# Analysis of Cost and Benefit on Safety Critical Systems

**Jussara Pimenta Matos**
Department of Electrotechnical
Instituto Federal de São Paulo
São Paulo, SP
jussara.pimenta@ifsp.edu.br

## Abstract

Along with this analysis this paper presents the necessary parameters to put on data cost-benefit that all the procedures describes intent to establish technical directions when such events occurs on the matter. It is applied a systematic negotiation for conflicts resolution adopting guidelines and international standards. To achieve satisfactory reliability, availability, maintainability and safety requested, these factors must be considered in early stage of the system development. With the increasing the system complexity, there is a growing necessity for knowledge on the application of concepts regarding the most suitable architecture, in order to reduce costs and increased quality. Then, this work aims to give a direction to the stakeholders regarding the choice of appropriate alternative structure considering the application domain by establishing a rational. This analysis is developed based on estimation methods and cost evaluation, using industry design standards and mathematical models to represent the analyzed systems and it is applied on the real case.

***Keywords—Safety Critical Systems, Architecture System and Software, Railway Domain***

## I. Introduction

It is very acceptable to confirm the necessity to estimate costs and benefit, considering reduced resources, involved in complex system development is constant in organizations. To attend international standards, to achieve satisfactory levels of reliability, availability, maintainability and safety, these factors must be considered in early stage of the conception phase. Despite the evolution of languages for description [1], methods for analysis and evaluation [2], [3] and modeling using scenarios [4], [5], to design system architecture, from the knowledge of a given domain, including an assessment of non-functional requirements, considering possible conflicts between them, there are few systematized procedures that indicate how to resolve them [6], [7], [8], [9], conflict solutions, in various situations, run through the expertise of project participants, carried out in an *ad hoc* manner. Organizations are investing heavily in technology in order to stay competitive. For many of those organizations, improving project success rates is critical for their survival. The failure projects is of often linked to shortcomings in the conception phase, especially in requirements identification dealing with non-functional requirements (NFRs), because NFRs is viewed as a particularly difficult part of requirements engineering.

The industry has to be competitive and efficient in railroad domain developing standard and low-cost solutions. In addition to competitiveness some factors that can result in undesirable effects must be considered to ensure the safety of the system and to avoid the loss of human lives or major financial and material damage. The high-cost for development, implementation, operation and maintenance system, inhibits the growth of the metro-railroad network. This paper presents a set of fundamental requirements for critical security systems, seeking to systematize the decision-making process, as well as, to relate standards and good practices presented in systems development, including the market reality and limitations, both scientific and practical aspects, the definition of an architecture, which meets the expectations of interested parties regarding the cost of its development. The objective of this work is to present a negotiation approach for conflict resolution, in order to support the documentation of the rationale, which can be used in similar projects. For this purpose, the guidelines presented in [7] are used to support decision making at the beginning of the system design. Taking into account the international standards [10], [11], [12] applicable on the railway domain and a combination of the guidelines presented in [13] for the use of scenarios and in [14], [15] for the stakeholder participation in the project and regarding the cost and benefit assessment of an architecture. For the development of this work a real case is used, the on-board Automatic Train Control (ATC) subsystem included on Railway Signaling System.

Section II presents the concept of critical systems and the rules applicable to the railroad domain, in section III main characteristics the railroad application domain is presented and the Reliability, Availability, Maintenability, Safety (RAMS) concepts, in Section IV is presented a system for conflict resolution, combined with [13] and [14], with the necessary adaptations and the directives of [12], in order to identify an architecture that match on the limitations imposed by the domain and establish a better cost and benefit in the selection solution and Section V presents the conclusion and suggestions for future work.

## II. Standards Adopted for Critical Railway Systems

Safety critical systems is traditionally described when failures can result in loss of life, loss of considerable assets or destruction of the environment like aviation, rail transport, nuclear power plant systems, medical systems, military systems. The concept of a critical system is broad and its definition must take into account a specific system to which it refers. In the context of this work, they are systems that combine failures of hardware and software and the inability of a system to perform necessary functions, according to the specified performance attributes, it can result in risk of loss of life, destruction of property or the environment [16].

Development of electronic hardware components increased, it became possible to manufacture more reliable and more complex hardware components, on the other hand, more compact ones. As the complexity and reliability of hardware devices increased, it also enabled the development embedded software applications. However, software applications become less reliable as a result of the complexity of their implementation.

The safe failure concept exists since the beginning of the conception of railway systems, the use of components when in failure that result in a safe effect on the system, were essential to ensure safe operation at a time when programmable devices were not developed, not even computer techniques or software, to perform checks and vital functions. The safe failure concept is based on the use of components with known failure modes, failure modes that bring the system to a safe condition, or in other words, failures in these components do not lead the system to a more permissive condition than when there is no fault.

