STAMP Method Application on Industrial Management

SYSTEMS THINKING APPLIED TO INDUSTRIAL MANAGEMENT

Lucas Jardim Ribeiro, lucas_ljr1@hotmail.com
Dr. Marcelo Santiago de Sousa, marcelo.santiago@unifei.edu.br

Institute of Mechanical Engineering
Federal University of Itajubá - UNIFEI

ABSTRACT

This work's main goal is to apply the STAMP (*System-Theoretic Accident Model and Processes*) method, a safety system thinking process, in order to detect evident and hidden waste causes in a small-sized I.T. company's production line. The company will be modelled as a general control system from client-company interface to the last hierarchy level.

1 INTRODUCTION

From research & development to scheduled maintenance, the aerospace industry deals with high cost labor, materials, procedures and human resources. Safety walks with the same pace of efficiency, given all wrapped costs.

The human ambition and curiosity led us to idealize new technologies that allow high atmosphere and space exploration. Electronic systems were one of these tools, and as mentioned by Roger [4], the Columbia Space Shuttle's embed software was mystified as "perfect", "bug-free" and "errorless". Although it is a controversial topic, this high level of safety has been reached by discipline, professionalism and modern people's and project's management practices.

That last one is purely theoretical and abstract, being impossible to materialize like a jet engine or a thermal ceramic protection. However, organization techniques are a concrete reality and a critical subject in a business.

According to Crute *et al*[1], manufacturing sciences radically changed since last decade, assuming a dynamic form just like high customization, specialization flexibility, lean thinking, high agility way of thinking, instead of a static form represented by mass production systems.

The Figure 1 represents a big motivator to this study, assigning compromised costs at each phase of a life of a product. At the conceptual phase, where only 8% of total cost was already invested, 70% of the total costs has been assigned. At production and test phase the defect's correction costs varies from 500 to 100 times the expended investment. That study in particular supports the urge to carefully plan the project at the conceptual phase.

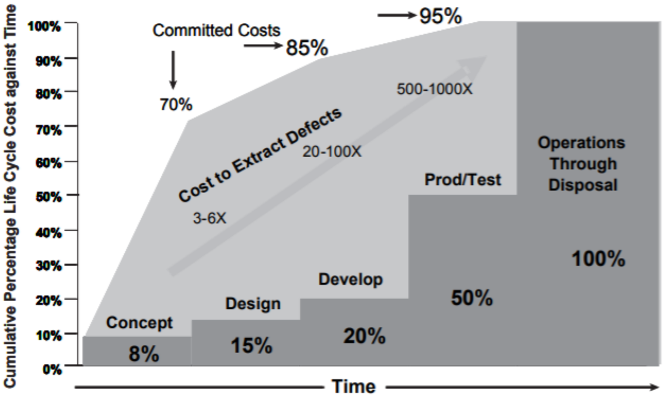

Fig. 1 . Compromised cost by time [2]

2 OBJECTIVES

This work's main goal is to identify possible or factual time and/or money waste in an entire project cycle of a software and propose corrections using the STAMP method as tool. This will be done by modeling the company as a standard control system with different levels of hierarchy and applying the STAMP methodology, more specifically the CAST (Causal Analysis using Systems Theory) tool that seeks to determine why the system components behaved incorrectly and eventually failed, and what were the control actions that allowed the accident to happen.

According to Womack [5], the lean mode of production took years to be implemented in the mass-production industries due to the inherent displacement and "pain" of changing. Although the study company does not have the lean structure in its entirety, corrective actions will be suggested taking into account that these will have a significant impact on the company's work culture.

It is important to note that the project management method used by the company will be evaluated, but there will be an effort to reconcile the proposed measures with the existing models to minimize the impact of the change. The company will be modeled and the method applied in full, with the publication of the change proposals.

After the conclusion of the case, a methodology will be outlined so it can be used as tool for other cases.

3 THE STAMP METHOD

This chapter will introduce the STAMP philosophy and methodology, as well as the procedures and mechanisms that will be used in the analysis. This method brings solutions to the gaps of chain-based security methods. The information presented here is a reference to Leveson's Engineering to Safer World: Systems Thinking Applied to Safety (2012).

