

Extending the Borders of Accident Investigation: Applying Novel Analysis Techniques to the Loss of the Brazilian Space Programme's Launch Vehicle VLS-1 V03

Ildeberto Muniz de Almeida,

Department of Public Health, Faculty of Medicine, Botucatu, São Paulo, Brasil.
ialmeida@fmb.unesp.br

C.W. Johnson,

Department of Computing Science, University of Glasgow, Glasgow, Scotland.
johnson@dcs.gla.ac.uk, <http://www.dcs.gla.ac.uk/~johnson>

Abstract There has been a rapid increase in the complexity and integration of many safety-critical systems. In consequence, it is becoming increasingly difficult to identify the causes of incidents and accidents back through the complex interactions that lead up to an adverse event. At the same time, there is a growing appreciation of the need to consider a broad range of contextual factors in the aftermath of any mishap. A number of regulators, operators and research teams have responded to these developments by proposing a number of novel techniques to support the analysis of complex, safety-critical incidents. However, most of the existing case studies focus on systems in the United States or Europe. Relatively few examples illustrate how these approaches might be used to analyse incidents in other working cultures and environments. The following pages, therefore, show how these novel approaches must be adapted to support the Serviço Público Federal investigation into the explosion and fire of the Brazilian launch vehicle VLS-1 VO3.

1. Introduction

The increasing complexity and integration of many safety-critical systems has led to the development of a number of novel accident investigation techniques. Most of these approaches are intended to help analysts identify the root causes and contributory factors that lead to adverse events involving high-technology systems. Previous generations of techniques, such as Multilinear Event Sequencing, Sequential Timed Event Plotting and Failure Event Trees (Johnson, 2003), have centred around the reconstruction of the events leading to an adverse event. In contrast, a range of alternative approaches have been developed to look at the organisational and operational constraints that create the preconditions for incidents and accidents. In particular, Rasmussen (1997) presents a series of models or frameworks that guide investigators to look beyond immediate events involving individual operators to look at management and organisation structures. Similarly, Leveson's (2004) STAMP technique models accidents in terms of the violation of constraints that hold between technical systems, individuals, teams and organisational groups. As far as we are aware, all previous applications of these techniques have focussed on the organisational and operational background to adverse events in the US and in Europe. In contrast, we were motivated to apply these approaches to a case study from a different engineering environment. We had two aims. First to determine whether the application of these techniques might help to identify any underlying differences in the technical and organisational environment involved in an adverse event outside the US and Europe. Secondly, to determine whether these techniques might need to be

adapted to better reason about any differences that might not already be captured by the existing approaches.

This work was inherently interdisciplinary. The co-authors have very diverse backgrounds as can be seen from our affiliations. One had previously focussed on epidemiological and sociological approaches to the analysis of incidents and accidents in Brasil. The other had a more technological background, specialising in the analysis of complex system failures including joint work with NASA on the Mars Surveyor Mission Failures (Johnson, 2003) and the mission interruption to the joint NASA-European Space Agency SOHO satellite (Johnson and Holloway, 2003).

1.1 The VLS-1 VO3 Accident and the Official Investigation

The remainder of this paper uses an accident involving a Brazilian VLS-1 V03 launch vehicle. The VLS launcher was developed by the Orbita company under control of the Centro Técnico Aeroespacial (CTA) and of the Instituto de Aeronáutica e Espaço (IAE). It is a 4-stage solid fuel rocket that weighs approx. 50 tons and measures 19 m high. It is made of a central body to which 4 boosters (derived from Sonda-4) are attached. Those boosters are 1 m diameter, 9 m long and weigh a total of 8.5 tons. The incident occurred during the afternoon of August 22, 2003. This was some three days before the scheduled launch from the Launch Centre of Alcântara (CLA), Brazil. The vehicle exploded killing 21 technicians that were preparing the rocket inside the mobile launch tower. It was the worst accident in the history of the Brazilian space program.

The Official Serviço Público Federal report (2004) argues that the most probable cause was an electrostatic discharge inside the detonator of the ‘A’ first-stage booster. This ignited the booster while the launch vehicle was still being assembled. The investigation team commented that further tests were required to firmly establish this hypothesis. The report also discusses others less probable hypotheses about the origins of the accident and identifies several problems not directly identified as “causes” but that might threaten the future safety and reliability of the project. This accident is used to illustrate the remainder of the paper because it is typical of a more general class of failures involving complex and tightly integrated systems. The focus on an incident involving a Brazilian launch vehicle also expands the scope of recent investigations into new generations of causal analysis techniques that typically focus on US or European systems (Johnson, 2003).

1.2 Objectives and methods

This paper analyses the information presented by Serviço Público Federal. In particular, we are keen to determine whether Rasmussen’s analytical framework (Rasmussen 1997; Rasmussen & Svedung 2000, Svedung & Rasmussen 2002) and Leveson’s (2004) STAMP techniques can yield insights into the events surrounding this incident. Previous case studies in the use of these novel techniques have focused on adverse events in North America and Europe, including the Walkerton Public Health incident. In contrast, an important aim behind our work is to determine whether these same techniques can be used to analyse adverse events within the very different regulatory and managerial context of the Brazilian Aerospace industry.

It is important to emphasise that our application of these techniques was initially based around the findings of the official report. This decision was partly due to the

sensitive and strategic nature of the systems involved in this incident. We were, therefore, concerned to determine whether the Serviço Público Federal's description of the accident was sufficient for us to use Rasmussen's and Leveson's methods. We were also motivated to compare the output from these analyses to identify any differences between these findings and those of the Serviço Público Federal.

We decide to use Rasmussen and STAMP model because both focus on the manner in which complex socio-technical systems create the preconditions that contribute to adverse events. Rasmussen's models focus on information flow. However, his approach does include a chain of events in its lower levels. These 'chain of events' models are similar to timelines; they describe the way in which particular incidents develop over time. They have, however, been widely criticised by the proponents of STAMP because they often encourage analysts to focus too closely on particular instances of human 'error' rather than at the context that makes those errors more likely. STAMP, therefore, does not use a chain of events. Instead, it relies upon a "control-theoretic approach down through and including the technical system and its development and operation" (Leveson 2004, p 249).

2. An Introduction to Rasmussen's Framework for Accident Investigation

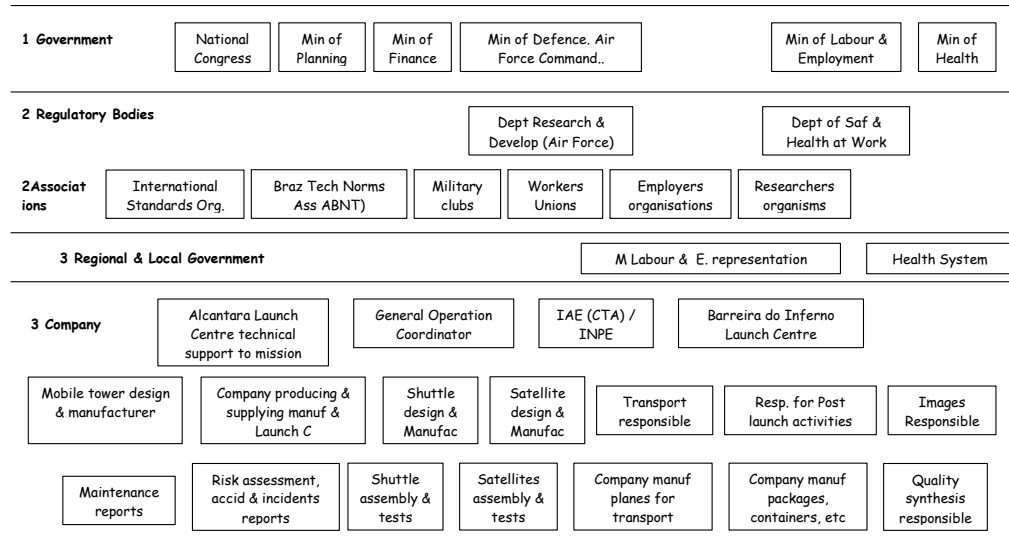
Rasmussen and Svedung (2000, p 18) recommend a sequence of phases to the analysis: 1) Select and analyse a set of accident cases; 2) identify the actors and represent them in an *ActorMap*. This provides a graphical representation of the individuals and groups that are involved in an adverse event; 3) construct a general *AcciMap* that builds upon the ActorMap to chart out the events leading to an incident or accident; and 4) a work analysis identifying the individual decision makers and planning bodies that should be subjected to further interviews and work studies as part of a more sustained investigation. From such interviews they recommend the construction of another *InfoFlowMap*. This represents "the information flow among decision makers during normal activities" (Svedung and Rasmussen 2002, p 403). This process can also identify weak links in the communication patterns within organisations. For instance, a number of case studies have been developed to identify conflicts among the actors involved in adverse events (Rasmussen & Svedung 2000, Woo & Vicente 2003).

It is important to emphasise that Rasmussen developed these techniques to be applied across a class of similar incidents and accidents. The intention is to identify patterns of failure in socio-technical systems using a cross-disciplinary analysis. However, Rasmussen and Svedung (2000) also recommend the use of these techniques to support the analysis of single adverse events. Hopkins (1999, 2000) and Woo & Vicente (2003) have also used the model in this way.

