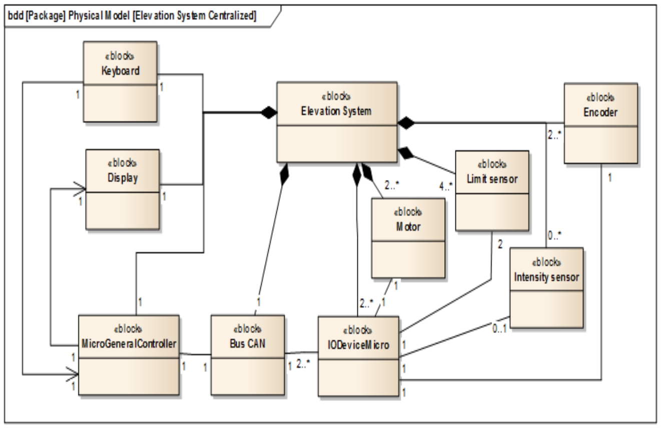


Fig. 5. Physical Model of System .

The students have done first the Structural Design and then they have defined the Dynamic and Behavioral Models of the System. The design has been done taking into account the results they obtained in the Reliability and Performance Analysis course. Using the CHESS tool, they have defined Safety Contracts for the system based on the Safety Requirements. Then, using the CHESS2OCRA tool the input file for OCRA was generated automatically and finally the students verified the defined contracts by the OCRA tool. The part of defining the contracts has been the most difficult but interesting one. The Contract Based Design has been a new concept for the students and the teacher have had to help them to finish their work. The interesting part is that the students have understood this new concept and the benefits that it would bring when the reuse of SW components is the objective.

The last part of the experiment has been done in the Real Time Systems course. In this case, the students have implemented the system using Lego based mock-ups. They have used two cranes (that can go up or down). The local control of the cranes has been done with a local micro-controller and there have been another micro-controller that acts as the one that synchronized the whole system. The development of the SW component that controls the local engine has been implemented taking into account the techniques defined in the safety standards for SIL2 and the models they have designed in the Life cycles of Embedded Systems course. Each group of students, has selected and reasoned why they have selected the techniques that they have used.

In the next figure, we can see one of the obtained results:

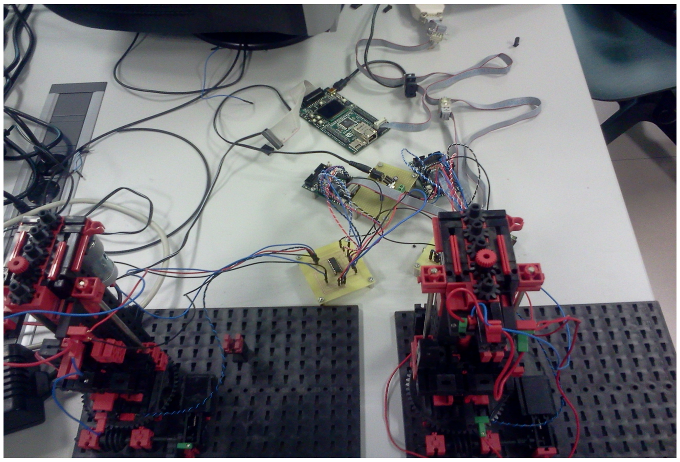


Fig. 6. Implementation of the use case in the laboratory .

VI. Conclusion

This first experiment has been done using the different concepts that we wanted to work in three different courses. The last objective is to design a common practice where the different concepts have to be integrated and define a more realistic scenario for the students. This scenario could be a real company department that has to develop the system.

Anyway, the obtained results are very satisfactory and this first experiment was necessary in order to see which aspects have to be prepared better or which ones require or not the teacher’s support.

Next step is to define and design the second year’s practice where having this first version done, a context change has to be defined and the students will have to design a similar system but using the benefits of the reusability. In this second experience, the work that they have to do in implementation will be less (they are going to reuse parts of the system), but it is very important to prepare a good practice to aim the objective of showing the benefits of the reusability and also showing that doing things in this way, using the SafeCer techniques and tools the development of the new reused system is much more efficient.

As is concluded in [4], the main conclusions of this work will come after finishing the realization of the Educational Use Case. Here, the results of the first step and the way the teacher group and the students are working in the Educational Use Case have been presented. Once the both planned steps are concluded, the results of the use case will be documented and the teacher group will use all this information as guidelines in the Embedded System Master. The desired final result of the Educational Use case 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 the active methodologies used in the master courses and the development of this practical 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, etc.) 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. It will be a very important result to have an educational use case able to demonstrate the benefits of reuse and automation of the certification/qualification process to train the next generation of engineers.

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, energa 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] CENELEC, "50126:1999, Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)," 1999.

[2] IEC, "61508:2010, Functional safety of electrical/electronic/programmable electronic safety related systems," 2010.

[3] IEC/PAS, "62814 Ed1.0:2012, Dependability of software products containing reusable components Guidance for functionality and tests," 2012.

[4] M. Illarramendi, L. Etxeberria and X. Elkorobarrutia, "Reuse in safety critical systems: Educational use case," in Workshop Session on Teaching, Education, and Training for Dependable Embedded and Cyber physical Systems [ERCIM/ARTEMIS/EUROMICRO], Santander, 2013, pp. 402-407. [

[5] Irfan Sljivo, Jan Carlson,Barbara Gallina and H. Hansson, "Fostering Reuse within Safety-critical Component-based Systems through Fine-grained Contracts," Icsr13, 2013.

[6] ISO, "ISO26262 Ed.1: 2012, Road vehicles- Functional Safety," 2012.

[7] Safecer, "A Generic Process Model for Integrated Certification and Development of Component-based Systems," 2013.

[8] SafeCer Project, "CTF platform prototype: Software description overview," Tech. Rep. D3.1.3, 2012.

[9] SafeCer Project, "Survey of available tools," SafeCer, Tech. Rep. D3.1.1, 2011. 2011.

[10] A. Sangiovanni-Vincentelli, W. Damm and R. Passerone, "Taming Dr. Frankenstein: Contract-based design for cyber-physical systems," Eur J Control, vol. 18, pp. 217-238, 2012.