3.1 System-Theoretic Accident Model and Processes (STAMP)

Initially, let's generalize the definition of accident: it is an unplanned and unwanted loss event. This loss may involve a human life or bodily injury, but also other significant losses such as mission, equipment, financial resources and information.

Losses are due to component failures, external system disturbances, interactions between system components, and behavior of individual systems that can lead to dangerous situations. As an example of dangerous situations, one can cite high doses of medication, oil leakage in a refinery and the doors of the wagon of a subway opening with the same in movement.

Properties such as security arise from interactions between system components. These properties are controlled by imposing behavior constraints and interaction between components, causing security to become a control problem, where the purpose of this is to force security constraints. Accidents are inadequate control results and restrictions in the development, design and operation of the system.

A controller has one main goal: to control the behavior of the system and force it out of dangerous situations. These controls doesn't need to be physical, but also human or electronic. Social controls include management, state organizations, corporate policy and even cultural (set of moral rules that shape the behavior of the individual in society).

In this section, understanding why the accident occurred requires the determination of why the control was inefficient. Accident prevention requires shifting the focus from failure prevention to a broader scope, which involves designing and implementing controls that will enforce the necessary restrictions.

The STAMP crash model is based on these principles described. Three concepts that support it are:

1. Security Restrictions;
2. Hierarchical structure of security control;
3. Process models.

3.2 Safety Restrictions

The most basic concept of STAMP is not an event, but a restriction. It is assumed that a loss only occurs because security restrictions have not been successful. The difficulty of applying this concept has been increasing from the past to the present, since the limited materials and processes of that time naturally restricted systems. Today, however, progress in these areas creates new constraints. As an example, the structure of a fighter plane can be designed to withstand much higher load factor than a human does. If the limitations were structural in the past, today the limitation is the operator itself.

The proper procedure is first to identify the safety constraints that must be met so that the controls can be designed, tested and incorporated into the system. The responsibility for imposing restrictions should be divided and allocated to appropriate groups. For example, members of a certain group may be charged with conducting risk analysis. The manager of the same group can be tasked with ensuring that the group has the resources, skills and authority to perform such analysis with a satisfactory level of quality. Higher level managers may be responsible for distributing budgets, determining work policies, and ensuring that risk analysis information is used by other groups. In this case, we are already describing the concept of hierarchical structure.

3.3 Security control's hierarchic structure

In hierarchical structures of systems, each level imposes conditions on the activity of the next level (just as a block receives information from the previous one). This means that the constraints (or lack thereof) of higher levels control the behavior of lower levels. Later we will verify this fact with the analysis of the impact of the actions of the CEO on the rest of the team.

Control processes operate between levels to control processes at lower levels. These, in turn, fulfill the security constraints for which the control process is responsible. When these processes provide inadequate control and safety restrictions are violated by the lower level components, there is the possibility of an accident.

These inadequate control processes can result from lack of constraints (undetected safety condition in the controller design process), inadequate control of security, poor execution of commands at lower levels, or failure to communicate feedback. For example, the operations coordinator may provide non-secure work instructions to operators, or instructions may be appropriate and operators ignore them.

Between each hierarchical level, effective communication channels are needed, both in the sense of "delivering" order and feedback, as shown in figure 4.1, due to the need to impose security constraints and receive information about how effective the orders are being made. The control uses the lower level response to achieve optimal conditions faster.

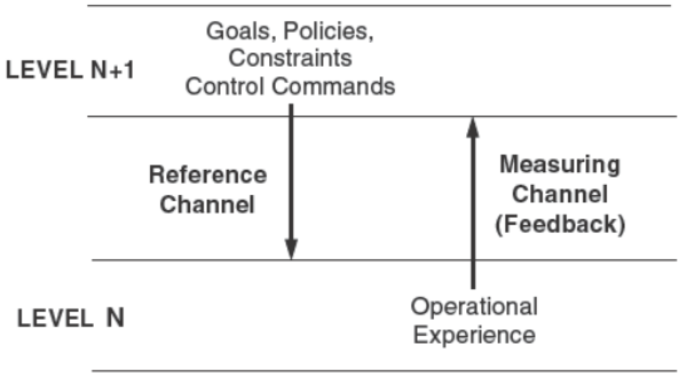

Fig.2 . Communication between levels [3]

Figure 2 shows a socio-technical structure of a typical regulated industry and that safety factor is critical, such as air transport. Each system must be modeled to perform its own functions. In the left column, there is the hierarchical base for the development, already in the right, for the operation. Although distinct, there is interaction between them. The aircraft manufacturer, for example, may have only the systems development division over its administration, however, security involves both development and operational use and both cannot be developed singly. For this, communication channels are created in case of need.