2.1 The ActorMap

Figure 1 presents an ActorMap for the VLS-1 accident. As can be seen, the main intention behind the diagram is to provide a broad-ranging analysis of the socio-technical system. Each diagram considers six different levels ranging from governmental issues at the top down to the local environment in which an incident might have taken place. Working up, the fifth level immediately above the local topography, describes the process that are being controlled. The fourth level describes

the individual staff members that are interacting with the process being controlled. The third level describes the managers that supervise staff activities and aspects of the company policy and strategic choices in a competitive market. The second level describes activities of regulators and associations responsible for monitoring the activities of the companies in that particular sector. The top level (level 1) details activities of the government and juridical aspects related to the same sector (Rasmussen 1997, Svedung & Rasmussen 2002).



(Obs: Details of teams composition not represented in lower levels)

Fig 1. Generic ActorMap for the Case Study

The motivation for representing each of these levels is that systems behaviours will adapt to environmental changes. In order to understand events at any particular level, it is therefore important to understand what has gone on at higher levels in the framework. According to Rasmussen, the pace of change in technical processes will often outstrip changes in management structures, legislation and regulations. People are constantly facing situations that are not covered by available rules and procedures (Rasmussen & Svedung 2000, p 13). In these situations workers have a degree of freedom to decide what to do and how to do it. These adaptations in the face of environmental changes go beyond the limits established in procedures and regulations. As we shall see, many of these observations have particular resonance in Brazil where there is a rapid pace of social and technological development within certain areas of the economy. In each level, in different parts of the system, changes are happening in such a way that is difficult for the people involved to foresee the possibility of adverse consequence for their actions. Local work conditions lead to frequent modifications of strategies and activity that show considerable variability (Rasmussen 1997).

2.2 The AcciMap

Rasmussen's approach relies upon an AcciMap to reconstruct the events leading to an adverse event. In most previous case studies, these maps have been based around a variant of cause consequence analysis. However, this technique is not well known in Brazil and we, therefore, resorted to causal trees (Monteau 1999; Binder, Almeida & Monteau 1995). Both causal trees and cause consequence analysis provide a graphical

representation of the factors that contributing to adverse events. Irrespective of the analytical technique that is used, the intention is to integrate information about the events that contribute to an accident in the ActorMaps that were introduced in the previous section. Figures 2 and 3 illustrate the way in which this can be done for the VLS-1 case study. Figure 2 represents the initial events in the lead up to the accident. Figure 3 represents the triggering events in more detail. In both cases, the diagrams consider events at various levels throughout the ActorMap.

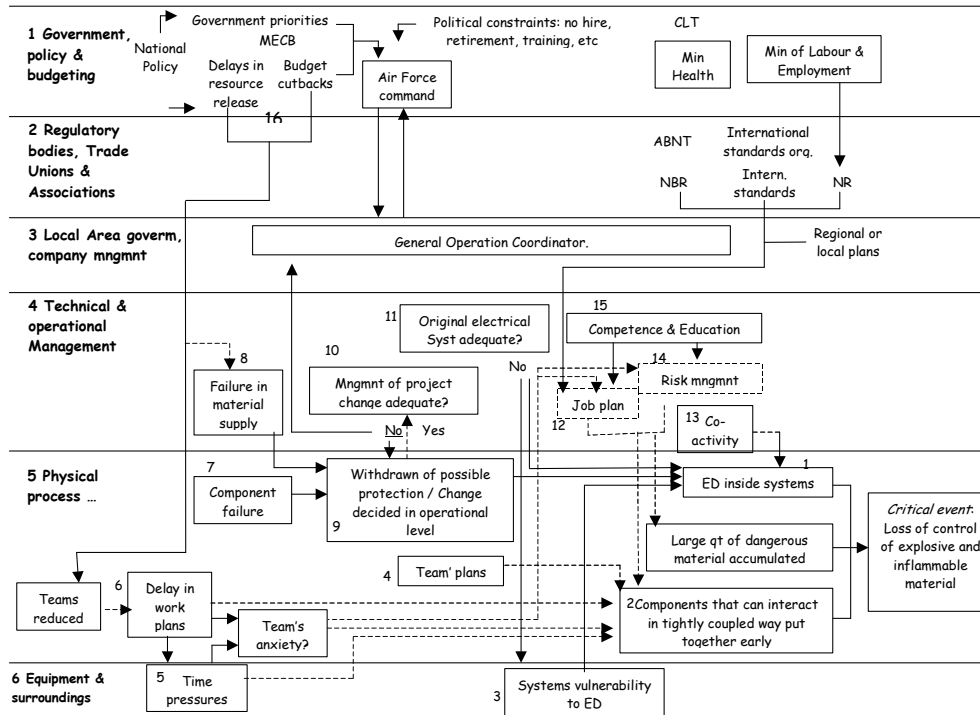


Fig. 2: Example AcciMap for the Case Study (Part 1)

For example, levels 4 and 5 of Figure 2 show that the failure to supply armoured wires combined with the withdrawal of mechanical protection for the detonator both contributed to the accident. These preconditions arose some time before the incident itself. The decision to remove the mechanical protection was taken almost five years before, in the aftermath of a previous failure during the launch of VLS-1 VO1. This protection device was identified as a primary cause of the earlier incident. In consequence, a relay module provided short circuit protection and in conjunction with armoured wiring, was used to replace mechanical protection. However, this decision together with the lack of armoured wiring combined to create the preconditions for the explosion involving VLS-1 VO3.

As we shall see, the higher levels of these diagrams possess many similarities to elements in the STAMP control structure. They can be used to trace back the organisational, government and regulatory factors that contributed to specific problems and design deficiencies. There are also many differences between STAMP and the AcciMap. Each of the numbers in these diagrams can be used to refer to specific evidence; in this case we use them to cross-refer between the diagrams and sections in the documents provided by the Serviço Público Federal using a look-up table. These numeric identifiers can also be used to denote particular events in the trajectory towards an incident or accident. Such events are explicitly excluded from the STAMP approach.

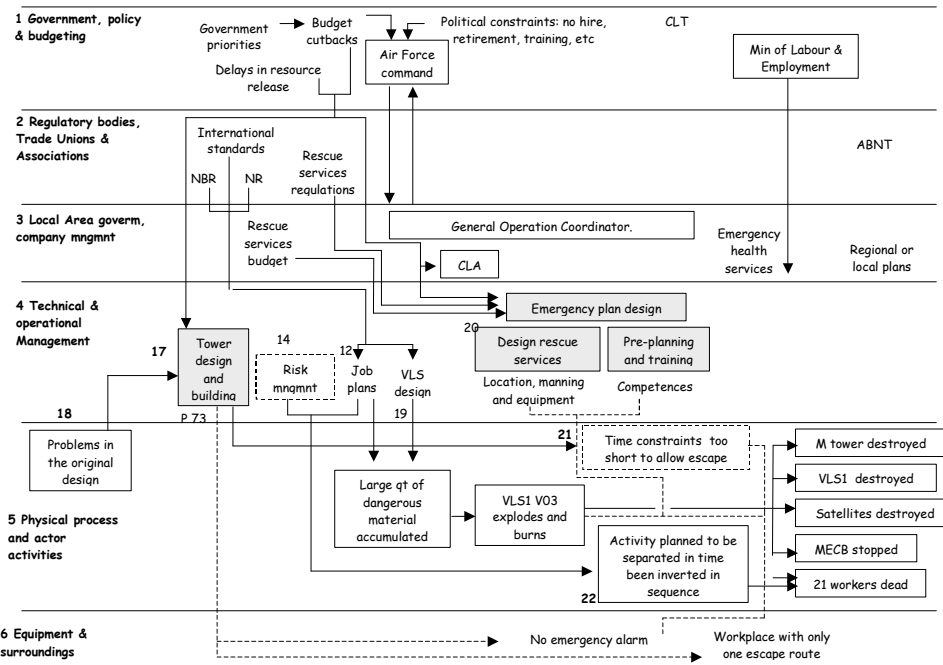


Fig. 3: Example AcciMap for the Case Study (Part 2)

Figures 2 and 3 map the events leading to an accident onto the structure provided by an ActorMap. The evidence supporting our analysis was drawn initially from the Serviço Público Federal. This raised a number of problems. In particular, Figures 2 and 3 use dotted lines to indicate where inferences had to be made about the relationships between groups and individuals involved in this incident. For example, the report raises some questions about whether the design of the mobile launch tower contributed to the severity of the incident. Areas of levels 4 and 6 in Figure 3 illustrate this. Uncertainty arises in our analysis because it is unclear whether or not a redesigned tower with shorter evacuation times would have had any impact on this incident where the lack of alarms did not prompt any more immediate evacuation. Similarly, the Serviço Público Federal report states that non-armoured wires had begun to be used approximately 4 years before this incident. This followed a period when it had been difficult for engineers to obtain supplies of these components. However, the report does not investigate in detail the reasons why the supply was cut back. Elsewhere in the report, there are passages that refer to reductions in the mission budget and delays in resourcing. In level 4 of figure 2 we put a dotted line to indicate a possible relationship between these two aspects of the incident although this connection is not made explicit in the report itself.