As a result of the growth in the use of integrated circuits and commercial microprocessors, a deterministic approach such as safe failure for complex systems becomes impractical, due to the exponential increase in the number of failure combinations. Modules with intrinsic characteristics of safe failure are currently used in railroads in parts of the system that are still dependent on hardware components, such as signal amplifiers and brake activation, in the case of the automatic train control subsystem. The adoption of standards is the result of good practices used by the industry.

The European Standards CENELEC (European Committee for Electrotechnical Standardization) for railways [10], [11] and [12] present a state of maturity for application in several projects by manufacturers in the main European countries, such as United Kingdom, France and Germany, with some variations in risk acceptance between these countries. These standards are applicable to both low density rail systems and mass transit systems such as the Metro. These standards represent the specific application of the series of international standards [16] for railway applications. They were created with the objective of developing compatible systems and allowing their use in different countries, adding measures of risk reduction factors adapted and specific to each one. region. The standard [10] defines a systematic management process based on the life cycle of the system to enable control over RAMS factors specific to this type of systems.

Safety integrity level (SIL) [12] is specified at four levels, where level four represents the highest and level one represents the lowest level, level zero represents the absence of safety requirements in the system, which are presented qualitatively in table I. Table II presents the relationship between SIL [12] and the safety objectives to be applied to each function performed by the system, to classify these functions and relate them to the level of safety integrity based on dangerous failure rates, in the design of a system. The values in table II are estimated based on a system operating in high demand mode, in which there is no independence between the protection and control subsystems, assuming that the maximum failure rate for an operator is 1 error per hour.

Table I. Safety Integrity Level (SIL)

| SIL | Description | | | | |
|---|---|---|---|---|---|
| 4 | Higher | Vital | Critical | Safe Critical | Safe Failure |
| 3 | High | Vital | Critical | Safe Critical | High Integrity |
| 2 | Medium | Semi Vital | Essential | Safe Envolved | Medium Integrity |
| 1 | Low | Semi Vital | Essential | Safe Envolved | Low Integrity |
| 0 | Absent | No Vital | No Essential | Not security related | Not security related |

Table II. Relation between SIL and Safe Objectives

| SIL | Operation Mode of High Demand |
|---|---|
| 4 | $<10^{-10}$ |
| 3 | $\geq 10^{-10}$ até $< 0{,}3x10^{-8}$ |
| 2 | $\geq 0{,}3x10^{-8}$ até $< 10^{-7}$ |
| 1 | $\geq 10^{-7}$ até $< 0{,}3x10^{-5}$ |

The common hardware security integrity analysis techniques are Markov models [18], [19], [20] and reliability of block diagrams [20]. In the case of complex programmable electronic systems, where there is cross-polling for reading channels and automatic tests are used, the reliability block diagram technique [21] has a loss of efficiency in relation to the Markov model technique [16], [ 22]. This loss in efficiency can be reduced when accurate reliability data is used. The block diagram reliability technique obtains more pessimistic results, that is, a higher probability of failure. The block diagram reliability technique [16] architecture analyzed:

- 1oo1: used on architecture of the type (1 out of 1), which consists of a single element and where any dangerous failure must be detectable for correct processing.
- 1oo2: used on architecture of the type (1 out of 2), which consists of two elements in parallel, both capable of commanding an output, where any dangerous failure must be detectable for correct processing.
- 2oo2: used on architecture of the type (2 out of 2), which consists of two elements in parallel, an output is commanded by the agreement between these elements, where any dangerous failure must be detectable for correct processing.
- 2oo3: used on architecture of the type (2 out of 3), which consists of three elements in parallel, an output is controlled by the vote between most of these elements and the state of an output is not changed if only one channel varies its state and any dangerous failure must be detectable for correct processing.

## III. Characteristics the Railway Application Domain

The railway domain involves many disciplines such as civil works, energy systems, rolling stock systems and signaling systems. This work is restricted to the signaling area, with the functions of supervision, control and protection of the operation of trains on a railway [24], [25], [26] and automatic train control subsystem. The quality of service in railways is directly influenced by the elements of Reliability, Availability, Maintainability and Safety (RAMS). RAMS is a characteristic measured by a long time of operation of a system and is achieved by the application of concepts, methods, tools and engineering techniques established throughout the life cycle of the system. RAMS is considered a qualitative and quantitative indicator that the system is reliable to perform the functions specified for it and to be available and secure. Therefore, it has an influence on the quality of service that is delivered to users of the system. However, quality of service is also influenced by features such as functionality and performance [23]. The following are the RAMS concepts for this domain according to [10].

a) Reliability: probability that an item can perform a required function under given conditions for a given time interval. In redundant configuration, it is assumed that a system is not repaired until a failure occurs, but can function while repairs are carried out.

$$\lambda = \frac{-dR(t)}{dt} \times \frac{1}{R(t)} \qquad (1)$$

- $\lambda$ is a unit of time-1 and means an instantaneous failure probability density. Expresses the density of probability of failure occurring at time t, which probability is conditioned to the failure of failures in the interval (0, t).
- R(t) is reliability system.
- In terms of failures/time.