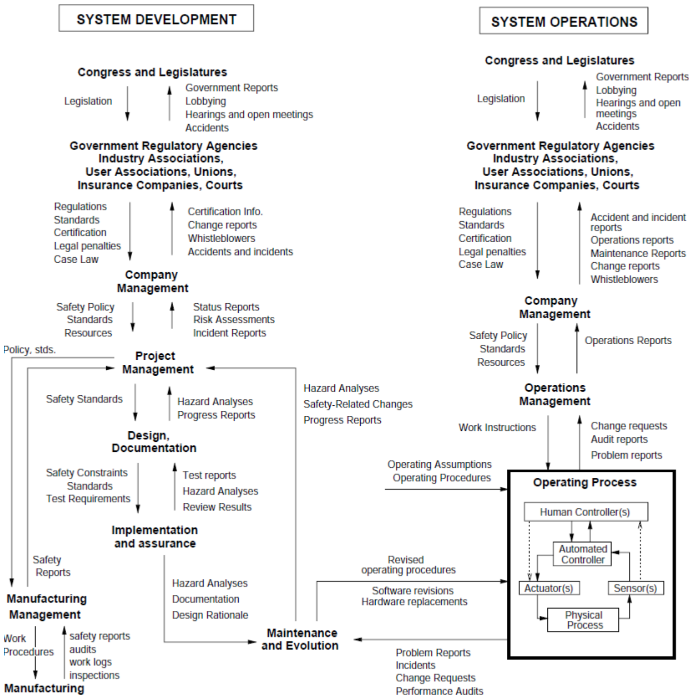

Fig.3 . Common structure of a regular socio-technical control model [3]

3.4 Process Models

The third concept is used in conjunction with the previous two. Four conditions are required to control a process:

1. Objective - In STAMP, are the security constraints that must be imposed by each controller in the hierarchical structure;
2. Condition of action - Go through the process from top to bottom, going from a higher level to a lower one;
3. Observation condition - It traverses the process from the bottom up and is embedded in the feedback;
4. Model Condition - Any human or automated control needs a process model that is being controlled to work properly.

An appropriate process model can contain from one or two variables in a simpler model to a complex state of variables and transitions, such as a model for air traffic control. Whether it is embedded in an electronic controller or in a person's mind, it must contain the same type of information: the required relationship between system variables (control), current state, and ways the process can change state. This model is used to determine what actions are necessary, from the information received by the feedback.

Accidents usually occur when the process model used by the controller is not suitable for the actual process, and as a result, incorrect or unsafe commands are executed, security control actions are not performed, correct commands are not executed at the right time and are unsynchronized.

3.5 Causal Analysis Based on STAMP (CAST)

The causal model used in an accident or incident analysis determines the image of the problem to be solved and subsequent judgments about it. The same accident model can generate very different views depending on the individual who analyzes it.

Most accidents are written from event-based perspective. When the "root cause" is found, immediately something or someone is blamed and the opportunity to learn important lessons is lost.

The use of CAST exceeds the identification of unique causes and factors by promoting the ability to examine the entire socio-technical set of the system, allowing identification of weaknesses in the safety control structure, and identifying changes that eliminate causal factors, including systems.

One goal is to distance yourself from the philosophy of blaming something or someone, and instead focus on why the accident occurred and how to act so that similar losses do not happen again. To do so, it is necessary to minimize the retrospective bias and to look for the reason why people acted in that way with the information received at that moment.

