Customizing the Methodology of Expanding RUP Software for Safety-Critical Systems

Mina Zaminkar
Faculty of Computer Engineering, Department of Software Enginering, Shahid Ashrafi Isfahani University
Ghaem Blv. Sepahanshahr, Isfahan, Iran, P. O. BOX 8179849999

***Abstract* — *Rational Unified Process is considered as an object oriented methodology. This methodology is a software development and production approach which is repetitious axial architecture and based on practicality. The RUP provide a process framework with the capability of customization in software engineering; frameworks for defining vast spectrum of different size, complexities and considerations projects. This concern provides the potential to produce software based on reduced risk and encounter main problems which leads to a reduction in cost and increase in potential success, hence an advantage. At this stage there does not exist any methodology to expand safe software from developing Safety-Critical systems based on objective orientation, axial architecture capable of gradual expansion and repetitious. Attempt is made in this article to apply RUP with respect to the safety rules printed in IEC 61508, in order to define and customize the necessities of Safety-Critical systems in Railway interlocking methodology is applied in controlling train movement in stations. This proposed RUP methodology a companied with the require Safety- Critical in developing the Railway interlocking system as a case study is assessed and the practical conditions are presented.*

Keywords — *Customization, IEC 61508 Standard, Safety-Critical, RUP, Object Oriented.*

I. Introduction

To develop the Safety-Critical system as well as the products thereof some of the standard and requirement, must be of concern in different phases and stages. The Safety-Critical require dependency and corpulent against the three fault, error and damage factors. To develop a potentiality in a system a specific design order should be followed as: engineering range, system engineering, protocol and network engineering, safety engineering, reliable engineering, immediate engineering, and systems engineering [1]. Of course, there exist another specific group of Safety-Critical systems named Safe failure that in case of damage in a section would respond in a manner that no harm or if any, the least, would be inflicted on other section. Designing software with safe-failure Feature has a significant affect in increasing the dependency system. Different software development techniques are discussed in order to develop Safety- Critical applications [2], [3], [4],[5], [6]. One of the main Safety-Critical development systems is the standard IEC 61508 package, standard and framework for developing the Safety-Sensitive software [7], [8]. This standard is an integrated approach to achieve efficiency in system with all its components based on foundation engineering that is the Waterfall methodology. This methodology includes obligations and prescription regarding safety for the initial steps and it does not cover the development activities in a complete manner. Few attempts are made in applying and customizing a software development methodology other than the Waterfall methodology in the realm of safety, since this realm often relates to the industrial outfits and therefore, it is confidential. On the other hand, the varieties of software development methodologies on software engineering are many [9].

Correlation between development and comparison is defined in this model. The Waterfall model has improved the testing and illustrates a more moderate approach [10]. The advantages and disadvantages of this model are described in full in [11]. One of the other credible studies run on safety is of the NASA [12], which is considered as an implementing work and it is not subject to any standard following a common methodology subject to customization. Due to lack of an appropriate software development methodology for the safety realm, developing such a methodology, for this purpose is essence. The RUP methodology is applied for any range and size of software systems [13].

II. Page The Safety Standards

Standards are agreed upon documentations which include technical description and other accurate information presented as definitions and guidelines in a sense that the product, process or the service would satisfy the predetermined objectives. Countries in an independent manner seek to develop their own production process standards to be implemented in software for administrative or military applications while in the same time the private sector does the same in different aspects of software engineering. Such standard, usually cover the whole product cycle beginning from the initial agreements between the client and the contractor and ending with the retirement of a product.

The NASA Safety standard [12], are concerned with personal identity, time, the reason for analysis of the software and how does its safety function operate. To prevent grade one hazards the emphasis of NASA is on hardware controls (of course together and in relation with the software controls). The hardware controls are well identified and have a better “record” in relation to that of the software controls. Nevertheless, software often is set at the front line of defence, supervise the unsafe circumstances and provide proper response thereof.