Reliability system evaluation, non-redundant portions are identified and these are classified as basic blocks, based on these blocks to characterize redundancy schemes. These basic blocks can be processors, memories, communication channels. The reliability assessment relevant to this work occurs in the architectural design phase, where alternative redundancy mechanisms are defined. The quantitative assessment (estimation of MTBF indexes and availability) is carried out using generic data on the failure rates of modules in a system. The indices obtained in this phase are an indication of the orders of magnitude to be achieved by the system, considering:

- Series Arrangement: the equivalent reliability of the series arrangement is given below for constant failure rates:

$$Rs(t) = \prod_{i=1}^{n} e^{-\lambda_i t}$$

- Paralel Arrangement: the equivalent reliability of the parallel arrangement is given below considering that the failure rate of each block is constant, but the failure rate λp of the arrangement is not constant:

$$Rp(t) = 1 - \prod_{i=0}^{n} \left(1 - e^{-\lambda it}\right) \quad (3)$$

$$\lambda p(t) = \frac{-1}{Rp(t)} \times \frac{dRp(t)}{dt} \quad (4)$$

MTTF is the average time to failure, or the mathematical hope for the time of failure. In real systems the MTTF is an index, not a function and is then estimated by measurements and observations, deviations may occur. For a redundant system, MTTF is the average time for as many failures as possible to take the system out of operation. The use of this index is suitable for non-repairable equipment, where the occurrence of one or more failures causes the system to be out of operation.

$$MTTF = \int_{0}^{\infty} t.f(t)dt \quad (5)$$

- f(t) is the probability density of failure. It is the derivative of the probability that at least one failure has occurred in a time interval (0, t).
- Express em λ-1.

b) Availability: Ability of a product to be in such a state to perform a required function under given conditions at a given time interval. The interaction between MTBF and MTTR characterizes the relative running and stopping times for repairing a system and directly reflects the availability of the system. Availability representation over a period of time assuming constant failure and repair rates is given below:

$$A = \frac{MTBF}{MTBF + MTTR} \quad (6)$$

A conflict between security and availability quality characteristics can impact the reach of system dependability, since the achievement of availability system cannot compromise its security. The dependability system is achieved by meeting all the elements of RAMS, in addition to long-term control of the operation, maintenance and environment system activities. Safety and availability have an inversely proportional relationship, in which availability increases, the probability of an unsafe failure occurring. Availability has a relationship and is influenced by the attributes of reliability, maintainability and more the operation and maintenance activities over time [12].

c) Maintenability: Probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval. Maintainability is the probability that a system will be restored to an operational state in a period of time, given that system is in a non-operational state. Preventive maintenance is part of maintainability and causes a system to prevent degradation of parts, in addition to increasing the availability of that system.

An automatic train control system on board the train is considered non-repairable during operation however this same system can be repairable when the train is retracted to the yard for maintenance. MTTR (Mean Time to Repair) is the average time to repair and is expressed in μ-1. It means the average time for the effective implementation of the system repair. M is a unit of time-1 and means an instantaneous repair rate. MTBF (Mean Time Between Failures) is the average time between failures in a repairable equipment context, it is the sum of MTTF and MTTR.

d) Safety: The requirements analysis in a railway signaling system can be conducted in order to configure the link between availability and security, and thus, consider the importance of each one in case of conflict. For a railway system, security is opposed to availability, as the ideal is to expect that in the event of failure the train stops, that is, there is an inverse relationship between security and availability.

A system security evaluation involves the following aspects:

- All possible hazards system under all operating, maintenance and environmental conditions. These hazards are safety-related failure modes, the estimated (probabilistic) or observed result of the cause of a failure or a state in relation to operating conditions at the time of a failure.
- The severity degree of the hazard occurrence.
- The probability of each security-related occurring failure mode system.
- Sequences or events coincidences, failures, operational states, environmental conditions and others in an application that can cause an accident and the likelihood of each occurring.

The importance of software in safety-critical systems is emphasized, as it contains functions, which can be combined with other implementation techniques, to ensure adequate operational performance and maintain the specified levels of availability, without compromising compliance with security requirements. However, to ensure that a software meets the safety requirements of a critical system in the railway area, one must first ensure the commitment to meet the RAMS attributes.

