Analyzing Resilience of an Oil Distribution Plant
Marcos P. Abech, Gabriel A. Berg, Michael G. Delis, Lia B. M. Guimarães, and David D. Woods

Abstract — This article presents the opportunities and challenges for improving resilience in an oil distribution plant. The plant is situated in the southernmost state of Brazil, and it distributes fuel products by truck and train. Based on observations and interviews with the people who handle the transfer and distribution process, this paper provides an analysis of how the system is resilient in some ways and brittle in other ways. The research focused on understanding how the system adapts to variations and disrupting events relative to expected conditions. The areas of brittleness are pointers to possible accident scenarios. The resilience analysis identified opportunities to improve how the system adapts to situations that challenge plans and procedures.

I. INTRODUCTION

New demands for productivity and efficiency or the introduction of new technology can change the risks of errors and incidents in an organization. Methods to proactively identify hidden or new risks are needed to help manage change [1]. Resilience Engineering seeks to manage risk proactively by developing methods to measure and enhance the resilience of organizations [2].

This paper presents results from a study of an oil distribution plant based on resilience concepts. During the project, strategies to enhance resilience in the system were developed to minimize the consequences of possible future accidents. The results indicated the need for improved accident prevention and risk control programs and the need to expand the company’s capacity to react to dangerous situations.

There are two main approaches to the treatment of failures. The first is the focus on the human being closest to the failure in terms of the consequences of forgetfulness, fatigue, and other limits to individual performance. The second is to analyze the system factors that lead organizations to miss systemic vulnerabilities or create conditions where errors can occur [3, 4]. In Brazil, organizational safety program and accident analyses continue to see accidents as due to a linear and deterministic chain of events that focuses on how operators err. The belief that most accidents are due to human error and procedure disobedience remains strong [5].

The new challenge is developing the tools to help organizations see how they have created the conditions that can lead to failure without having to wait for serious accidents to occur. It is critical to understand that the label human error is the beginning and not the conclusion of the investigation as suggested by many researchers such as Reason, Rasmussen and Woods [2-3, 6-8]. When this guidance is followed investigations usually reveal a variety of latent factors that eroded defenses and contributed to the failure [3].

Due to the dynamics of the systems, new forms of error and risks can emerge everyday. Strategies that had been effective may be less effective as processes of change and adaptation go on, especially as pressure to be efficient grows. This inherent variability means it is impossible to chase and eliminate all of the latent conditions and holes in a system. Instead, systems approaches to safety management emphasize an organization’s ability to adapt to disturbances, disruptions, and variations. These are properties that characterize the resilience or brittleness of the organization [2, 9].

The objective of this work was to understand the resilience/brittleness of the Depot and to enhance the adaptability of the Depot when events challenge the model of how it should operate. Through an understanding the system in its entirety, individual interviews and observations were combined to discover the holes and gaps in the organization especially when the Depot became busy. While observing the Depot as it ran, it was important to make note of how systems was able to function through the gaps and holes that were in place. Observing how latent factors are blocked from combining into more hazardous situations helps make sources of resilience visible.

It is also important to remain alert to other incidents that occur both within this company and throughout the world. Recent cases, such as the Buncefield fuel depot fire, December 2005, near London, show that apparently small problems can cascade into large consequences.

This paper also will provide background information on
the oil distribution company, the problem definition, and the case study.

II. BACKGROUND

PETROBRAS (Petróleo Brasileiro S.A.) is a state-owned company established in 1953 to run the oil sector in Brazil on behalf of the Federal Government. PETROBRAS is the country’s leader in the distribution of oil products, and also is one of the fifteenth largest oil companies in the world, reaching eight billion dollars of net income per year. PETROBRAS is responsible for more than 90% of the oil extraction in Brazil, and refines the raw oil into five major divisions shown in Figure 1.

Year 2006 is a milestone in Brazil's goal to be self sufficient in oil production. To achieve this, PETROBRAS began a program P-50 FPSO (Floating Production Storage Offloading) operations in the giant field, Albacora Leste, in the northern part of Campos Basin, Rio de Janeiro State. This program is expected to help reach the mark of two million barrels produced per day. This is enough to cover the domestic market's daily consumption of 1.8 million barrels.

BR Distribuidora is an affiliated company of Petróleo Brasileiro S.A. (PETROBRAS), and operates in the commercialization and distribution of oil products in all the national territory. The Depot studied in this paper is located aside the Alberto Pasqualini Refinery (REFAP). BR Distribuidora is experiencing significant changes due to the enlargement and modernization of REFAP’s industrial park, which is increasing its capacity to 10,000m³/day of refined oil. The increase of REFAP’s production increased the demand for transportation of oil products. BR Distribuidora is a distribution system conducted through two transportation terminals: trucks and trains. The spike in demand creates a concern since the Depot needs to adapt and to be prepared for the impact of these changes on the system.

III. PROBLEM DEFINITION

The PETROBRAS Oil Distribution plant is situated in the southernmost state of Brazil, and it distributes refined fuel products by truck and train. REFAP pumps roughly thirty refined oil products to the distribution center through underground pipes, where large tanks collect the products and hold them for filling.

