Using UML diagrams for system safety and security environment analysis

F. M. Rachel & P. S. Cugnasca
Safety Analysis Group, Department of Computer Engineering and Digital Systems, Polytechnic School, University of São Paulo, Brazil

Abstract

In this paper, the use of UML (Unified Modelling Language) diagrams as software tools for system safety and security environment analysis is proposed and evaluated.

The UML diagrams are used to plan and build systems based on the Object-Oriented approach. As these diagrams allow many system aspect viewpoints, they also allow a deep analysis and understanding of the system architecture and implementation details, as well as system functioning and operational features.

When a system safety/security environment analysis is accomplished, many aspects of system operation, functioning, data flow, data types, architecture and implementation details must be well known, understood and modelled in order to determine possible weak points for the system safety (or security, or both, depending on the system application). The various UML diagrams supply all the information needed for a safety/security system analysis and many aspects of the UML methodology can be applied for the same purpose.

Finally, a case study for an Object-Oriented ATO (Automatic Train Operation) control system proposed for use on a subway system is conducted in order to analyse the safety environment and to identify possible risks and danger situations to the system operation.

This control system proposed was presented and discussed in COMPRAIL 2004, in the paper called "Object-Oriented Approach for Automatic Train Operation Control Systems"; now this paper presents a complement of that study, using the drawn diagrams to make an analysis of the system safety environment.

Keywords: automatic train operation, control systems, train control, object-oriented project, object-oriented analysis, UML diagrams, safety-security analysis.

WIT Transactions on The Built Environment, Vol 88, © 2006 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR060321

1 Introduction

In 2003, a study was started in the Safety Analysis Group at the Polytechnic School of São Paulo University to make a viability analysis of the use of predictive fuzzy logic in an automatic train control for subway systems. In order to do this viability analysis, there were many aspects to be considered.

One aspect of this study was the use of the Object-Oriented (OO) approach, presented in Comprail 2004, in the paper called "Object Oriented Approach for Automatic Train Operation Control Systems". The main reason for choosing OO techniques was the viability analysis of using the OO approach for safety critical applications, such as subway transportation control systems [1].

In that study, a proposal for an object-oriented project was developed for an Automatic Train Operation (ATO) system. UML diagrams were used to specify all project dimensions – static, dynamic and method dimensions; all project phases were presented and detailed in the UML diagram forms [1].

Another study aspect considered was the use of predictive fuzzy logic itself. As this tool is an Artificial Intelligence (AI) tool, some considerations had to be taken into account in order to make the project comply with the IEC 1508 standard (Functional safety of electrical/electronics/programmable electronic safety-related systems), because subway transportation is a safety-critical system [2].

Some subway systems, such as those used in the Japanese city of Sendai and in the Brazilian city of São Paulo, were chosen as models for this proposed system design. The Sendai subway uses fuzzy logic and São Paulo subway uses track circuits to control train movement in a fast and safe way.

Another study aspect considered was the safety aspect. As a subway control system, it is fundamental that a risk analysis is conducted on this kind of system. Although the system has not yet been built and implemented, it is possible to make a preliminary risk analysis in order to detect weak points to be improved in the system final design [3].

Later in the study, some improvements took place based on the preliminary project; the study presented in this paper aims to show these improvements, incorporated to the project, and to point whether is possible to make a safety/security environment analysis based on UML diagrams that describe the system design and functioning by means of its project implementation characteristics.

The improvements and the adaptations needed to be updated and to make the system comply with the IEC standard lead to a system architecture rebuilding, showing that it is possible to make an ATO controller using AI tools, maintaining the system safety operating margins. However, some changes in the system architecture will take place in order to accomplish this task [2].

At the moment, this project is still not implemented in any subway system and there are some points to be analysed in future researches in this area, as the incorporation of other ATO functions to the project, such as program stop, doors opening/closing and data communication between the train and the station.