## IV. Application Trading System Combined to ATAM and CBAM

An easy communication and the ability to make the best decision with all participants in a project, with different knowledge profiles are as important as the development of activities for their development. This ability is the key to elaborate a group of decisions, in group, as to the rationale to be used, considering the different objectives, criteria, preferences and issues in organization. Each individual in a group deals with a portion of the problem, which is part of the whole. One aspect is to manage the negotiation process in relation to the construction of the system. The other is to identify and resolve the conflicts generated, when different individuals are analyzing the system, from their point of view and their specialty.

Despite the evolution of methods for the definition and evaluation of an architecture, such as ATAM [13], in its evaluation logic the social aspects are not explicit, nor how the solutions are obtained. CBAM [14] uses ATAM scenarios, analyzes and supports decisions regarding software architecture alternatives, considering economic factors. Despite this, it is not clear how the alternatives explored are generated in order to meet the objectives, criteria, and how they satisfy the initial requirements presented by the project participants, who have different roles, responsibilities and priorities.

The negotiation system describes the project direction in the decision-making process and has the following steps:

- Identify the group of stakeholders: identification of whom, directly or indirectly, influences decision-making for building the system.
- Identify restrictions: factors that can restrict a particular solution, restrictions are generated, which includes both technical and organizational restrictions.
- Identify the operating modes of the system: check if there are different operating modes, including the definition of acceptable levels of degradation for operating the system.
- Propose a conceptual structure: initial structure domain is proposed, according to the experience of each participant in the group.
- Develop model perspective: all participants express their opinion for each concept regarding the conceptual structure.

Perspective analysis is an approach where a detailed analysis is carried out, observing the possible conflicts that may exist between the different views of each of the participants and consists of:

- Define strategies: the key application domain concepts, the existence and adoption of standards and norms are reviewed, and the predominant architectural style in similar projects is verified.
- Identify technology: the platform to be used or developed and the interfaces with other products and systems are identified.
- Generate and evaluate the arguments: the arguments that led to a particular solution or decision making are recorded. These records will serve as a basis for future projects, as they describe the rationale used in detail.
- Share results: the final result is shared with all participants.

The architecture definition which serves the implementation of the set of business rules is fundamental in enterprise success. Systematization ensures that the right questions are asked in the initial phases, where problems

and changes can be resolved more economically, guides those interested in the project to seek to identify conflicts regarding the requirements and resolution of these conflicts, throughout the development process.

Figure 1 shows the automatic train controller or ATC, which represents the train movement control and supervision functions. The ATC is installed on board trains or locomotives to ensure efficient and safe operation, being responsible for carrying out the functions of command and supervision of the movement of the trains, in order to guarantee the specified levels of safety and performance. It is typically configured as a 2 of 2 (2oo2) architecture arrangements [17]. An alternative to this configuration is the specific functions duplication, using redundancy, at the opposite end of the train, or even, the use of simple or triplicate architecture arrangements, to improve the availability or security subsystem.