Although the process has predefined steps, which will be presented next, this does not imply that it is linear or that the steps must be followed systematically. Adaptability is key in the analysis:

1. Identification of the system and hazards involved in the loss;
2. Identification of safety restrictions and system requirements associated with this hazard;
3. Documentation of the safety control structure to control the hazard and impose safety restrictions. This structure should include the roles and responsibilities of each component of the structure beyond the controls provided for them to perform their tasks and feedback from each;
4. Determination of the events that led to the loss;
5. Loss analysis at the physical level of the system. Analyze the

contribution of each of the events: physical and operational control, physical failure, dysfunctional interactions, coordination and communication failures, and random disturbances. Determine why physical controls were ineffective in hazard prevention;

6. Determine how and why each higher level allowed or contributed to inadequate control at every level, from the lowest to the highest. For each security restriction, or the responsibility for enforcing them has not been delegated, or the component (s) responsible have not performed proper control to ensure correct compliance. Each human decision or defective control action must be understood in terms of: information available for decision making or necessary information but not available

4 THE OBJECT OF STUDY

The object of study is a software and information systems development company, founded in 2005. Its products are institutional websites, e-commerce, data management systems, Intranet and customized software. It employs approximately 25 workers in the areas of computer science and computer science, and approximately half of these were trainees. It has annual revenue less than R$ 500,000 (around US$128.000). It has several partnerships with state and federal development agencies, which provide benefits for the expansion of services, in addition to being certified with ISO 12207 and Information Technology Law (a tax reductive condition).

The facilities had an individual workstation divided into two environments: main room with CEO, HR and customer support, and secondary room with project manager and programmers. Let's define the set of project manager with programmers as production sector. Being of the computer sector, only one of its products was physical (DVD media), which occupied insignificant space in the premises. All other products were digital and did not take up physical space.

Its clients ranged from individuals to businesses throughout the country. The success of previous projects has increased the visibility of the company in such a way that there were no marketing campaigns, meaning that all customers who sought the services had already pre-selected the company, with mutual interest in the client-company relationship.

This flexibility meant that it was often necessary to invest more time than usual in capturing customer's requirements. Despite this, the main feature of the company, which is flexibility, brings out the need for excellence in the ability to identify design requirements.

The student's internship was focused on the area of project management, having close contact with all interfaces of the company's activities. The activities developed were analysis, classification and division of tasks for product development, supervision of the productive process, design and implementation of improvements in the production process, development of organizational plans, identification of customer needs, alignment between customer needs and development team, integration of the tasks of the development team, alignment of the pace of the development team with deadlines and deadlines, communication and constant updating of productive activities to the customer, acquisition of customer feedback after product delivery.

4.1 Structure

The company has a standard structure with 3 distinct levels but with great interaction between them: the CEO, who also coordinated the sales team, is the first level, the project manager is the second level and the development and production teams, support customer and management are the third level.

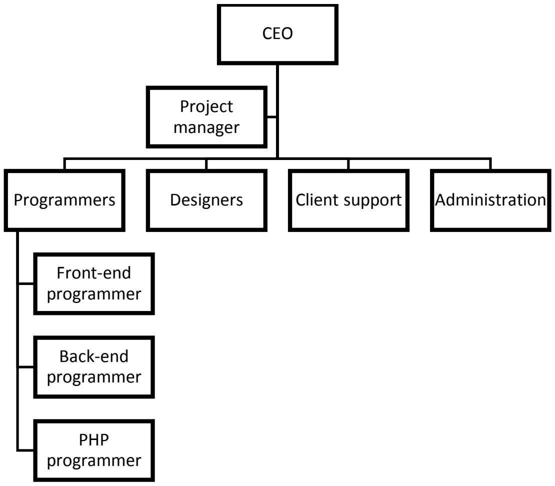

Fig.4 . Company's hierarchy

The distribution and management of tasks is based on the *Scrum* method, which consists of a block of activities with a certain execution time called sprint, which was evaluated daily.

The client has contact with two areas of the company, simultaneously: the sales sector, which negotiates monthly bureaucratic and financial matters, and the project manager, responsible for the product itself. It is possible to model the interface by the client's vision, such as:

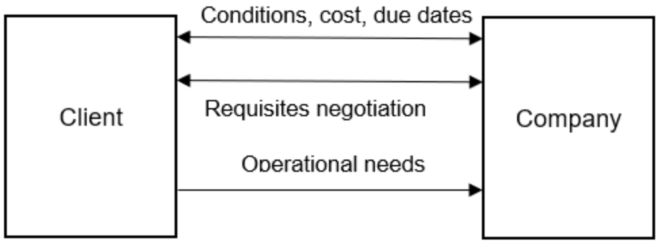

Fig.5 . Client's systemic view

4.2 Encountered problems

The production area presents the following characteristics related to the tasks performed in the daily life of the company, as experienced and reported by the employees:

- Fraction of projects close to 100%;
- Low product conformity;
- Lack of clarity in communicating the project to the team;
- Difficulty in understanding customer requirements initially detected;
- Project Manager does not have a tool for querying individual team tasks;

- Communication of delivery conditions to the customer is ineffective;
- The production sector does not receive a briefing with sufficient technical details of the requirements;
- Employees are always overloaded;
- High employee turnover;
- Low autonomy of the interns, who make up a large part of the company.