A. The IEC61508

The International Electronic Commission Standard with its safety title is a function of electronic and safety systems, describing one general approach for all safety and safety functional activities. This service includes samples of applications, software engineering implementation methods and a strategy in increasing confidence in abilities with respect to safety and Safety-Sensitive systems. By applying an applicable and instrumental interactive approach the IEC 61508 content is applied in product development. This contributes to the confidence in product safety and an increase in system confidence by reducing the detrimental occurrence.

This standard is observed in developing safety-sensitive software and is a framework for special range safety standard. This standard is an integrated approach in achieving safety efficiency evaluation of a system with all its components. The main objective of IEC 61508 Standard is to provide an integrated approach for safety performance life-cycle with logical and adoptive features in addition to facilitating product development. All factors related to product or the program are considered in full, hence, eliminating specific requirements on users, product and software parts. Moreover, this standard is able to develop systems regarding safety where there is product or interaction software parts.

In this standard the system safety protection is of E/E/PE^2 type with the requirements of hardware efficiency and system efficiency divisions in both the efficiencies. In a system for a potential level of determined safe efficiency the requirements of both the divisions must be observed. Safety integrity level (SIL) is based on the potential damage analysis of a system.

III. CUSTOMIZATION

A variety of methodologies and process are introduced in software development, each with determined principles and regulation fit for specific projects. After a methodology is selected, customizing it for the specific project is the next step through one of the limited instrument like Eclips Process Framework Composer (EPF).

By applying EPF, the product (process), function and the role in a software can be defined and their features inserted based on which the process (order) is defined as well. Moreover, guidelines, perceptions, examples and other issues can be added easily. Connection among the key components of the methodology where instruments contribute to its occurrence is illustrated in Fig. 1.

This instrument divides the whole concepts in constructing a methodology in two content and process model groups. In the content model all the necessary elements in constructing the process are present. To construct a methodology the roles, products, performed roles of every task, the obligatory and optional entries and the outcomes of every performance should be defined and determined. In the processing method it would suffice to place the desirable task and produce the appropriate process structure.

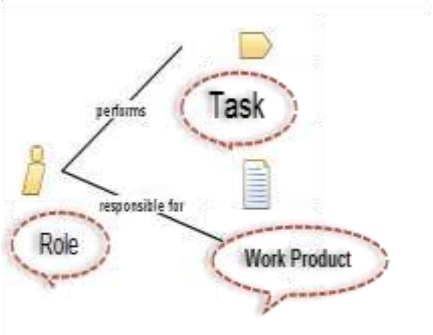

Fig. 1. Connection among the Key Components of the Methodology

A. Implementation of Methodology Based on Safety-standard

To implement the developed methodology based on Safety-Standard in the interlocking system the initial tasks are performed in describing this methodology for the interlocking system development team and the software team, in specific. To do so, first, the methodology cycle is designed in a schematic manner to allow the software development team become familiar with generalities Fig.2. This cycle is based on presented methodology, active in all the tasks and in all orders.

The project management, configuration and changes management, and knowledge management’s orders are added to this cycle based on the project requirements in order to increase the expansion team’s efficiency. This is not considered as a section of safety development standard.

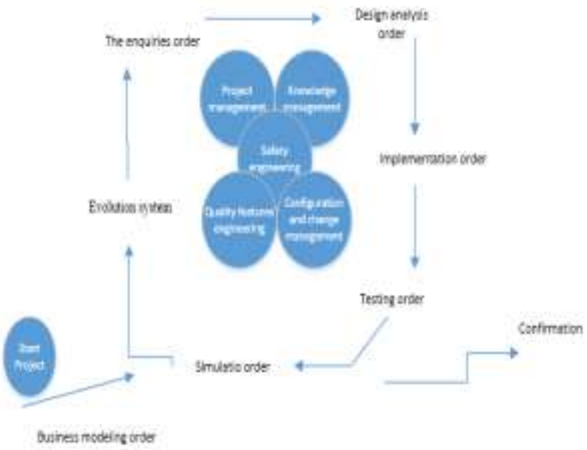

Fig. 2. Interlocking System development methodology cycle.