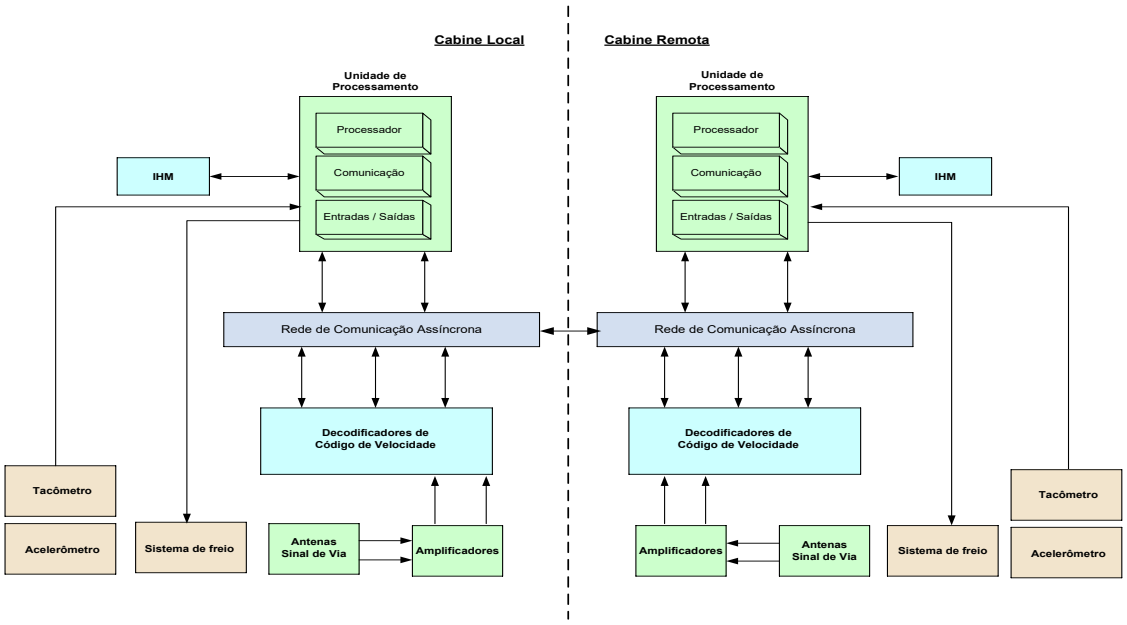


Fig. 1. Onboard Automatic Train Control Subsystem

The ATC general architecture subsystem is based on automatic train protection units, which are formed by processing modules that perform the same functions and perform comparisons of processing results, providing routines for programming the internal and external peripherals of the processor, in addition to to access the input and output interfaces. Critical entries are doubled or tripled to enable the software to perform consistency analysis of information. The vital outputs of each of the two processing units are triggered by the processing units, but voted for fail-safe circuits, which generate the outputs for a train's traction and brake subsystem in order to guarantee levels train safety integrity level (SIL). It has control and communication functions, the first is responsible for controlling the movement of the train and the second has the means for the ATC to communicate between its processing units and with the external units. The ATC receives the maximum permissible speed limits in each section, depending on the distances between trains, the layout and construction profiles of the track, the desired level of performance by sections and environmental factors.

The first stage of ATAM [13] is to understand the system quality attributes, to transform this analysis of quality attributes into scenarios, choosing the most appropriate and meaningful scenarios requires interaction between stakeholders, and in this way, helps to elicit and refine quality attributes. Stakeholders must be focused on scenarios that represent critical uses and must consider possible changes to the system. The second step is to validate the information from the first step. The elicitation and analysis steps are reviewed and summarized for the other stakeholders in the system. All stakeholders of the system are added to the analysis group, the typical participants recommended for this phase are the evaluation group, the people responsible for decision making on the project and architects of the system. The third stage takes place after the end of the evaluation and analysis work of the previous stages. The typical participants recommended for this phase are those in the project evaluation group and are responsible for preparing the final report on the application of the method and updating the artifacts produced. Final reports are prepared and delivered. The biggest gain in this phase is the self-assessment of the participating group and improvement of the method, assessment and documentation of the system.

CBAM [14] has a structured elicitation process with a probabilistic cost-benefit analysis combined with a decision analysis structure, the objective is to support the elicitation tasks and documentation of costs and benefits to allow interested parties a basis for taking of decisions. This decision-making is carried out through a decision-making process that takes into account the needs and risks of the system to be designed. The purpose of describing the business rules is to guide the participants' efforts. For the system in question, the following business rules and restrictions have been taken into account, as they are important to meet the needs of customers or to gain competitiveness in relation to competitors:

1. High system availability, or better, to increase system availability and reliability.
2. Maintain compatibility with products already installed on customers, without neglecting the development of new solutions.
3. Attend SIL 4 safety integrity level.
4. Decrease the developing the system cost.
5. Meet International Standards.

The utility tree [13] is a mechanism for directly and efficiently transforming business rules into scenarios. Based on the established business rules, the following assessment is made:

- The business rules listed as 1 and 2 are related, since improving the attribute of quality availability should be limited to maintaining compatibility with products already installed on customers. These two business rules are combined to generate the quality attribute tree.
- Business rule 3 means improving the quality of safety attribute, having to add testing, verification and validation activities to the process.
- Business rule 4 is a business rule that is addressed by the CBAM method.
- Business rule 5 must be associated with rule 2, as they are related and should not be conflicting.

Based on these business rules and RAMS, the attribute of quality availability is chosen for the construction of the utility tree. The other quality characteristics, such as safety, reliability, maintainability and functionality, and activities throughout the project such as operation, maintenance and system environment are taken into account for analysis, as a consequence of the application of the RAMS concept. After eliciting and clarifying the business rules, which are also the organization guidelines for the projects, the stakeholder involved selected scenarios through the utility tree. This activity is not an individual elicitation by the interested parties, but a consensus on the necessary changes. For this work, the following scenarios are proposed regarding the business rules for the automatic train controller:

- D1: Detect speed code signal failure and switch to a redundant channel.
- D2: Detect failure in the speed code decoding unit and switch to redundant decoder.
- D3: Detect processing unit failure and switch to redundant unit.
- D4: Detect failure in the IHC module and switch to redundant IHC.

The evaluation is based on the standard [17] regarding the reliability of the block diagrams 1oo1, 1oo2, 2oo2 and 2oo3. In order to carry out the analysis of architectural approaches, architectural decisions, sensitivity, tradeoffs and risks, the following calculations are considered:

- Failure rate according to the standard [28], based on the components of each CAT unit and module.
- Rate of dangerous failures, rate of coverage of diagnostics (DC) and rate of failures in common mode, according to the guidelines of the standard [17];
- Standard block diagram reliability techniques [17];
- Determination of the safety integrity level (SIL) standard [12].