2 The updated object-oriented system proposed

In this section, the updates to the original project presented in Comprail 2004 will be shown. In that study, one possible solution was presented, among many others, and since its beginning, in the object point of view based on the UML, a well-defined and standardized methodology developed for object-oriented projects creation was used [1]. The UML uses several diagrams for all project dimensions: static, dynamic and method. For safety applications, one more dimension is added [4]. Figure 1 shows the safety/security aspect added to the other dimensions and the respective diagrams.

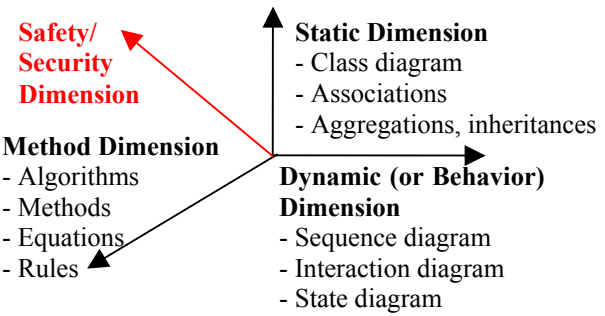

Figure 1: Safety/security dimension is added to static, dynamic and method project dimensions.

The system project and construction process have many phases, each focusing on a system aspect. The updated waterfall model including the improvements phase is shown in figure 2 [5].

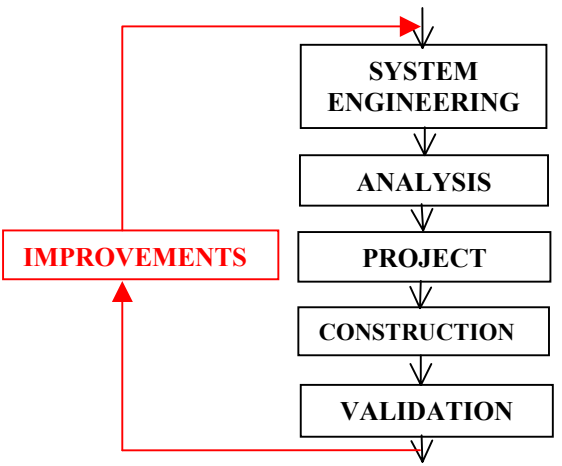

Figure 2: Waterfall model including improvements phase.

2.1 System engineering

When improvements are included in the original project, the project cycle reinitiates and, again, understanding the problem is essential to the project success. However, it is not necessary to begin from scratch, but to understand how the improvements affect the original project. In the original project, the system to be controlled was the Automatic Train Control (ATC), including two main functions - Automatic Train Operation (ATO) and Automatic Train Protection (ATP). This was not modified and figure 3 is only a reference for understanding the problem [1].

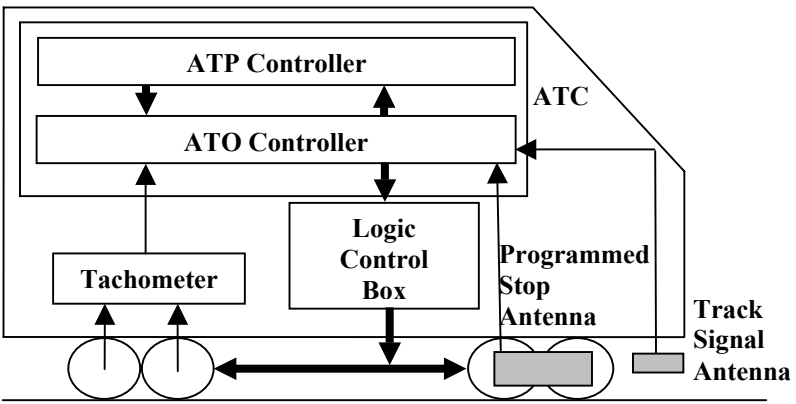

Figure 3: Schematic diagram of the ATC system [1].

The improvements to the original projects include an operational need for control system performance, according to certain operational situations. For example, the operational team has different needs for performance, according to operational demand on users. At peak times, the trains must run with shorter headways (time intervals between trains) and on valley demands the trains can run with larger headways, seeking energy consumption saving. This new problem was solved including a new entry called *Time or Performance Level* and it is related to the time interval used by the train for going from one station to another.