Figures 2 and 3 also illustrate a number of other aspects that contributed to the VLS-1 VO3 accident. The Serviço Público Federal argued that the Brazilian teams suffered from a lack of knowledge about and experience with electrostatic discharge. This is represented in level 6 of figure 2 and the associated links back to risk management at level 4. The system's vulnerability to electrostatic discharge was exacerbated by the presence of potential sources near the non-armoured wires. Many of these sources stemmed from the activities of the many different teams that were working inside the launch tower at the time of the accident (level 5, figure 4).

The diagrams in Figures 2 and 3 present important strengths of the AcciMap approach; it is possible to overlay a number of different relationships onto the ActorMap structure. In this case, we have tried to distinguish between latent and catalytic events in the lead up to the accident. It is, however, possible and in many cases necessary to create links between these different representations. For instance, levels 4 and 5 in Figure 2 and level 5 in Figure 3 refer to the sequence of planned activities during the day of the accident. In the morning two of the four detonators of the first stage boosters had been connected to the electrical net (level 5, figure 2). According to the investigation team this activity should have been postponed after the decision had been made to put back the original launch day. In particular, there were a number of additional assembly tasks that should have been completed before any of the detonators were connected. These preparatory tasks had also been delayed. This sequencing of tasks was intended to insure that only a few workers were in the tower after the detonators had been connected. The fact that these other tasks had to be completed *after* some of the detonators had been connected made a direct contribution to the large number of victims (level 5, figure 3).

2.3 The Conflict Map

Figure 4 presents a final stage in the Rasmussen technique. Conflict maps provide a means of documenting a further stage of analysis that can be based upon the results of the AcciMaps shown in the previous section. These conflict diagrams are again structured using the six levels from the ActorMap hierarchy. In this case, however, the investigators annotate each of the levels with potential conflicts and tensions that might have contributed to the preconditions for the incident. In other words, there is an attempt to look behind the particular problems identified in the AcciMap to locate the underlying problems. For example, the budgetary problems affecting the Air Force command in Figure 3 can be traced back to areas of Planning and Finance Ministries and also Congressional Appropriation Committees that control the budget elaboration, and approbation. Similarly, difficulties in preparing an emergency plan notes at level 4 of Figure 3 might be traced back to issues of feedback and conflicting priorities between various organisations in level 4 of Figure 4 including the Centro Técnico Aeroespacial (CTA) or the Launch Centre of Alcântara (CLA).

The identification and analysis of these conflicts necessarily involves a degree of subjectivity. It is unclear whether two analysts would identify the same issues if they were to independently construct conflict maps based on the same ActorMap and AcciMap. For this reason, it is important that any analysis should be validated. For instance, each of the conflicts mentioned on the right hand side of Figure 4 should be annotated to provide a reference to the available evidence that might support such claims.

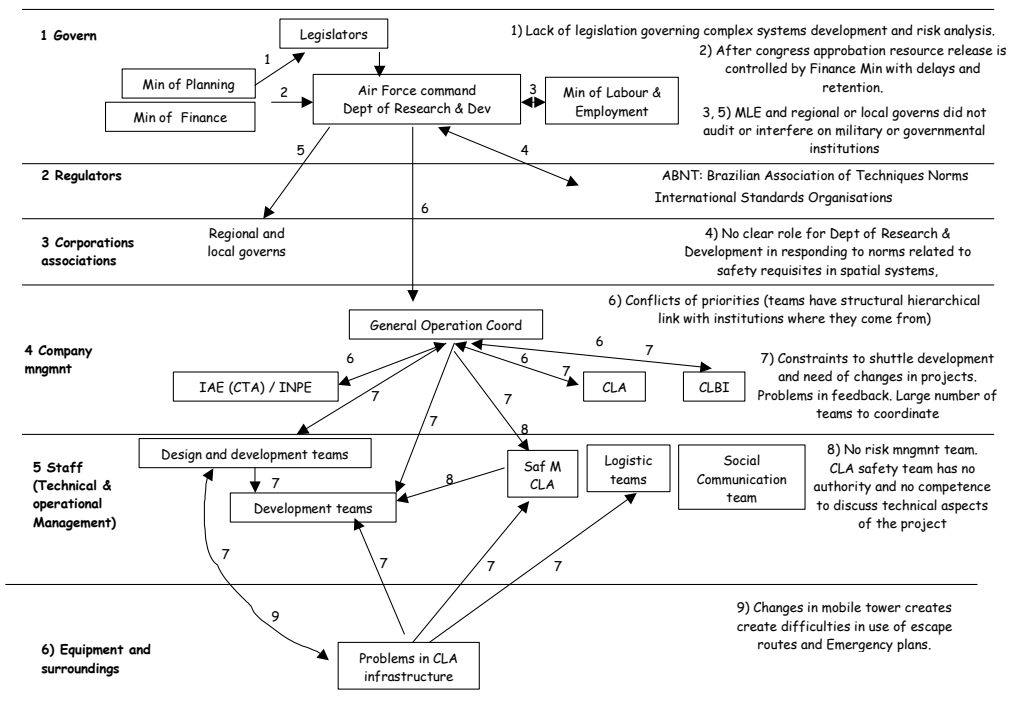


Fig. 4: Example Conflict Map for the Case Study

Figure 4 shows the main actors involved in the accident, based on the initial analysis of the ActorMap. Most of the launch plans were developed in Centro Técnico Aeroespacial (CTA) or the Launch Centre of Alcântara (CLA). However, the report says very little about the role of the General Operation Coordination (GOC) in these activities. It seems clear, however, that the GOC was responsible for controlling many different aspects of the launch. The use of Rasmussen’s conflict map can, therefore, help investigators to identify potentially relevant information that might not be apparent within the documentation that is made publicly available in the aftermath of an adverse event. It is important to emphasise that this does **not** imply specific bias on the part of the investigators. Not does it imply that the General Operation Coordination group were implicated in the events leading to the accident. Instead, we would argue that Rasmussen’s technique identifies the need to explain in more detail the precise role that this important group played in allocating and monitoring the activities of key groups during the launch preparations.

2.4 The InfoFlowMap

Rasmussen recommends additional stages of analysis within his approach. For instance, the InfoFlowMap can be used to chart the transfer of critical information between the entities identified in the ActorMap. This enables analysts to trace the ways in which problems can be exacerbated by lack of critical information or by bottlenecks in the transfer of key facts during an adverse event. In Rasmussen & Svedung (2000 p 56) the InfoFlowMap is developed using a “connectivity matrix”. This characterises the relationships between information receivers and information sources. After this they represent the flow into the actor map. According to them, “an evaluation of the information flow from a closed loop control perspective is required” (p57). Unfortunately, the information available in the Serviço Público Federal report did not allow us to construct the InfoFlowMap in our case study. This limitation

partly stems from our decision to use publicly available information sources as the basis for our work, so that others can validate our findings. There were also a number of more pragmatic caveats about the feasibility of this approach in practice. Most complex organisations support a mass of explicit and implicit communication channels that can be extremely difficult to reconstruct in the aftermath of an adverse event. Concerns over blame, responsibility and litigation frequently complicate the investigation of these social and organisational processes.

3. Leveson's Systems Theory Accident Modelling & Process (STAMP)

As mentioned, a primary objective in this paper was to determine whether a number of novel analysis techniques could be applied to represent and reason about the causes of an adverse event in the Brazilian aerospace industry. Rasmussen's techniques were selected because they focus on the interaction between different levels in a socio-technical system. Leveson's Systems Theory Accident Modelling & Process (STAMP) has a similar motivation. However, it adopts a very different approach based on elements of control theory. Mishaps occur when external disturbances are not adequately controlled. Similarly, adverse events can arise when the failure of process components goes undetected or when the actuators that might respond to such a failure are unsuccessful in their attempts to control any adverse consequences from the initial fault. Control failures can also arise from 'dysfunctional interactions' between system components. For example, if one subsystem embodies inappropriate assumptions about the performance characteristics of another process component. In this view, mishaps do not stem from events but from inappropriate or inadequate constraints on the interactions among the elements that form complex, safety-critical applications. Safety is viewed as a dynamic property of the system because the constraints that are applied and the degree to which a system satisfies those constraints will continually evolve over time.

3.1 The Control Model

Figure 5 illustrates one of the ways in which Leveson has developed the ideas that motivate the STAMP approach. This diagram illustrates elements of control theory. Automated controllers use sensors to detect properties of the controlled process. In a process control system, these sensors might provide pressure readings or changes in temperature. Control systems can then use actuators to intervene and produce some change in the process. For instance, a catalyst might be introduced to excite a chemical reaction. The sensors can then be used to determine whether or not the actuators have helped to achieve the desired outcome. As mentioned in previous paragraphs, mishaps can arise from sensor or actuator failure or from problems with process inputs. There may also be external disturbances that can affect production processes.