For each scenario and ATA architecture decision, the points of sensitivity, tradeoff and risks related to the scenario are recorded, with the decisions of alternative architectures elicited by the interested parties. The quantification of quality attributes, considering the analysis has the following considerations:

- Failure rates and MTBF measured according to the standard [19].
- Eight hour MTTR.
- Diagnostic coverage rate from 0 to 99%.
- Common mode failure rate between redundant channels from 1 to 10%.

The scenario utilization is based on the importance of each one with respect to the anticipated response values. CBAM [14] uses scenarios set, which are variations in the response values of the same scenarios elicited by ATAM [13], however the different response values for each quality attribute that allow the construction of utility response curves. To determine the utility response curves, levels are chosen between the worst case and the best case for each quality attribute. For each element in figure 1, the rate of dangerous failures per hour, reliability and availability are calculated. Based on the range of values presented for SIL, response curves for availability, reliability and safety are elaborated.

The response curve for the utility and security level for the CAT processing unit, in terms of architecture decision, presents the 2oo3 arrangement, with redundancy in the opposite cabin, the best result. The expected utility associated with the quality attributes of an architectural decision is the calculation of the benefit of those architectural decisions by adding the benefits of all relevant quality attributes. The benefit of an architectural decision is the sum of the differences between the expected and current utility for each quality attribute of that architectural decision. This benefit is multiplied by a factor corresponding to the importance of each scenario, factors originating from a consensus among those interested in the system design.

The calculation of the return on investment (ROI) for this analysis is not intended to define in terms of the amount and time of return, but rather to use a relationship between the determined benefit and the cost of developing and implementing the elicited architectural decisions, based on the definition of the scenarios. The calculation of the relationship between the total benefit of an architecture and the associated cost of implementation in all phases of the life cycle, establishes that the architectural decisions, the most suitable are those with the highest ROI rate. The estimate in table III is based on the sum of the hardware and software development involved during the project life cycle for the CAT system. The proposed analysis for assessing the cost of implementation and the benefits of a railway system security architecture, for CAT, similar to the systems implemented in railroads in large cities in South America, to meet the specific need of the scenarios, RAMS and risks of each proposed architecture decision, in order to obtain a classification for architectural decisions regarding the benefit and return on investment, and the guidelines presented in [12], the most positive results are presented considering the ROI in table III:

Table III. ROI para as Decisões de Arquitetura

| Scenario | Architecture Decision | ROI |
|---|---|---|
| D1 | Use an amplifier set with antenna association in a 1oo1 configuration | 0,1274 |
| | Use an amplifier set with antenna association in a 1oo1 configuration with redundancy across the remote cabin set | 0,1228 |
| | Use an amplifier set with antenna association in a 1oo2 configuration with redundancy across the remote cabin set | 0,1288 |
| D2 | Use decoder unit in 1oo2 architecture for local cabin redundancy | 0,0676 |
| | Use decoder unit in 2oo2 architecture for redundancy in the opposite cabin | 0,0636 |
| | Use decoder unit in 2oo3 architecture for redundancy in the local cabin | 0,0542 |
| D3 | Use 1oo1 architecture | 0,0488 |
| | Use 2oo2 architecture with remote cabin redundancy | 0,0502 |
| | Use 2oo3 architecture with remote cabin redundancy | 0,0438 |
| D4 | Use 1 IHC per cabin | 0,1293 |
| | Use 2 IHC per cabin | 0,0937 |

- Scenario D1: to use a set of amplifiers associated with antennas in a 1oo2 arrangement with redundancy over the remote cabin, that is, even though it is the option with a higher hardware and software development cost, it is also the decision of architecture for preamps and antennas with the best benefit, which presents as the best response curve for the usefulness of availability as being the 1oo2 arrangement. It presents as the best response curve for the usefulness of the SIL level as the 1oo2 arrangement. Therefore, only a business rule to increase reliability would justify the choice of an architecture decision different from the 1oo2 arrangement.
- Scenario D2: to track signal decoder unit in a 1oo2 arrangement with redundancy by the local cabin. This result is due to the significantly lower hardware and software costs associated with this decision, even with the worst benefit. It presents as the best response curve for the utility of reliability as the 1oo2 arrangement. It presents the best response curve for the usefulness of the SIL level as the 2oo2 and 2oo3 arrangements. Therefore, availability and SIL level indicate the 2oo2 and 2oo3 arrangements as the best decision.
- Scenario D3: is used a processor unit in a 2oo2 arrangement with redundancy over the remote cabin. This result is due to the cost of hardware and software associated with this decision being intermediate in relation to other decisions, but with the best benefit. It presents as the best response curve for the

availability utility as the 2oo3 arrangement. The best response curve for the utility of reliability as the 1oo1 arrangement. It presents the best response curve for the usefulness of the SIL level as the 2oo3 and 2oo2 arrangements, in that order. Therefore, availability and SIL level indicate the 2oo3 and 2oo2 arrangements in that order as the best decision, and with the best ROI for the 2oo2 arrangement.