The causes of the problems will be investigated later by the STAMP application procedure.

5 METHOD APPLICATION

5.1 System and control structure’s identification

The modeling of the cycle of operations is the starting point for the application of the methodology. In the first moment before the sale is made, the customer only has negotiations with the CEO, who is responsible for the commercial sector, and the contact with the manager happens only during the development of the product. The sign of the opinion is sent to the CEO, but not processed.

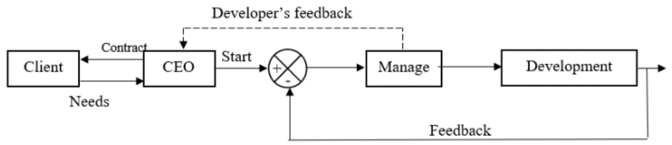

Fig. 6. First level system

Starting at the second level, the CEO block is analyzed initially, represented in figure 6.2. The "needs" signal contains the technical needs and deadlines of the customer, while the "contract" signal contains the conditions, deadlines and prices proposed by the company. The "look" signal, issued by the manager, reaches the CEO but is not processed. This signal contains information about the development team's opinion with workloads and timeliness. The "start" signal contains the requirements data, deadlines, and division of tasks for project execution.

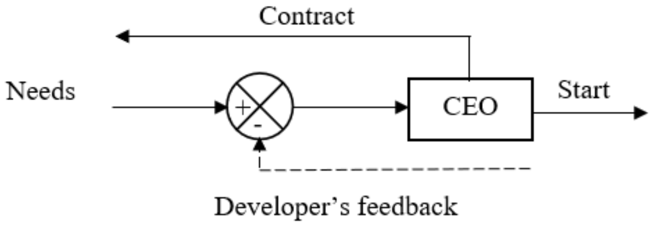

Fig. 7. CEO’s second level system

The manager block is represented by figure 6.3. The "start" signal is processed for pointing out information deficiencies, identifying objectives and development philosophy to be adopted. This processed signal is passed on to the development team as a "mission". At this point in time, the development team processes the information and, prior to the start of the activity itself, sends the "opinion" signal to the manager, who processes the information to identify inconsistencies and risks (such as failure to meet deadlines) “opinion of the development team "

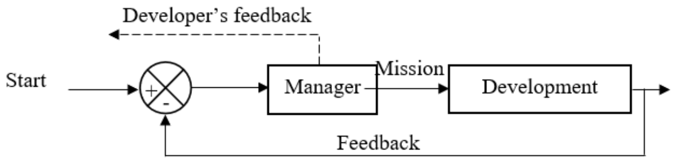

Fig. 8. Manager’s second level system

The block of the development team is represented by Figure 6.4. The "mission" signal generated by the manager is received and processed by the programmers, who identify the workload and items to be met. If the task needs to be performed by two or more employees, the group initially uses the coupling block to discuss the technical ability to fulfill and possible task reallocation between members. After the signal is sent back as "look" and processed, there is the beginning of development. At this point, the coupling is the junction between the split work blocks using Scrum. There is no quality sensor during this cycle and the iteration has a long period, meaning that inconsistencies during the process will be financially costly.

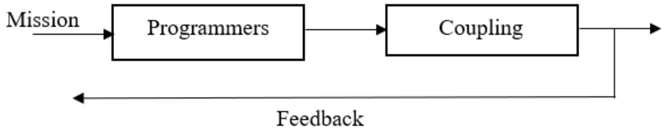

Fig. 9. Developer’s second level system

In the second moment, the system turns to development and delivery and there are changes in its form.