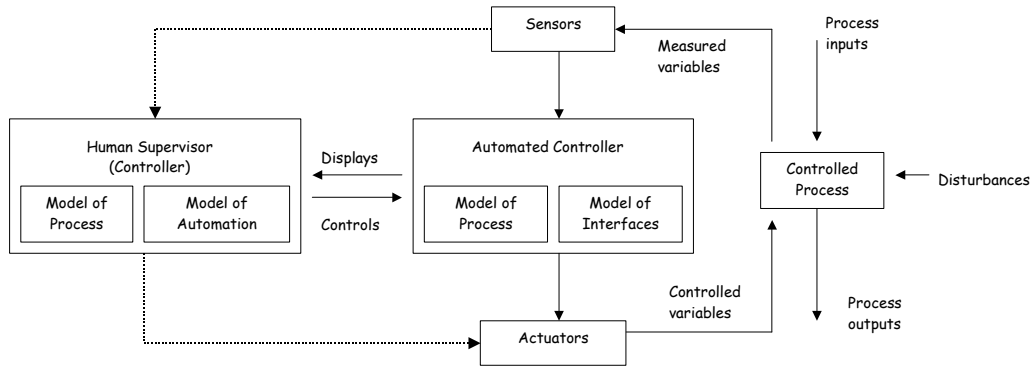


Fig. 5 High-level Elements of a Control Model

Figure 6 illustrates the results of applying the STAMP control modelling technique to aspects of the VLS-1 VO3 accident. As can be seen, this model does not explicitly represent the sequence of events leading to the accident. This is an important strength of the technique because it encourages analysts to focus on organisational and managerial factors rather than the immediate catalytic events that are usually associated with system operators. Unlike Rasmussen’s ActorMaps and AcciMaps, however, STAMP does not enumerate the different levels that are to be considered within a control diagram. It is difficult to be sure whether this additional support in Rasmussen’s approach is necessary or overly restrictive. Our experience in modelling the case study is that the six levels from equipment and surroundings up to government policy and budget did help us to look for additional actors in our analysis. This structure might, therefore, usefully be added to the STAMP control model. Informally, we found that our development of the control model had string parallels to the ActorMaps illustrated in previous diagrams even though they were developed independently.

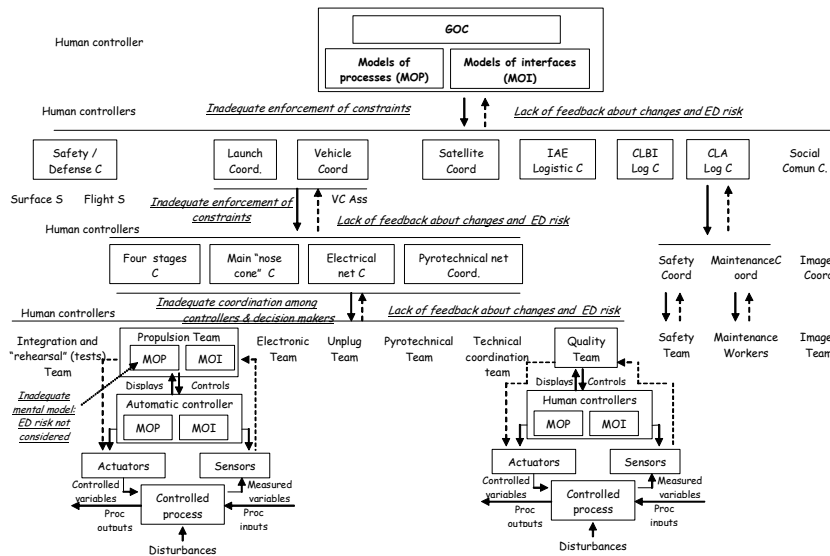


Fig. 6 Control Diagram of General Operation Coordinator in the VLS-1 V03 Accident

As can be seen in Figure 6, the bottom level shows the actors involved in the process including the controls loops between the different hierarchical levels (Leveson 2004, Leveson et al 2002). The Serviço Público Federal did not focus directly on the individuals in each work group. Hence, at the lowest level the control model represents the team structure during the launch operation. This diagram also abstracts away from both the formal and informal communications mechanisms that must have existed at these lower levels. The official documentation into the incident does not describe these in any detail. However, it seems likely that the large number of different teams may have caused some coordination problems in the lead-up to the accident.

Figure 7 extends the previous control model to include information about the role of higher-level organisations in creating the preconditions for the VLS-1 VO3 accident. It places the role of the General Operation Coordinator activity of the Sao Luis operation within the wider context of the Air Force command structure in Brazil. It also, in turn, shows how they were potentially influenced by congressional policy and budgetary constraints. As mentioned, this extended control model resembles the ActorMaps in Rasmussen's earlier approach because it focuses attention on wider aspects of the socio-technical systems that are involved in an adverse event.

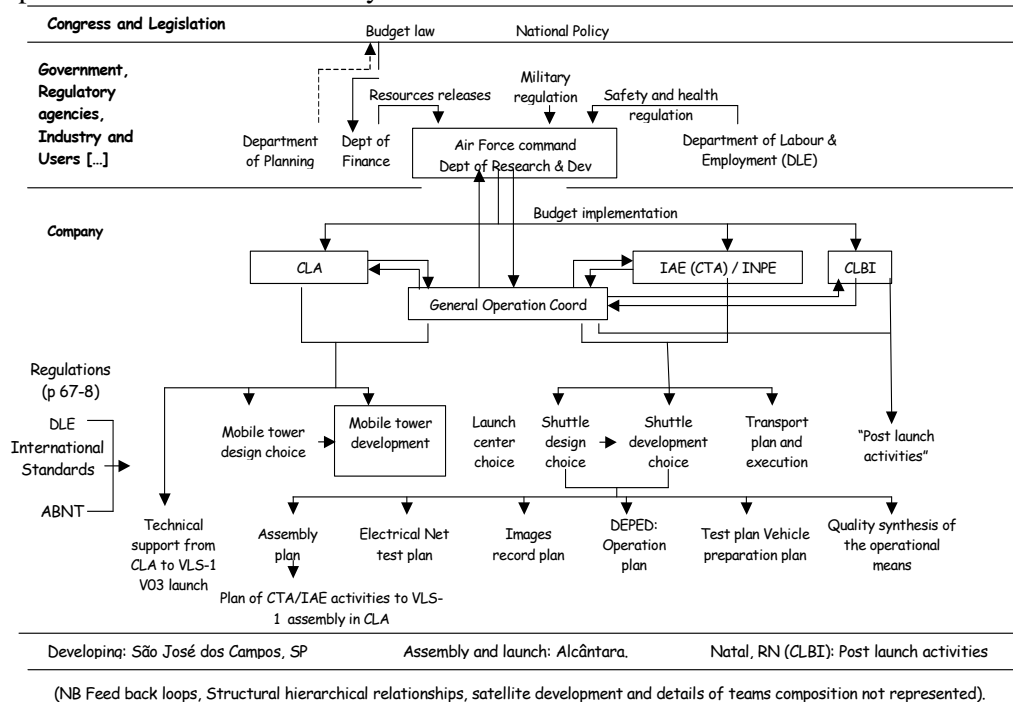


Fig. 7: STAMP Control Analysis

The official reports contain little information about the particular make-up of each team. In particular, few details are provided about the composition of mixed teams where workers were drawn from the Centro Técnico Aeroespacial (CTA) and the Launch Centre of Alcântara (CLA). The lack of information about the composition of the different teams, about workers origins and about interrelations among the teams during launch preparing is reflected in the bottom levels of figures 6 and 7. It can only be inferred that the large number of teams from several different institutions may have

had contributed to the incident. However, these details are not included because such information would rely entirely on speculation.

This introduced an important caveat both about our work and that of the Brazilian investigators. It can be argued that both Rasmussen's approach and Leveson's STAMP techniques should be used in a normative manner. This would imply that omissions such as the one mentioned above should be rectified to address important deficiencies in the existing analysis. However, a number of practical caveats can be raised about this line of argument. As mentioned, many of the communications flows between working groups are seldom documented. In the aftermath of an adverse event, it would be difficult to obtain post hoc evidence to support such inferences especially when many of the individuals involved were either dead or injured. It is for this reason that Figure 7 does not include these control relationships and instead focuses on those that could be documented by the Brazilian teams in the aftermath of the VLS-1 VO3 accident. Traditional forms of accident analysis did not focus on these aspects of system activity. If analytical techniques, such as STAMP, were more widely adopted then it seems likely that this information could be gathered. It would, however, require considerable investment in training investigation teams to elicit sensitive information about implicit control structures and feedback loops.

The development of the control model illustrated in Figure 7 can also help to expose further areas for clarification in the official documentation. Many of the teams listed in the lower levels of the STAMP control model are assumed to belong to the Instituto de Aeronáutica e Espaço and to the Centro Técnico Aeroespacial. However, there may have been teams working on the safety aspects of the mission that were not directly drawn from these organisations. This uncertainty is compounded by several changes in the composition of the teams working on the launch. During the lead-up to the accident, the Launch Centre of Alcântara (CLA) team was reduced. In consequence, the Instituto de Aeronáutica e Espaço and the Centro Técnico Aeroespacial seconded staff to support the work. According to the Report without sufficient financial and human resources, the Launch Centre of Alcântara was not in a position to coordinate the launch and satisfy the rules and regulations governing their operations.