- Scenario D4: is used an IHC unit in a 1oo2 arrangement with redundancy over the remote cabin. This result is due to the lower hardware and software cost associated with this decision, and with the best benefit. It presents as the best response curve for the availability utility as the 2oo2 arrangement. It presents as the best response curve for the utility of reliability as the 1oo2 arrangement. It presents as the best response curve for the usefulness of the SIL level as the 1oo2 and 2oo2 arrangements. Therefore, reliability, SIL level and ROI indicate that the 1oo2 arrangement is the best decision.

It can be seen that the proposed scenarios are analyzed, according to the cost and benefit of each of the options, in order to give the necessary support to those interested in the project, in relation to decision making.

## V. Conclusion

In a systematic way of negotiating conflicts, an evaluation of the costs and benefits associated with alternative architectures in a railway system, for the automatic train control subsystem. In analysis elaboration, adaptations are included, in order to propose a systematic, improving the way of driving and avoiding subjectivity in the judgment of the interested parties, in relation to the evaluated scenarios. The analysis is guided by RAMS concepts and the specific needs of critical security systems, to support both a quantitative and qualitative assessment of the architecture. This analysis proposal is not intended to be definitive and cover all possible conditions, but rather to support system managers and architects, for decision making between alternative architectures. Throughout the development of this work, relevant points that make up their contributions are identified.

Good architecture documentation is crucial for the success of evaluation methods, especially regarding the diagrams and descriptors of architecture of a system, in order to organize the rationale adopted in its conduct [29], [30]. There is an initial effort in activities to redo the architecture documentation and to elaborate more significant scenarios for the operational issues of the system and in order to meet the different requests and changes. The possibility of a consensus among those interested in the scenario elicitation phase can result in architectural decisions that serve only those stakeholders with greater decision-making power, even when applying a negotiation system, this trend exists. The stakeholders involved have different levels of knowledge and before the assessment starts, this knowledge must be leveled. In addition, stakeholders are often unaware of the business rules and restrictions desired by an organization. A simulation of the projects to be developed would provide indirect gains to the system and the organization that carries it out, such as the dissemination of technical knowledge, business rules and organization guidelines.

An organization needs information on how much it will have to invest to increase earnings, and to control and mitigate the risks in a project. This systematic way of conducting the definition of an architecture can support the identification of risks and quantification of gains. Architectural decisions have an associated cost, the calculation presented through ROI, can improve these decisions, clarifying and improving the uncertainty index. The difficulty in adopting the methods is the choice between the possible changes that can occur in a system. Selecting a subset of strategies is difficult. As the resources for building and maintaining a system are finite, a rational method is needed to support the choice of architecture options during the initial design and in the subsequent phases. Getting stakeholders to take over this process is essential.

For future work, it is considered the need to carry out more simulations to refine the systematization of negotiation in the decision process and that the cost and benefit analysis can be compared with previous results, in order to improve the rationale to be adopted in other projects. In addition, they must be applied to other application domains, in critical security systems, in which case, the technical standards and concepts used as a reference, must be revised for the domain in question. In addition, it is necessary to develop automated tools, which can be made available, at a low cost, to improve the decision-making process.

## References

[1] R.N. Taylor, N.Medvidovic, E.M. Dashof, “Software Architecture, Foundations, Theory, and Practice”, John Wiley, 2010.

[2] L.M. Daville, C. Zhang, “A Semi-Automation of a Cost Benefit Analysis Method”, Journal of Software Engineering and Applications, 2012, 5, pp. 385-394.

[3] K. Tuma et al., “Finding Security Threads that Matter: An Industrial Case Study”, www.arXiv.org, acessed in 2019, December.