The updated IDEF (Integration Definition for Function) diagrams for this new configuration are shown in figures 4 and 5. As presented in Comprail 2004, they have a pattern graphical notation to represent the information flow and the processes used, in a hierarchical top-down architecture, in which processes can be expanded and detailed in hierarchical diagrams. The main process is represented in the IDEF0 top diagram called IDEF0 level 0 or context diagrams [6].

Again, the system engineering phase must detail the additional time and costs needed to implement the new solution [4].

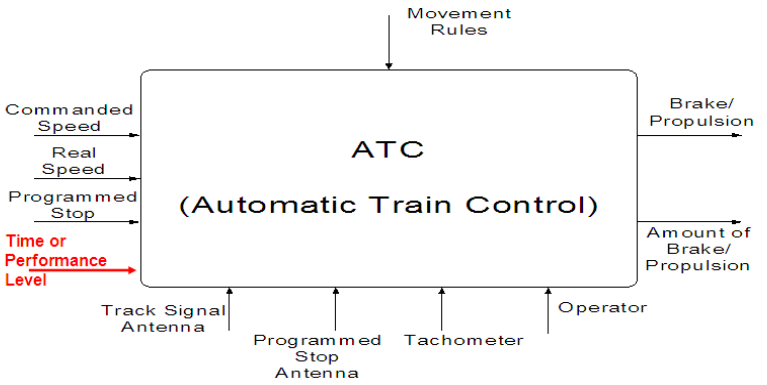

Figure 4: IDEF Level 0 (Context Diagram) including the new entry.

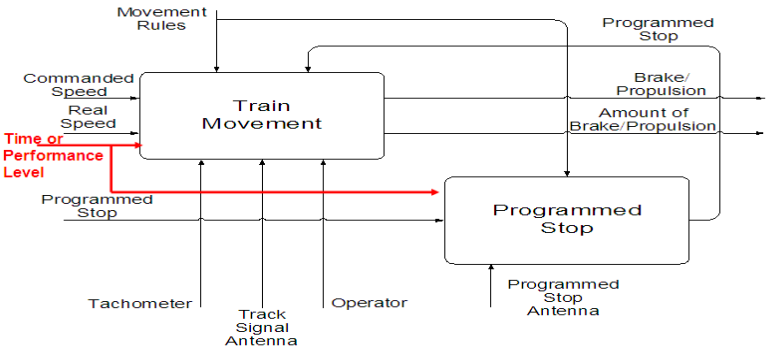

Figure 5: IDEF Level 1 including the new entry.

2.2 Analysis

At this point, besides the new solution implementation, the main objective of this paper is presented, that is, to verify whether the UML diagrams can be used to analyze the safety/security application environment. As will be shown, the answer to this question is *yes*. The static diagrams can be checked about wrong entries, out-of-range values or format errors, while dynamic diagrams can point the error consequences or predict how error scenarios can influence system behaviour. Unexpected answers shall be predicted and the system behaviour to these answers must be predicted and mapped in the diagrams.

Figure 6 shows the class diagram, including a new class (*Performance*) for new entry representation, while figure 7 shows the state diagram including an

unsafe state and figure 8 shows an example for sequence diagrams including the unsafe conditions scenarios not predicted in the previous project. Again, the analysis phase must produce a system prototype, replaced by a function simulation, in this case due to lack of screens or user interfaces [1, 7]

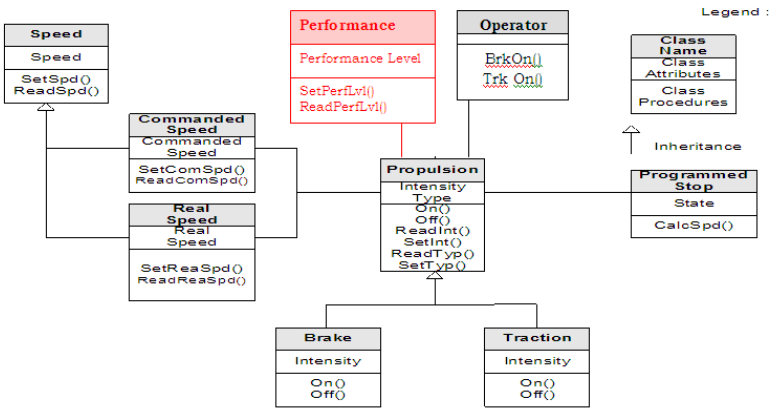

Figure 6: Class diagram including the new entry (*Performance*).