The development of the STAMP control model also highlighted an issue that had arisen in previous applications of this technique. For instance, one of the co-authors had previously worked on a NASA project to apply this technique to analyse problems with the SOHO satellite mission (Johnson and Holloway, 2003). During this incident, several meetings were postponed or not held that might otherwise have acted to prevent or mitigate the failure. It was difficult to represent these omissions in the STAMP diagram because the focus is on representing relationships that exist between key groups involved in an adverse event rather than on representing groups and control relationships that did not exist. In the VLS-1 VO3 incident, it is difficult to identify the team that was responsible for coordinating mission risk assessment. These critical tasks and responsibilities might have been distributed to the various teams shown on Figures 6 and 7. Another group might also have shared these duties with other functions at a higher level in the control model. In either case, extensions have been proposed to the STAMP control models so that analysts can explicitly represent the individuals, teams and systems that are not mentioned in the official

documentation but which could have played a significant role in the course of an adverse event (Johnson and Holloway, 2003).

3.2 Constraint Analysis

Figures 6 and 7 show how the STAMP control analysis can be extended upwards from the operator, the control system and the production process to consider the relationships between project and company management, between management and regulatory agencies and between regulation and legislature. These different relationships must be captured in any analysis because they have a profound influence on both the development and operation of safety-critical systems. After having conducted this extended form of control analysis, the STAMP technique progresses by considering each of the control loops that are identified in the ‘socio-technical system’. Potential mishaps stem from missing or inadequate constraints on processes or from the inadequate enforcement of a constraint that contributed to its violation. Table 1 illustrates the general classification scheme that guides this form of analysis. It provides a classification scheme that helps to identify potential causal factors in the control loops that exist at different levels of the management and operation hierarchy characterised using diagrams similar to that shown in Figures 6 and 7. Leveson (2002) points out that the factors identified in Table 1 can be applied at all levels, however, the interpretation will differ. For instance, a failure in a sensor to provide the operator with information when they need it can be classified as a time lag leading to inadequate feedback. Similarly, the same classification can be used to describe the failure of company management to provide adequate information about a potential hazard to senior company executives.

<p>1. Inadequate Enforcements of Constraints (Control Actions)</p> <p>1.1 Unidentified hazards</p> <p>1.2 Inappropriate, ineffective or missing control actions for identified hazards</p> <p>1.2.1 Design of control algorithm (process) does not enforce constraints</p> <ul style="list-style-type: none"> - Flaws in creation process - Process changes without appropriate change in control algorithm (asynchronous evolution) - Incorrect modification or adaptation. <p>1.2.2 Process models inconsistent, incomplete or incorrect (lack of linkup)</p> <ul style="list-style-type: none"> - Flaws in creation process - Flaws in updating process (asynchronous evolution) - Time lags and measurement inaccuracies not accounted for <p>1.2.3 Inadequate coordination among controllers and decision makers</p> <p>2 Inadequate Execution of Control Action</p> <p>2.1 Communication flaw</p> <p>2.2 Inadequate actuator operation</p> <p>2.3 Time lag</p> <p>3. Inadequate or Missing Feedback</p> <p>3.1 Not provided in system design</p> <p>3.2 Communication flow</p> <p>3.3 Time lag</p> <p>3.4 Inadequate sensor operation (incorrect or no information provided)</p>

Table 1: Control Flaws Leading to Hazards (Leveson, 2002)

In past case studies, the outcome of this form of constraint analysis has been represented either in prose format or using a tabular notation. These tables use different columns to denote the actors involved in the control relationship as well as the particular type of control flaw extracted from Table 1. In contrast, Figure 8 shows a more direct approach in which these problems are represented on the control model derived from the previous stages of the analysis. This technique is only

tractable during a preliminary analysis and text-based alternatives or tool support would be necessary for any more sustained analysis. These approaches are illustrated in Johnson and Holloway (2003).

<p>1) Inadequate enforcement of constraint</p> <p>1.1. Unidentified hazard:</p> <ul style="list-style-type: none"> • Electrostatic discharges. There's no control loop to this risk. <p>Reasons:</p> <ul style="list-style-type: none"> • Inadequate mental model: The report describes some problems in team's safety education. • Inadequate control algorithm: There's no control loop to electrostatic discharge risk. • The context in which decisions and actions took place. <p>1.2. Inappropriate, ineffective, or missing control actions for identified hazards.</p> <ul style="list-style-type: none"> • Flaws in creation of risk management control loop and to consider complexity management. • Lack of enforcement to respect original design leaving to change without feedback to GOC: Operational team substitutes armoured wires present in original design for non-armoured wires (without communication to GOC). • Process change without appropriate change in control algorithm. Failures in material supply, probable originated in resourcing problems, did not accompanied for changes in control algorithm. Delays in activities in the morning of the accident pushing changes in scheduled sequence of activities without controllers' detection. • Flaws in updating process: The General Operation Coordinator did not identify change (use of non-armoured wires) in original design. It was present during almost 4 years up to the accident. <p>1.3. Inadequate coordination among controllers and decision makers (boundary and overlap areas)</p> <ul style="list-style-type: none"> • Changes in the sequence of activities in the morning of the accident influencing others teams activities. <p>Reasons:</p> <ul style="list-style-type: none"> • Inadequate mental model. For example, people did not understanding the use of separation in time as a safety measure and did not considering the possibility of tightly coupled interactions after detonator connection. • Inadequate control algorithm. Lack of enforcement to maintain the separation in time. The lack of information about the design of control algorithm prevents us to complete the analysis. • Coordination among multiple controllers. Possibility of responsibility overlap. Degrees of freedom of the lower levels team not clearly established. • The context in which decisions and actions took place: work delay, time pressures, several teams working simultaneously, etc.
<p>2) Inadequate execution of control action</p> <ul style="list-style-type: none"> • Communication flaw. Analysis is incomplete but Official investigation describes top-down emphasis.
<p>3) Inadequate or missing feedback</p> <ul style="list-style-type: none"> • Communication flaw: operational level did not inform about the change of wires.

Table 2. Some possible control flaw leading to hazards in VLS-1 V03 accident.

Table 2 shows a partial example of the STAMP constraint analysis applied to the VLS-1 V03 accident. As can be seen, this classifies key attributes of the accident according to Leveson categories of control flaws. As mentioned, this is a partial analysis. We have classified only aspects related to the activities of the General Operation Coordinator and of teams involved in some actions considered critical to the accident. One of the most prominent aspects is the absence of a control loop related to the management of the electrostatic discharge risk (1.1). The table also shows flaws in the creation of a risk management control loop. The formal organization of this activity is not clearly described in the Report, but it includes a list of failures in this aspect of the overall 'safety system'.

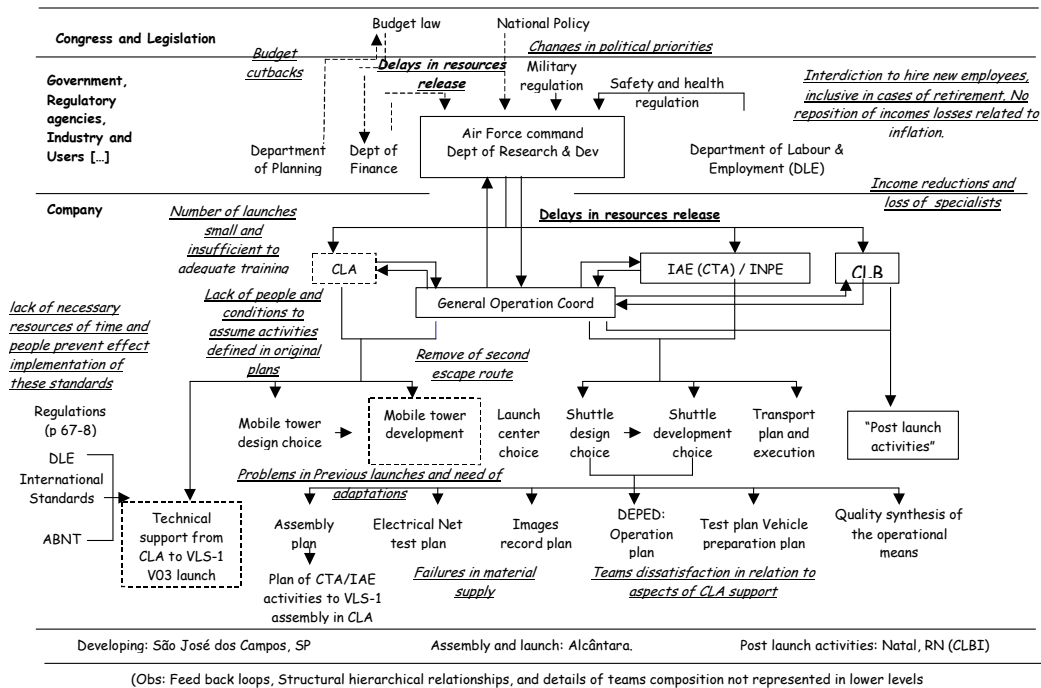


Fig. 8: STAMP Constraint Analysis of the VLS-1 VO3 Accident

Figure 8 captures some of the political and financial constraints on the project. The report gives little information about the way in which these constraints affected particular technological or operational decisions. For instance, the official documentation describes a number of human resource problems that increased the staff turnover in the Centro Técnico Aeroespacial. In addition, a significant number of staff that was involved in the previous stages of the programme retired as their terms of service expired. The official documents make it clear that this had knock-on effects for the Launch Centre of Alcântara. Staff had to be moved to cover for their colleagues. It became increasingly difficult to support these transfers and to plan for their integration with existing teams. It is less easy, however, to map from these general observations to specific technical failures.