[4] D. Leffingwell, D. Widrig, "Managing Software Requirements, a Use Case Approach, Addison Wesley, 2nd. Edition, 2003.
[5] A.V. Roriz, G.N. Rodrigues, L.A. Laranjeira, "Analysis of the Impact of Implied Scenarios on the Reliability of Computational Concurrent Systems, VIII Simpósio Brasileiro de Componentes, Arquiteturas e Reutilização de Software, SBCARS, 2014.
[6] E. R. POORT, P.H.N. WITH, "Resolving Requirements Conflicts through Non-Functional Decomposition", Proceeding of the Fourth Working IEEE/IFIP Conference on Software Architecture (WICSA'04), IEEE, 2004.
[7] J. P. Matos, "Concepção de uma Arquitetura de Software com Base nos Estilos de Arquitetura e Requisitos Não Funcionais". Tese de Doutorado, Escola Poliécnica, Universidade de São Paulo, 2005.
[8] M. Davena, A. Herrmann, "Requirements Priorization Based on Benefit and Cost Prediction: A Method Classification Framework", 34 th. Euromicro Conference Software Engineering and Advanced Applications, IEEE Computer, 2008, pp. 240-247.
[9] R. Wohlrab, T. Gooijer, A. Koziolek, S. Becker, "Experience of Pragmatically Combining RE Methods for Performance Requirements in Industry", aceito pelo IEEE em 2014, não publicado.
[10] EN 50126, "Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)", Cenelec, 1999.
[11] EN 50128, "Railway applications – Software for Railway Control and Protection Systems", Cenelec, 2001.
[12] EN 50129, "Railway applications - Safety related electronic systems for signaling", Cenelec, 2003.
[13] L. Bass, P. Clements and R. Kazman, "Software Architecture in Practice", Addison-Wesley, 3th. Ed., 2013.
[14] SEI, "CBAM: Cost Benefit Analysis Method". Technical Report, http://www.sei.cmu/activities/architecture/product/cbam.html ., acessed in September, 2017
[15] C. Dhaya; G. Zayaraz, "Combine Architectural Framework for the Selection of Architecture using ATAM, FAHC and CBAM", International Journal of Computer Applicatons in Technology, Vol. 54, Issue 4, 2016.
[16] IEC 60050(191), "International Electrotechnical Vocabulary chapter 191: Dependability and Quality of Service", IEC, 1990.
[17] ISO/IEC 61508, "Functional safety of electrical/electronic/ programmable - electronic safety-related systems", IEC, 2000.
[18] B. Knegtering, A.C. Brombacher, "Application of Micro Markov Models for Quantitative Safety Assessment to Determine Safety Integrity Level as Defined by the IEC 61508 Standar for Functional Safety", Reliability Engineering & System Safety, Volume 66, Issue 2, November 1999, pp. 171-175.
[19] W.J. Gutjahr, Software Dependability Evaluation Based on Markov UsageModels", Performance Evatuation, Elsevier, 2000.
[20] W.S. Greenwell, "Pandora: An Approach to Analysing Safety-Related Digital-System Failures", Universiy of Virginia, 2007.
[21] IEC 61078, "Analysis Techniques for Dependability- Reliability Block Diagram Method, Geneva, IEC, 1991.
[22] R. Soya, "Software Reliability", Computational Statistics, Vol. 3 (3), pp 269-281, 2011.
[23] ISO/IEC 25010:2011 –" Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models", ISO/IEC, 2011.
[24] Alstom, http://www.transport.alstom.com/, acessado em junho de 2014.
[25] Bombardier, http://www.bombardier.com/ acessado em junho de 2014.
[26] Siemens, http://www.siemens.com.br/, acessado em junho de 2014.
[27] B. Boehm, D. Port, A. Shah, J. Kwan, R. Madachy, "A Stakeholder Win-Win approcah to Software Engineering Education", Annals of Software Engineering, J.C. Baltzer AG, Science Publishers, 1998, pp. 295-321.
[28] MIL-HDBK-217-F - NOTICE 2, "Reliability Prediction of Electronic Equipment. Military Handbook", Department of Defense of USA, 1995.
[29] ISO/IEC/IEEE 42010, "System and Software Engineering- Architecture Description", Engineering Standards Commitee, New York, NY, 2011.
[30] A. Tang, M.F. Lau, "Software Architeture Review by Association", The Journal of System and Software", Ed. Elsevier, 88, 2014, pp. 87-101.

## BIOGRAPHY

**Jussara Pimenta Matos** an is professor in the Department of Electrotechnical at Instituto Federal de São Paulo, São Paulo, SP. She earned her PhD in Computer and Digital System from Escola Politécnica da Universidade de São Paulo (USP), São Paulo, SP, Brazil. She has experience in Computing Engineering, focusing on Safety Systems. Development of Software Project and elaboration of Test Procedures for the Message Switch System (CCAM) using Aeronautical Fixed Telecommunication Network (AFTN), based on standard ICAO (International Civil Aviation Organization). Technical analysis of the SIVAM System Management Plan and its related documents (Software Development Plan, Master Test Plan), regarding the responsibilities of Brazilian Integrating Entity, in USA and development of computer software based on the IEEE Software Recommendations. System and Software Requirements Analysis, classification and allocation in subsystems for the CCAM project. Development of Operation Control Center of Hydroelectric Power Generation for Itaipu Binational Company, joint effort with ABB (Austria). Development of Digital Control System for the Brazilian Navy, for controlling an Atomic Power Generation Unit. Development of the Software Development Methodology based on standard DOD-STD-2167A. Elaboration of Technical Proposal for development project of Operation Control Center for Itaipu Binational Company. Participation in HVDC Project in Consortium ASEA-PROMON for a Turn-Key system.