IV. Orders Defined

Definition of each one of the orders is expressed in the following subheadings:

A. Business Modelling Order

This order is based on the RUP Business modelling order. To identify the interlocking system features the project requirements must be identified and modelled. In this order a total of software engineering and business modelling techniques are applied in order to, first, facilitate connection among different groups of the project and next, make the script of the produced products in business modelling to the products of the software development project possible.

B. The Enquiries Order

This order in concerned with the interlocking system and the beneficiary enquiries. Through the interlocking system adopts a set of standards and regulations to perform its tasks which often affect the system function and are considered as the interlocking system requirements, the requirements should be modelled in a structured manner through appropriate modelling to establish strong foundation for the system development. All the mentioned steps and procedures above are tested to confirm their complete and comprehensive manners. Methods like formal and or patterning and form diagrams can be adopted for this modelling.

C. Design Analysis Order

The objective of this order is to convert the requirements to design features through comprehending them and selecting the best implementing strategy which in fact describes the subject system. A total of UML model, some evolved in an automatic manner through special instruments to reduce error, are adopted for this purpose. This design includes software and hardware applied in interlocking system. This design consists of different abstract layers among which conceptual, architectural detailed design layers are the most essential. In designing the renowned standard systems in this context and RAMS features architectural and design techniques and patterns are considered and applied.

D. Implementation Order

This order develops the project's software and hardware. The applied hardware in this design are capable of being implemented in laboratory engineering and industrial samples. The implemented simulating and marginal software are considered in this order as well. Production of different samples and their gradual increasing manner in integrating the system by applying the major standards in Railway applications is the objective here. To achieve the objectives of this order a set of milestone are considered on the path; passing each one of them would indicate that a sample of main interlocking system is achieved.

E. Testing Order

In this order the developed software and hardware are tested in reference to predetermined measures. These tests would determine the practically and would make the product ready for simulation and evaluation with respect to safety. Here a set of activities are involved in order to determine the test strategies, system required evaluations, conducting the test and error and problem analysis. In this order a set of milestones is of concern as well.

F. Simulation Order

Since the interlocking system has specific features which cannot be tested in real world it is necessary to adopt methods to simulate them as close to real world situation as possible in a safe manner. This can be accomplished by applying station simulation. The station simulation order is made and the application of the recorded results would improve the system function. The concept of milestone is adopted in this order as well.

G. Positioning Order

Implementing activities regarding interlocking system positioning in the Railway station is the objective of this order. This would assure the system ability in satisfying the requirements of users all beneficiations in the system. The final milestone here guarantees that the system actual ability based on adjustments made in this order and when installed in its proper place.

H. Configuration and change management order

This management protects the accuracy and wholeness of the project output, by determining configuration issues, limiting their changes, taking care of changes designated for those issues and define the configuration of the same. Methods, processes and instruments adopted and applied in this configuration system can be are of concern in this management. The importance of this order in interlocking project a set of different configuration activities and tracing changes are predicted in the system development.

I. Project Management Order

Software management is the art balancing the competitive objectives, risk management and overcoming the restrictions for the successful delivery of a product that would fulfill the client users requirements. The objectives of this management are: providing a project management framework, providing scientific guidance for designing, providing proper human resources, implementing and supervision the project and introducing a risk management framework which is essential in all projects.

J. Knowledge Management Order

This is an ongoing order with no restriction and it expands as projects are accomplished. Milestone is applied here and guarantees that the acquired Knowledge in this project is applicable in a complete and comprehensive manner.