One possible explanation for the difficulty of mapping between organisation and technical issues is that the origins of many operational decisions stretch back more than 20 years. Figure 8 represents a snapshot of the control relationships and organisational constraints that affected this project. Particular operational decisions may originate from different control structures that held at previous stages in the project. This trajectory of control structures is further complicated by the observation that the loss of VLS-1 VO3 was the third major accident in this programme. These different events acted as important catalysts for decision making in the development of the VLS-1 VO3. They affected both explicit control structures, such as those shown in Figure 8. However, it also seems clear that they also affected a number of implicit relationships and information flows both between and within the various organisations in the aftermath of these previous investigations.

The previous diagrams illustrate an important aspect of both STAMP and Rasmussen's approach. They each emphasise the need to consider changes and adaptations that occur after a system has been operating for a period of time. This form of analysis often highlights the differences between intended modes of operation at design time and actual operating practices observed once a system has 'gone live'. The comparison of figures 7 and 8 allow us to identify some of these changes and adaptations in what Rasmussen terms the 'migration towards an accident'. For instance, in Figure 8 the dotted rectangles are used to denote aspects of the system that underwent significant changes in the lead-up to the accident. The design of the mobile tower was originally developed with two escape routes. However, this plan had to be revised when one of the failed after deployment. Similarly, the technical support available from the launch site never met the levels that were intended in the original programme plans.

4. Comparisons Between the Analytical Techniques

The previous sections have provided an introduction to the use of Rasmussen's accident modelling techniques and to Leveson's STAMP approach. We have used the loss of Brazilian VLS-1 VO3 to illustrate the discussion. The intention has been to identify areas in which these different techniques might need to be developed or extended to support the analysis of adverse events in operational and regulatory conditions that are different from those in Europe and North America. We have also identified a number of more generic strengths and weakness for these two accident analysis techniques.

The following paragraphs build on the initial sections of this paper to make a number of more detailed observations from the use of STAMP and Rasmussen's analysis to examine the VLS-1 VO3 case study. These include specific insights into this incident that were arguably less apparent from the official documentation. They also include a number of issues that were difficult to represent in both of these approaches and that were emphasised in the Official Serviço Público report.

4.1 Complex, Dynamic Management Structures

Arguably the greatest benefit of both of the analytical techniques presented in this paper is that they provide means of visualising complex organisational structures. These visualisations can then be used to focus subsequent analysis on critical aspects of an adverse event. Both of the approaches offer different strengths and weaknesses. For example, STAMP arguably provides the clearest means of representing and reasoning about the generic relationships between the key actors in an incident or accident. Rasmussen's approach provides greater support for analysing the propagation of events between different levels in a management hierarchy. In spite of these differences, however, both approaches focus on the central role of budget cutbacks in the lead up to the loss of VLS-1 VO3. Delays in the release of necessary resource releases and political constraints both affected mission management at key stages in the lead-up to this accident.

The STAMP analysis and the ActorMap can also be used to identify the 'double' control structures that affected many of the teams involved in this incident. As mentioned previously, many individuals had to be seconded by the Instituto de Aeronáutica e Espaço and the Centro Técnico Aeroespacial to support the Launch Centre of Alcântara. The General Operation Coordination group is shown by both

the ActorMap and the STAMP control models to play a key role in negotiating between these institutions to obtain the necessary permission to send a technician in support of the launch activity. However, these secondments created two reporting structures for individuals who were temporarily working within a mission group, providing functional services, but who also considered themselves to be working for another host institution, providing a structural relationship.

4.2 Vertical Rather than Horizontal Reporting Structures

The AcciMaps in Figures 2 and 3 as well as the conflict diagram in figure 4 all seem to accentuate the vertical rather than horizontal relationships between the groups involved in this accident. Similarly, the control models in Figures 6, 7 and 8 also focus in on the reporting structures between groups at different levels in the hierarchy. It is difficult to be certain whether this focus on vertical reporting mechanisms is an artefact of the particular analytical techniques that were used, of the particular VLS1-VO3 case study or of the investigators. However, the resulting diagrams are similar to those produced in other case studies (Johnson and Holloway, 2003).

There is some evidence in the official documentation to suggest that considerable resources were invested in vertical communications channels. During the lead-up to the accident the number of diary meetings held by middle management in the Launch Centre of Alcântara was increased from two to three per week so that messages could be passed back between the different groups in each of the functional areas. Interviews were conducted with employees after the accident. According to many of the individuals involved, the emphasis in meetings was on top-down communication.

4.3 Financial Constraints

Both the STAMP analysis and the conflict charts within Rasmussen's techniques identified the importance of financial issues in creating the context for the accident involving VLS-1 VO3. Political involvement led to budget cutbacks. These, in turn, led to the loss of specialist support and to interruptions in the schedule. In the aftermath of the incident, several members of staff argued that the programme had not been seen as a political priority and that the impact of these various pressures had been to create additional difficulties in coordinating the launch work programme.

The conflict diagram in Figure 4 shows the way in which delays and retentions may have affected the higher level organisations involved in this incident. The following paragraph discusses the difficulty to adequately representing the direct effects of these constraints at lower levels in the operation of the launch mission. For now it is sufficient to observe that both STAMP and the Rasmussen models illustrate the close relationship between budgetary pressures and high-level political decision-making. The official reports show that between 1980 and 1995 the total resources allocated were less than 50% of those planned for the mission programme. Again this has a strong resemblance to the problems that led to NASA's Mars Global Surveyor mission losses (Johnson, 2003).

Figure 7 also illustrates the role of budgetary cutbacks. This is, however, represented indirectly as a constraint on the Air Force Command, Department of Research and Development. The model is assumed to represent the transitive impact of these financial pressures on the General Operations Coordination group and then on to the individual project teams. It can be argued that this represents a necessary

compromise. However much we might like to directly represent the impact of these governmental and regulatory constraints on the operational staff, it would be difficult to represent every possible influence on all of the groups without creating a diagram that would be difficult if not impossible to use through all of the redundant interconnections.

4.4 Local Government and External Oversight

Both of the analytical techniques used in this paper help to identify the apparent lack of involvement from local government and from external agencies during the lead-up to this accident. For instance, the conflict map in Figure 4 shows the Ministries of Planning, of Finance and of Labour and Employment as the only outside influences on the Air Force command structure. However, the Labour and Employment Ministry was not responsible for performing detailed audits on the operations and procedures in military or other federal institutions. In practice, of course, there are likely to be a myriad of other influences but these are prominent in the official accounts of the incident. This caveat also illustrates a further benefit of the graphical formalisms introduced in this paper. They provide a valuable series of communications tools that can be shown to other analysts and thereby validated in case there are significant omissions in their representation of an adverse event.

Figure 7 illustrates the higher-level influence of external agencies as part of the STAMP control model. In particular, it indicates the influence of international standards relating to operational quality management. It also indicates the impact of the guidelines provided by the Brazilian Technical Norms Association. This raises an important issue in the development of any STAMP analysis. In particular, although Figure 7 illustrates these outside influences, the limited impact of these regulations is not made apparent until the subsequent constraint analysis. According to the investigation team there were problems related to the record of changes in project and development (p 71); problems in documents elaboration, changes and documentation control (p72), and problem in configuration management (p 72). It is for this reason that we have directly annotated Figure 8 so that readers can identify constraint flaws from the control diagram. Next to the annotations illustrating the potential impact of external standards and the Brazilian Technical Norms Association is the comment 'lack of necessary resources of time and people prevent effect implementation of these standards'.

4.5 Identifying Omissions

The official accident report provides a rich source of information about the VLS-1 VO3 accident. The investigation team tested several hypotheses, used different techniques for data collection and actively encouraged the participation of external organisations. The associated enquiry explored many broader aspects of the Brazilian space program. The analysis helped to identify a large list of recommendations. However, the different analytical techniques introduced in this paper can be used to identify areas for further investigation. For example, Rasmussen's AcciMaps and conflict diagrams are intended to identify the ways in which complex socio-technical interactions help direct the 'migration' towards an accident. These analytical techniques are intended to encourage investigation teams to look for environmental changes or adaptations that make adverse events more likely to occur. An important element of this analysis is to ask what were the cognitive precursors to the decisions identified in the AcciMap or to the potential

disagreements in the Conflict Map. Figure 2 provides an example of this additional form of analysis based on elements of an AcciMap. This diagram includes the observation that project management accepted the removal of a mechanical subsystem in favour of a relay module that was intended to provide short circuit protection for the detonators. This is represented by the rectangle labelled as '9. Withdrawal of possible protection and change decided at operational level' in Figure 2. The official reports into the VLS-1 VO3 incident provides very few details about the decision making process that led to the withdrawal of the safety device. We do not know the precise reasons for the replacement nor do we know the processes of validation and verification that supported this decision. The same is true also for the use of non-armoured wires. Similarly, few details are provided about the reasons why armoured wire was not available in key areas of the launch vehicle. The key point here is that Rasmussen's technique not only confirms the considerable achievements of the official investigation team, it also highlights a number of areas for further investigation. The following paragraphs extend this analysis by identifying a number of further omissions that were identified during our application of Rasmussen's approach and the STAMP technique to the VLS-1 VO3 accident.