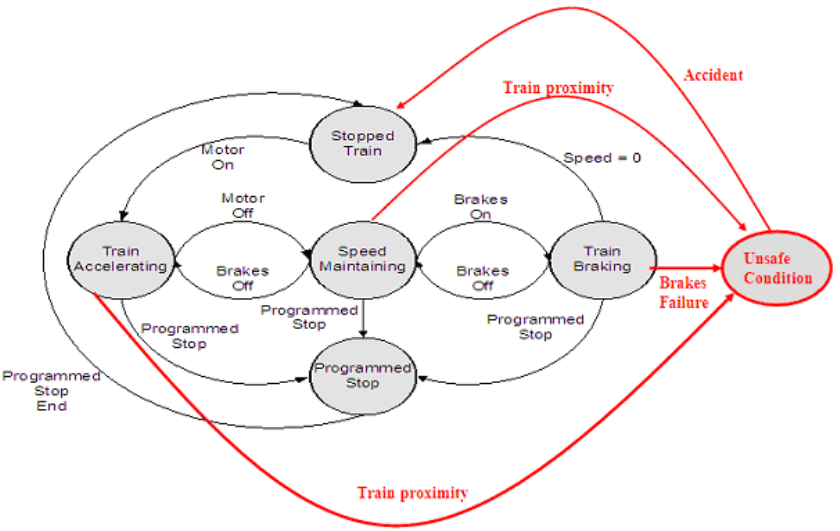

Figure 7: State diagram, including an unsafe state.

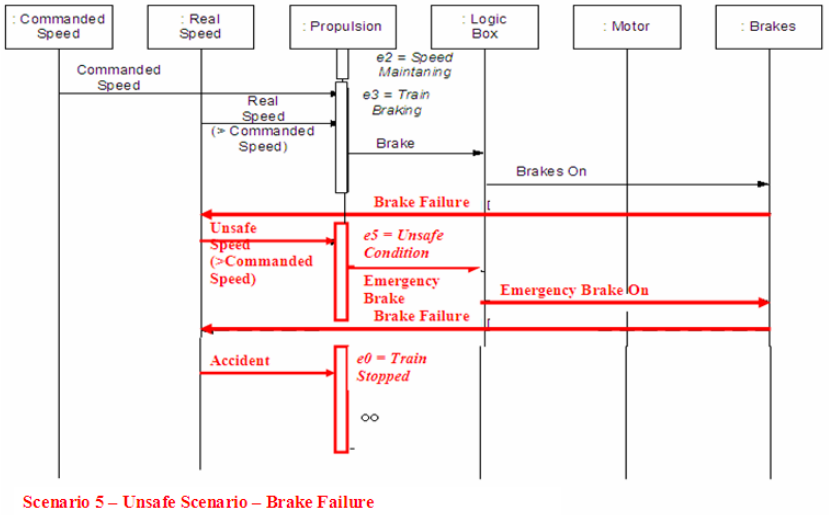

Figure 8: Example of a sequence diagram including an unsafe scenario.

2.3 Project, construction and validation

Again, after the whole system modelling, the next step is to put the plans into practice, implementing all the functions by means of hardware and/or software [4].

The component software diagram includes the new entry class that can be either handled as a separate component or grouped to operator class and compose a new component called external interface. In the project phase, all the modules and components must be technically specified and dimensioned [4, 7].

The following phases are construction and validation. In the construction phase, the software modules are coded in a specified programming language; in the validation phase, the system is tested and put into operation.