K. Quality Features Engineering Order

Quality Features in software and hardware are essential especially in industrial projects is the main requirement in software and hardware design. In interlocking system the four main Quality Features are: safety, preservation ability, reliability and accessibility. Here, the last than Quality Features are of concern. Safety with all its importance is subject to another order. In principle Quality Features are considered in determining software and hardware requirements. In interlocking systems … Quality Features are considered as one order. The objective here is to establish strategies, tactics and pattern required in software, hardware sectors in addition to controlling and evaluating the products.

L. Safety Engineering Order

This is one of the most important orders in Railway interlocking system development safety system. Safety in projects is considered as a quality features and it is involved in system architecture. In Railway interlocking area this issue is of big concern, thus, in Railway interlocking system development it is dealt with in a specific manner.

The objective of this order is to establish safety strategies, tactics and patterns in hardware and software as well as correctness and evaluation of the products as far as safety is concerned. Different milestones are considered to secure safety at different levels and sections.

V. The Implementation Results Based On Safety Methodology

To implement the project the presented methodology a total of iterations which are defined by the related safety standards must be established. In each interaction a set of objectives assessed by the project management are determined. After the methodology is described for the project manager in a tracing institution, the manner of development system is applied based on the introduced method by the development team.

In every interaction the weak points of the methodology is gathered for re-inspection. Through the initial methodology provided to the interlocking development team has some weak points with respect to the connection among the activities on the methodology, in three different iterations the weak points are removed allowing the complete implementation of the methodology.

VI. Conclusions

In order to establish a customizing process it is necessary for every organization to develop a private process framework like (RUP). This framework is a version of the common process customized for to the specific capabilities of a given organization. The RUP methodology by integration, of the analysis and design phases assists the analyzer to announce the clear necessities of the system and convert it to a comprehensible language in code form. Since issue of safety is an important prerequisite in development the IEC 61508 standard is asses here. One of the main standards in Safety-Critical system is IEC61508 which provides a framework to develop safety-sensitive software, this standard is an integrated approach to achieve the applied safety in a system with all its elemental is founded based on the basic methodology engineering for software. Due to the safety features of this standard and all the activities involved all that is accepted from the concept of safety and a safety-sensitive are imbedded in this methodology.

References

[1] J. R. Pimentel, "*Designing safety-critical systems: A Convergence of Technologies,"* Kettering University, Flint, Michigan, 2008.

[2] E. G. Leaphart, et al, *"Survey of software failsafe techniques for safety-critical automotive applications*," in SAE World Congress, Detroit, 2005

[3] J. M. Sulek and M. R. Lind, "*Fail-safe methods for paratransit safety*," Journal of public transportation, 2005, vol. 8.

[4] BSI Group, "*Draft BS EN 50126-5 Railway applications*," The specification and Demonstration of Reliability, Availability,Maintainability and Safety (RAMS), 2013.

[5] G. Sugandba, "A Comparative study of Usability Evaluation Methods," *International Journal of Computer Trends and Technology (IJCTT)*, V22(3):103-106, 2015.

[6] Rizwan Ahmed, et al, "*Design of safety-critical systems using the complementarities of success and failure domains with a case study*," 2011.

[7] B. J. Krämer, N. Völker, "*A highly dependable computing architecture for safety-critical control applications*," Real-Time Systems, vol. 13, 1997.

[8] International Standard, "IEC 61508-3-1, 2ndedition, 2010.

[9] Rlewallen, "*Software Development Life Cycle Models*," 2005.

[10] Steve Easterbrook, "*Software Lifecycles*," University of Toronto Department of Computer Science, 2001.

[11] M. Zaminkar, M. R. Reshadinezhad, "*A Comparison between Two Software Engineering Process, RUP and Waterfall Models*," International Journal of Engineering Research and Technology, 2013.

[12] NASA-STD-8719.13A, NASA Software Safety Standard, 1997.

[13] P. Borges, et al, "*Mapping RUP Roles to Small Software Development Teams*," SWQD, 2012.