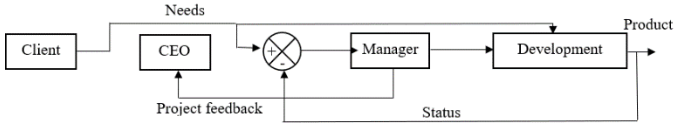

Fig. 10. First level system during development phase

At this moment, the client starts to see the interface of the company from the manager to the development team. The manager has the responsibility of managing the expectations of both parties, while the developer of the development team is the technical side. The "start" signal carries the needs of the product. The "status" signal returns the status of the product, while the "project opinion" reports the progress of the project.

5.2 Accident identification

Following the steps outlined in chapter 4.5, you should first identify the accident. Because it is a business model, the relevant accidents are simply:

- Waste of time (and money);
- Closing a project contract that exceeds the capacity of the company;
- Customer dissatisfaction.

Situations such as negative financial impact and bankruptcy are considered indirect consequences of these accidents.

Dangerous situations are those that have the potential to cause an accident. Based on the situations and the industrial process model , the following are listed:

- Delay in the delivery of tasks;
- Failure to understand the process;
- Failure to capture customer requirements;
- Failure to evaluate the possibility of executing the requirement;
- Internal communication failure;
- Erroneous and disproportionate task distribution;
- Lack of employee autonomy;
- Escape from scope.

From the fourth step these situations will be able to indicate which system commands led to the occurrence of hazards.

5.3 Safety constraints

The second step is the imposition of security restrictions, which will act to prevent the occurrence of dangerous situations. Each risk situation has the appropriate constraint, defined from the tasks that must be performed and taking into account the responsibilities of each position:

1. Delay in the delivery of tasks
   - Tasks should be performed in a timely manner;
   - Timelines should be realistic;
   - Contingencies must be communicated in advance for job reassignment.
2. Failure to understand the process
   - The briefing should be clear and succinct;
   - The briefing should include information and technical specifications;
   - The operator should be able to comment on the quality of the briefing.
3. Failure to capture customer requirements
   - The project manager with technical capacity must capture requirements;
   - A technical specialist in the production area must check the conformity of the requirements;
   - The process must be iterative, but not with substantial changes so that there is no loss of focus.
4. Failure to evaluate the possibility of executing the requirement
   - A technical specialist should determine what is executable or not.
5. Internal communication failure
   - The employee must be trained to communicate constantly with the entire team;
   - There should be a tool for the employee to know the timeline of their task, the next task, who depends on it and who it depends on.
6. Erroneous and disproportionate task distribution
   - Tasks should be quantified in terms of workload by the technical specialist;
   - The tasks should be distributed by the manager and technical specialist;
   - No more sales to be made than the company can produce and deliver.
7. Lack of employee autonomy
   - There should be a training program for each position of the company;
   - The turnover rate should be decreased;
   - The employee must have enough energy to perform his responsibilities;
   - The company's internal policies and cultures must be well-publicized.
8. Escape from scope
   - The project focus should be defined via a contract for legal protection;
   - The scope should have some flexibility, however not significant enough to affect the internal organization.

5.4 Determination of events leading to loss, analysis by level and interaction of contributions

The contribution between levels will be listed linearly in the “responsible” column, while the reasons for the accident / dangerous situation listed above are listed in the “reason” column.

Reason	Responsible
1. Delay in the delivery of tasks	
Short time	CEO, manager and developer
Impossible due dates	CEO, manager
Unforeseen events	Manager, Developer
2. Failure to understand the process	
Low quality briefings	CEO
Incomplete briefing	CEO
Ignored feedback on briefing quality	Manager
3. Failure to capture customer requirements	
Failure in capturing requisites	CEO, manager
4. Failure to evaluate the possibility of executing the requirement	
Evaluation failure	CEO
5. . Internal communication failure	
Internal communication failure	Manager, developer
Inexistent managing tool	Manager
6. Erroneous and disproportionate task distribution	
Quantification failure	CEO, manager
High sales volume	CEO

7. Lack of employee autonomy

No training program	CEO, HR
High turnover	CEO
Worker’s low energy	CEO
Weak work habits	CEO, HR, manager

8. Escape from scope

Client’s close contact to developer	CEO, manager

5.5 New structure

The proposed new organization is represented below.