4.5.1 Omissions of Key Actors

A key objective behind the ActorMaps in Rasmussen's approach and the control model in STAMP is to identify the "players in the social system that interact to shape this [the causal] topology and to understand the forces that drive their efforts to succeed individually during normal work, e.g. in response to be locally cost-effective" (Svedung & Rasmussen 2002, p 403). In the case of Rasmussen's approach this analysis can, in turn, be used to identify critical decisions made by key 'players' at various levels in the organisation. In STAMP, subsequent analysis can be used to trace the constraints that affect individuals and groups involved in an adverse event. Unfortunately, it was difficult to identify all of the key players and the relationships between them from the information available in the official reports.

As mentioned these analytical techniques help investigators to look beyond the immediate events of particular individuals to focus on the managerial and organisation aspects of this mishap. For instance, the AcciMap in Figure 3 traces the decision to synchronise various activities back to the work of a risk management group. In particular, their vigilance helped to develop plans that would minimise the number of staff working in the launch tower after the detonators had been armed. However, some of the elements of these high-level diagrams can be misleading. For example, there was only one "safety technician" who had very limited access to other sources of engineering or professional guidance. The official report indicates that there was only minimal risk assessments conducted after the initial development phase. Hence, it was difficult for staff involved in particular operational decisions to identify the potential hazards that might arise as pre-existing plans began to be revised.

4.5.2 Omissions of Important Functions

The various analytical techniques in the approaches proposed by Rasmussen and by Leveson help investigators to probe behind the individuals and teams that are involved in an adverse event. In particular, the control model in STAMP and the AcciMap in Rasmussen's approach can be used to look at the functions and constraints that applied to various actors. For example, Figures 4 and 6 show how integration and assembly phases involved many different teams and workers.

However, these diagrams arguably provide few clues as to the quality of interaction between these various groups. They do not explicitly represent the unexpected interruptions, delays in one or several activities, the large number of components and activities, problems in components adjustments or quality of materials, climatic changes, fatigue, psychosocial aspects including the problems of working away from home in difficult conditions, etc. These factors can be considered during subsequent stages of analysis, for instance as part of the constraint modelling in STAMP. However, our experience in using these techniques was that there was little explicit support for the identification of these factors that can have a critical impact on the course of an accident or incident. For instance, it can be difficult to identify the increasing time pressures and anxiety that many individuals reported in the final three days before the scheduled launch of the VLS-1 VO3. The official investigation focussed on the failure to adequately identify potential risks associated with rescheduling key tasks after the detonators had been armed. They also recommended improvements in quality management; “all tasks should be planned and systematically evaluated in relation to their degree of risk and compatibility with others tasks [to] avoid unnecessary exposing to potential hazards” (p 67).

The issue of risk assessment raises a number of further caveats about the analysis presented in previous sections of this paper. The Serviço Público reports state that the risk evaluations in the assembly and integration phases were largely ‘subjective’. They lacked grounding in quantitative techniques. Further problems stemmed from the different criteria that were used to determine acceptable level of risk, for instance in order to permit access to the launch platform. Classic probabilistic risk analysis was not used to calculate accepted levels of risk. In particular, there were few feedback loops to “manage the real process” by comparing the frequency of observed events with any of these previously ‘accepted’ levels. In Brazil, in general, there can be a reticence to discuss or consider the hazards, especially technical issues that might threaten the operation of complex, safety-critical systems. The CLA safety team was also reduced to one “safety technician” and most of his attention had been directed towards the use of personal protective equipment and the existence of fire extinguishers rather than providing operation feedback on wider ‘systemic’ hazards.

4.4.3 Omission of Decision Making Processes

As mentioned previously, the two analysis techniques in this paper both helped to identify funding issues as a central problem in the loss of VLS-1 VO3. Several of the preparation teams had lost key members of staff and the plans for hiring additional workers were never implemented. The lack of resources also led to interruptions in the assembly and integration schedule. Both STAMP and Rasmussen’s approach also helped to focus on the decision to connect the detonators before much of the other scheduled work on the launch vehicle had been completed. This is illustrated by the rectangle labelled ‘22 Activity planned to be separated in time had been inverted in sequence’ in the AcciMap of Figure 3. It was also inferred as a potential constraint problem in the relationship between the launch coordination group and the various teams working on the platform in Figure 6.

As in previous paragraphs, it is possible to raise a number of caveats about the support provided by these two techniques. Neither approach can easily be used to model or analyse the detailed events leading to the loss of the launcher. For example, two daily meetings were usually scheduled at the start and the end of each day’s work on

VLS1 VO3. The chief of Vehicle Planning and Control used the first of these daily meetings to distribute written information about the activities for the next 24 hours to each of the team chief. In turn, they used these meetings to provide feedback and hand-in completed progress forms about the previous day's work. The meeting at the end of each day was used to plan future activities and to discuss any problems that had arisen. Immediately before the planned launch, this pattern was changed to three meetings per day and the participants were widened to include individuals from Launch Centre of Alcântara and the CTBI. The official investigation team criticised the record keeping during these meetings and the lack of effective planning in relation to the "risk interfaces" (p 69).

The key point here is that although both approaches help to identify the importance of key decision-making groups on the course of an adverse event, they provide little guidance for any subsequent analysis that might examine the reasons why those groups acted in the manner that they did. For instance, the official reports argue that confused decision-making stemmed from cultural characteristics of the teams involved. It was also argued that they underestimated the risks associated with their decisions, partly because a previous period without accidents had contributed to a sense of over-confidence. The official investigation conceded that if the individual tasks had been isolated activities then the risks would not have been as great as they were. However, the decision to arm the detonators before the other preparations had been completed left many more people exposed to the potential hazards than would otherwise have been acceptable.

The official report identifies similar instances in which workers had been exposed to unnecessary risk. There were other problems in the planned sequence of activities on the morning of the accident. A number of hazardous activities had been planned for the previous night when there were few staff in the mobile tower. Delays forced them to be rescheduled for the morning of the accident. Hence it can be argued that any analysis of this incident must consider the wider "*style of work* adopted by actors, a kind of working culture depending on factors such as 'cognitive style' and 'management style'" (Rasmussen & Svedung 2000, p 60). However, we found it difficult to represent and reason about these more detailed issues using STAMP or the Rasmussen approach. This should not be surprising. Few accident analysis techniques provide this level of guidance (Johnson, 2003). It is also important to stress that the official reports provided no specific information about the content of these daily meetings. It can, therefore, be hard to validate the Serviço Público Federal's criticisms about the limited forms of risk assessment that were conducted prior to the decision to arm the detonators. We cannot tell whether the various teams had considered the hazards associated with having so many co-workers in the launch tower after this critical decision. Similarly, we cannot be sure whether or not anyone who was involved in the original risk assessments actively participated in these daily-planning meetings.

4.4.4 Omission of Historical Information

There are several areas in which our independent analysis of the VLS-1 VO3 incident raised questions that were not answered by the official investigation, or by the analytical techniques that we examined. In particular, the technical decisions leading to this accident seemed to be closely entwined with the earlier loss of VLS-1 VO1 five years earlier. As mentioned, this previous mishap led to the decision to remove

the mechanical safety devices on the detonators. The official reports identified an electrostatic discharge as the most probable immediate cause of the VLS-1 VO3 accident hence they argued that the accident might have been avoided if this protection had been retained. The official report criticises the decision of the previous board and argued that it was the result of risk 'underestimation'. However, this form of reasoning can also be ascribed to hindsight bias. It is unclear whether had anyone would, or should, have reached another decision had they possessed the same information that was available following the loss of VLS-1 VO1.

The official report's scepticism about the results of the earlier investigation raise numerous questions. In particular, it is unclear whether we have any additional assurance that the recommendations made in the aftermath of this accident might not also suffer from the problems of 'risk underestimation'. There are few details about the investigation of the VLS1 VO1 failure; hence it is difficult to be certain that the more recent investigation is immune from the previous problems. Similar comments can be made about the decision not to use armoured wire within critical subsystems of the launch vehicle. We do not know enough about the previous decision making processes to be sure that future plans will be more resilient to mission failure.

5. The Brazilian Dimension

The previous paragraph identified a number of important contextual factors that cannot easily be represented in the analytical techniques that were introduced in this paper. The dominance of subjective risk assessment techniques and the lack of feedback mechanisms to calibrate more quantitative approaches are first class concerns, both from our analysis of the incident and that of the official investigators. There are further issues that are arguably less significant in the course of the accident but that also had an impact on individual commitment and behaviour in many different teams of co-workers. In particular, the assembly and launch phases of the VLS-1 VO3 took place in Alcântara. This is in the centre-west region of Brazil. It is a long way from many of the population centres from which the engineers had to be seconded. These teams had to be transported; installed, and live for a period outside of their own homes and towns.

The dislocation of technical staff not only had social and personal consequences, which are often overlooked in incident investigations. It also, arguably, had technical consequences on the transfer of engineering knowledge between and within the teams. Over 50% of the Instituto de Aeronáutica e Espaço (IAE) and Launch Centre of Alcântara (CLA) mission personnel had not been involved in the VLS1 VO3 mission at Alcântara before the launch phase. In other words, they had not visited the region during the first phase of booster integration, nor had they participated in the initial integration inside the tower.