The use of UML diagrams and techniques made the improvements implementation much easier and consistent with the original project. This was possible due to object-oriented approach characteristics that are used in UML project techniques.

Is important to stress that, even if the UML diagrams can be used to identify potential risk scenarios and to map the dangerous and unsafe consequences to the system, they do not substitute the risk analysis that must be conducted on the real system implemented, because this analysis must include real situations in real system operational environment.

Therefore, if the UML diagrams used for system safety/security environment analysis do not substitute the traditional risk analysis method, why should they be conducted? The answer is that conducting UML risk analysis will increase the system understanding in terms of safety/security and this will avoid

surprises (generally unpleasant ones) concerning system operation related to safety aspects.

3 Conclusions

Along the study development, an operational need was detected: that was the system performance control, in order to adequate system performance to the user system demand. This need required a new entry, called performance level and represented the implementation of one adjustment (or control) in the overall system performance.

The choice for the object-oriented approach for developing the system project brought the main advantage to improvements implementation: the ease of project rebuilding. This new entry implementation task was enormously facilitated due to the design approach chosen. This approach feature is very useful for new improvement implementations. However, the relation between cost and benefits provided for new solution implementation must be taken into account in order to determine whether this implementation task is worthwhile [4, 7].

The risk analysis for the project developed led to some modifications in the system architecture initially proposed. For the project to comply with the IEC 1508 standard, which aims at functional safety of electrical, electronic and programmable electronic safety-related systems, the AI tools could not be used to control critical systems related to safety such as subway transportation systems. On the other hand, the use of predictive fuzzy logic showed to be a suitable solution for control systems applications [2, 3].

The solution was encountered by separating the functional tasks from the safety monitoring tasks and implementing these tasks in separate units, one for ATP functions and the other for ATO functions. The ATP unit must be in parallel with the ATO unit and its function must be restricted to the monitoring of ATO inputs and outputs, acting with priority over ATO decisions in case these inputs and outputs lead the system to an unsafe condition.

With this separation, the ATP unit must be implemented using the traditional safety redundancy techniques such as hardware and software redundancy, modules with voting system and multi-version programs. In the latter case, the ATO functions could be used as one version, whereas the ATP could make another version for the program. One voting mechanism could produce a final action.

The ATO unit, therefore, once monitored by the ATP unit, can execute the functional tasks of train control using any AI tool, without disagreeing the rules provided in the IEC 1508 standard [2].

Another conclusion is that, even if UML diagrams can be used efficiently for safety/security system environment analysis, they do not substitute the traditional risk analysis tools, fundamental for critical safety systems such as subway transportation systems and must be done in addition to these traditional tools. The UML analysis will support the traditional system risk analysis and will increase the system safety environment comprehension, avoiding unexpected systems behaviours related to safety aspects [3].

References

[1] Rachel, F.M., Cugnasca, P.S., *Object-oriented approach for automatic train operation control systems,* Computers on Railways IX Proceedings, Wit Press, 2004.
[2] IEC International Eletrotechnical Comission, *Functional safety of electrical, electronic and programmable electronic safety-related systems,* IEC 1508, 1997.
[3] Almeida Jr., J.R., Camargo Jr., J.B. and Cugnasca, P.S., *Risk Analysis of Railway Control Systems*, 8th International Heavy Haul Conference Proceedings, International Heavy Haul Association Inc., 2005.
[4] Pressman, R.S., *Engenharia de Software, A Análise Estruturada e Suas Extensões*, *Análise Orientada a Objeto* e *Modelagem de Dados and Projeto de Tempo Real,* Makron Books, 1995.
[5] Rumbaugh, J. et al., *Modelagem e Projeto Baseado em Objetos*, Ed. Campus, 1994.
[6] FIPS – Federal Information Processing Standards Publication (FIPS Std 183), *Integration Definition for Function Modelling (IDEF0),* 1993.
[7] De Champeaux, D., Lea, D. & Faure, P., *Object-Oriented System Development*, *Object Dynamics* and *Object Interaction,* Addison Wesley, 1993.