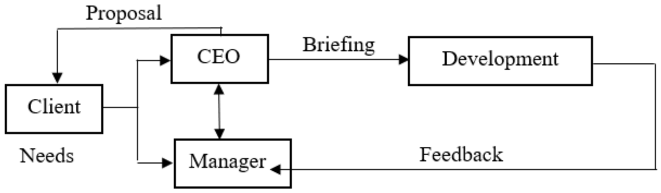

Fig. 11. New structuring of the first level system at the time of pre-sale

The client will convey their needs to the CEO and manager with the "needs" sign, which will translate them into technical requirements. There is constant communication between CEO and manager to define the possibility of project execution. The development team is also consulted for the evaluation of these requirements via a "briefing" signal, which carries this opinion by "opinion". The CEO gathers this information and puts together a proposal, contained in the "proposed" signal.

After the sale is done, the system reorganizes itself in the form:

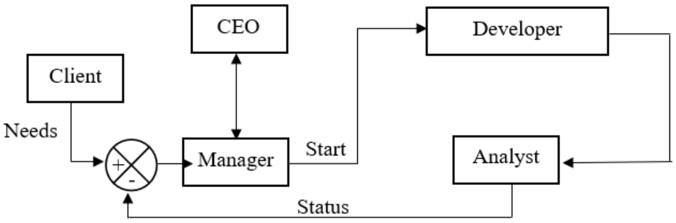

Fig. 12. New structuring of the first-level system in the after-sales moment

The "start" signal contains the requirements already translated, the deadlines and the organization of the project. The development team receives and executes the command, while the sensor, which will be a person of the development team with the role of quality analyst, will capture the conformity of the product and progress, generating the status. The manager will compare the development team's response with the signal that carries the client's wishes, process them, and confirm if there is a need for organizational change. Communication with the CEO is constant.

6 CONCLUSION

The first point evidenced by the method is the retention of tasks by the CEO, which concentrates the probability of failures or dangerous situations in the actions taken by only one person. At first, it is understood that this responsibility is inherent to the position. However, from the systems engineering philosophy, security must prevail and lessons must be learned: decentralization of responsibilities is a necessity for this position.

The direct contact of the client with the developer proved, over time, a situation of danger for the company. Due to the incomplete briefing, the developer sought information already passed by the client, creating wastage of time and wear, showing the sense of disorganization.

Another real situation was the absorption of one of the employees by the customer, which was another company that had the need of a programmer to comply with the system maintenance plan. This close relationship, in addition to exposing the company to a "showcase" situation, means that the client has the possibility to expand the scope of the project through direct pressure on the development team, negatively impacting the planning done by the group. These two reasons are reasons to increase the degree of isolation between the two - taking into account that communication is one of the paths to compliance.

Increasing employee autonomy is also a critical topic. The current model directs critical tasks to the trainee, who does not receive a solid training program to certify the trainee. The reduced workload and inexperience limit the productive power of these employees who, with proper planning, can become key parts of the company.

The picture of the engineering companies today shows an overvaluation of the intern figure, who are increasingly qualified to perform functions of graduate level. In spite of this, the problems of autonomy mentioned above are inherent to this position, which become serious when the majority of the staff is composed of them. The current situation of the Brazilian economy causes that the companies look for alternatives of cheap labor and decisions are taken for the above situation to occur.

It is important to point out that the graphical block diagram language was chosen among the systems engineering vocabulary. However, exploring UML-like languages, or more specifically SysML, can be a point that makes process understanding easier and more efficient.

For a person with training and experience, perhaps these shortcomings can be noticed more clearly. The STAMP method made it possible to survey these points mechanically using a procedure, which can be performed by a professional with the minimum of managerial training.

For the continuation of the work, it is proposed the financial quantification of the implantation costs and avoided wastes.

REFERENCES

[1] Crute, V.; Ward, Y.; Brown, S.; Graves, A.; “Implementing Lean in Aerospace – challenging the

assumptions and understanding the challenges", Technovation, v.23, pp. 917-928.

[2] INCOSE, I. N. C. O. S. E. Systems Engineering Handbook. 2006. Third version.

[3] Levenson, N.G., January 2012, "Engineering a Safer World", The MIT Press, MA.

[4] Roger, D.; Lanius J.K.J.; 2013, "Revolutionizing Electronics: Software and the Challenge of Flight Control", Space Shuttle Legacy, Library of Flight.

[5] Womack, J., Jones, D., Roos, D., 1990. "The Machine That Changed the World". Rawson Associates, New York.

Copyright Statement