Our analysis identified further insights into the technical management of the Brazilian space programme. The official report argued that many of the engineers involved in the development and launch preparations for the VLS-1 VO3 lack any formal education in safety management. The Launch Centre of Alcântara's safety team only had one technician. There was no 'Safety Engineer' in the team. However, we cannot simply assume that this accident would have been avoided if the Brazilian engineers had received a more sustained grounding in safety analysis. Similarly, it cannot be argued that the provision of additional safety engineers would have made major

changes in risk management within the launch centre. It can be argued that some areas of the Brazilian programme had not recognised the importance of safety management systems, such as those recommended in the North American and European space industries (Johnson, 2003). The official report argues that the development of an appropriate 'safety culture' received relatively little attention. Constant reviews, external audits and expert validation for risk assessments were all missing.

The official report into the loss of VLS-1 VO3 described a number of previous failures within the programme, including the loss of VLS-1 VO1. A common theme between each of these incidents and accidents is a failure to manage complexity under difficult circumstances. Several of the causal aspects identified, including component failures; lack of material supply, delays, inadequate human resources, forced the General Operation Coordination (GOC) together with the individual work teams to make numerous small adaptations to their work processes. Alternative resources had to be found, daily optimisations had to be made to previous plans and so on. In all these situations the control process between the different hierarchical levels of the socio-technical system, and in particular communication, assumes a critical role. It seems that a critical aspect in this case was the development of an adequate system of control of changes.

At one level it can be argued that our analysis has identified problems in extracting the information that is necessary to apply these different analytical techniques from the official documentation. For instance, the reports focus on the actions of workers involved in the events immediately before the detonation rather than on the more detailed events leading to the latent causes, such as problems in supply armoured wire or the scheduling issues that led to increased number of workers being employed on the site after the wiring of the detonators. Although there are some references to these latent causes, there are even less references to the workers involved in preparations outside the tower. Similar comments can be made about the other end of the organisational structures embedded in STAMP control models and the Rasmussen's ActorMaps. It is difficult to determine the role of the Department of Research and Development of the Air Force Command in the lead-up to accident. Similarly, the official reports do not consider in detail the relationship between the General Operation Coordination (GOC) and the organisations that provide its membership, including the Centro Técnico Aeroespacial (CTA), the Instituto de Aeronáutica e Espaço (IAE) and the Launch Centre of Alcântara (CLA).

It is important, however, to place these apparent omissions within a wider context. There is nothing distinctively Brazilian about these oversights. In particular, previous work on the application of STAMP and similar techniques to the NASA-European Space agencies SOHO mission interruption faced similar problems in tracing the sources of technical decisions back to higher-level organisational structures (Johnson and Holloway, 2003). A previous analysis of the Mars Surveyor'98 missions was faced with several notable omissions and the impact of numerous changes in the management structure during the lifetime of the project (Johnson, 2003). In another domain, a reanalysis of the Milford Haven petrochemical accident helped to identify a number of explicit and implicit control relationships that could not easily be reconstructed in the aftermath of this adverse event (Johnson and Howell, 2004). The experience of applying Rasmussen's models

and the STAMP approach has, therefore, only served to highlight the similarities that arise in investigating complex technological failures across three continents.

6. Conclusions and Further Work

The increasing complexity and integration of many safety-critical systems has made it difficult to trace the causes of mishaps back through the complex interactions that lead to adverse events. At the same time, there has been a growing appreciation that many different contextual factors contribute to incidents and accidents. These different developments are placing considerable burdens on the investigatory agencies in many different industries. A number of regulators, operators and research teams have, therefore, proposed novel techniques to support the analysis of complex, safety-critical failures. Unfortunately, almost all existing applications of these techniques have focussed on the United States or Europe. Relatively few examples illustrate how these approaches might be used to analyse incidents in other working cultures and environments. We have, therefore, used Leveson's STAMP and Rasmussen's accident analysis techniques to re-evaluate the Serviço Público Federal investigation into the explosion and fire of the Brazilian launch vehicle VLS-1 VO3.

A number of methodological problems have affected our work. Ideally, we would have liked to use these methods as part of a contemporaneous incident investigation. Such an approach would rely upon training investigators to exploit the analytical techniques as part of their everyday activities. A number of ethical and organisational constraints prevented us from exploiting this approach. Instead, we were forced to rely on official documentation that was produced during the previous enquiry. We were not permitted to conduct any additional elicitation. In many cases, our application of the novel investigation techniques helped to identify areas of the incident that did not receive sustained attention within the official documentation. In particular, we were keen to clarify the coordinating roles of several groups in the management of the launch site. There were also other aspects of the incident that were not identified by either technique nor were they mentioned directly in the official report but that emerged as key concerns during our discussions of this incident. For instance, we were keen to determine any differences between the validation of recommendations from the investigations into VLS-1 VO1 compared to VLS-1 VO3. Such a comparison might have increased our confidence that any subsequent interventions did not suffer from the same 'risk underestimation' that led to this accident.

Arguably the greatest benefit from using the Rasmussen and STAMP frameworks was that they helped to identify key 'actors' in the accident. Individuals, groups and systems could be placed within control relationships or at different levels in a management hierarchy. This encouraged us to look beyond individual human 'errors' and system 'failures' to look for the latent causes of this incident. The graphical representation of the entire project as a complex system helped to focus on communications issues, especially the need for an integrated risk management strategy. The graphical representations in these different techniques also helped to identify constraints and local adaptations at all levels of the socio-technical system. This can help decision makers of the Brazilian Spatial Program to become aware of the potentially dangerous network of side effects, for instance as a result of decisions to change the financial management of safety-critical projects. The use of both STAMP and Rasmussen's approach also helped us to take a more integrated approach

to the accident. It was possible to map out complex interactions between the various subsystems in a manner that, arguably, was not readily apparent in the documents from the official investigation.

The closing sections of this paper have used this analysis to identify a number of factors that relate very closely to the Brazilian context of this incident. These included geographical, organisational and technical factors. The official investigation identified the way in which financial and political constraints might have affected the perception of work safety over time. Equally there were many other issues, such as communication and coordination failures in multiple teams that are indistinguishable from any other high-technology enterprise on any other continent.

Further work intends to build on the findings that are presented in this study. We have recently completed similar studies of Brazilian accidents in other domains, including railway transportation and the process industries. The intention is to determine whether the similarities that we uncovered in this study were atypical because of the sophistication of the systems being studied. The extreme technical demands of the VLS-1 VO3 launch forced management to use practices and procedures that are common throughout the space industries in many different countries. In contrast, however, the results of our work in other domains have highlighted the strong common features between these Brazilian accidents and 'counterparts' in Europe and North America. One by-product of this work is that we are beginning to identify generic features in the causal analysis of incidents on different continents as a first step in the induction of patterns that might be used to describe wider classes of adverse events around the globe.

Acknowledgement

This study has received financial aid from Fundacao de Amparo a Pesquisa do Estado de Sao Paulo (FAPESP), Brazil, process number 0302475-4.

References

Binder, MCP., Almeida, IM., Monteau, M. Arvore de causas. Metodo de investigacao de acidentes de trabalho. Sao Paulo: Publisher Brasil Editora; 1995.

Hopkins, A. Managing Major Hazards. The Lessons of the Moura Mine disaster. Allen and Unwin, 1999. Sydney.

Hopkins, A. Lessons from Longford. The Esso Gas Plant Explosion. CCH, 2000. Sydney.

Johnson, C.W., A Handbook of Accident and Incident Reporting, Glasgow University Press, Glasgow, 2003.

Johnson, C.W., Holloway, C.M. The ESA/SOHO Mission Interruption: Using STAMP Accident Analysis Technique for a Software Related Mishap. Software – Practice and Experience, 2003; 33:1177-1198.

Leveson N A New Accident Model for Engineering Safer Systems. Safety Science, 42 (2004): 237 – 270.

Leveson, N., Allen, P., Storey, M-A. The analysis of a friendly Fire Accident Using a Systems Model of Accidents. 2002 In: 20th International conference on system Safety.

Rasmussen, J. Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, 1997; 27 (2/3): 183-213.

Rasmussen, J. & Svedung, J. Proactive risk Management in a Dynamic Society. Karlstad, Sweden. Räddningsverket; Swedish Rescue Services Agency. 2000. Monteau, M.

Monteau, M. Analysis and reporting: accident investigation. In International Labour Office. *Encyclopaedia of Occupational Health and Safety* [CD Rom]. Ginebra: International Labour Office; 1999. (Chapter: audits, inspections and investigations, Vol 2 – 57.1 – 57.31).

Serviço Público Federal. Ministério da Defesa. Comando da Aeronáutica. Departamento de Pesquisas e Desenvolvimento Relatório da Investigação do acidente ocorrido com o VLS1-V03, em 22 de agosto de 2003, em Alcântara, Maranhão. São José dos Campos, Fevereiro de 2004. Available in Portuguese from <http://www.aeb.gov.br>

Svedung, J. & Rasmussen, J. Graphic representation of Accident Scenarios: Mapping System Structure and the Causation of Accidents. *Safety Science*, 2002, vol 40: 397-417.

Woo, D.M, Vicente, K.J. Sociotechnical Systems, Risk Management, and Public Health: Comparing the North Battleford and Walerton Outbreaks. *Reliability Engineering and System Safety*, 2003, 80: 253 – 269.