The Depot is divided into three main sections. The back third of the center is a field filled with numerous storage tanks, containing the refined products. The middle third of the center contains the truck filling station, equipped with three platforms and thirty-six stations. This section also contains a maintenance garage, a check-in center, and the administrative building. The last area of the campus is across a narrow section of a highway and contains the railroad filling station. Both the truck and railroad filling stations are supplied by an underground piping network, controlled by a set of manual and electronic valves to control the flow of products to the stations. On average, four hundred tankers and twenty train cars are filled daily at the center’s two main filling stations.

The filling stations are equipped with twenty-two trained operators, eight foremen and fourteen workers that are given the title “operator one.” Sixteen operators (foremen and “operator one”) work daily at the truck refilling platforms section and four operators work on the train platform. Two operators rotate monthly with the other twenty operators to receive their four weeks of yearly vacation. Each operator, except one “operator one” from the trains, is rotated; therefore an operator performs one specific job function no longer than one month. There are, in total, eight sectors in the Depot, each one with different tasks and demands. Most of these sectors are located in the truck section of the Depot, but are not related only to the truck platforms.

The process of filling the trucks involves the truck drivers, as the operators’ main functions are product testing/analysis, supervision of the filling process, troubleshooting. Each truck driver must attend one day of formal training conducted by PETROBRAS, followed by two supervised, hands-on filling sessions. There is a station in the truck platform that also randomly selects trucks for inspection.

The train platform filling operations are performed by a foreman, and three “operator ones.” The platform can simultaneously fill twelve train cars. All of the train station logistics are controlled by ALL (Latin America Logistics), which requires coordination and scheduling with the foreman at PETROBRAS to ensure efficient procedures.

Analyses were performed through employee interviews and through observation of Depot operations over four months. By studying different aspects of the system, it quickly became clear that there were many holes in the procedures. For example, the observations revealed there were many potential communication gaps within the system. These gaps could occur between operators, truck drivers, and operators with their machines. These gaps pose potential risks for accidents and errors. The specific risks and error prone procedures are detailed in the Resilience Applications section of this paper. Signaling is also absent in the system.
Currently, there is no kanban system present within the tuck filling station, signaling trucks when to enter the Depot and when to enter a platform. Signage is incorrect on twenty seven of the thirty six stations, creating a potential hazard in filling a truck with the wrong product. The methods of truck drivers communicating with PETROBRAS employees on site are poorly designed, as technology is not utilized to improve this aspect of communication.

PETROBRAS could not disclose specific accident investigation information due to security purposes, yet it was understood that there is no formal re-creation of accidents or root cause analysis takes place after an event. The studies focused instead on discovering the gaps in the procedures and in the system and on how these gaps were bridged normally [10].

IV. METHODOLOGY OF RESILIENCE ENGINEERING

A system that is resilient has the capability to adapt to handle disrupting events especially those that challenge the base of plans and procedures. As Resilience Engineering grows it developing new tools to assess this adaptive capacity to classes of disruptions. The effort to develop these tools begins by looking at how well plans and procedures match up with the variability and complexities of actual operations [2]. The gap between work as imagined in the plans and procedures and how work is actually practiced provides clues about how the systems has adapted and what factors, such as production pressures and uncertainties, drive the process of adaptation. Understanding how gaps are bridged reveals how the system is brittle and how people in different roles currently adapt to close gaps. Adaptation to unanticipated factors and events is one of the most important tests of a resilient system. Some unanticipated events are rare. But others occur and represent latent contributors either directly or through the local work arounds that develop [2].

When trying to examine the resilience of a system one needs to be able to classify situations or events that threaten a system. Westrum suggests one can start by categorizing situations into those that exhibit: regular threats, irregular threats, and unexampled threats [11]. Regular threats occur often enough for the system to develop a standard response. These regular threats can also be broken down into more exact categories. Internal regular threats occur regularly and are generally not the cause of an extremely terrible error. External regular threats occur frequently enough that they can be expected, but they are more unpredictable and therefore more dangerous because they are originated from some external factors. Irregular threats do not occur frequently enough to be expected. Unexampled events deviate far from what was previously considered in the realm of possibility, and a shift in mental framework is required.

At this stage, possible points of brittleness that could contribute to a major failure have been identified. Possible means to enhance the resilience can then be listed and evaluated. Then decisions about which interventions should be pursued can be determined given resource limits. It is important to monitor any change to look for any side affects which may be introduced by the new additions.

V. GAPS

A major system failure, such as an explosion, will require the combination and occurrence of several smaller related failures to occur. During the analysis of the distributions procedures, processes, and layout, the team discovered a list of gaps within the operations at PETROBRAS. These are points of brittleness which could contribute to start or fail to stop a sequence of events that risk major system failure.

A. Unclear Lines of Sight

There are no clear lines of sight for the operators working in the train filling section of the distribution center. This is important because each operator is responsible for the filling and monitoring of four train cars simultaneously. The filling system currently in place is a manual system without any type of integrated warning system built in. Therefore, the operators cannot monitor two additional filling stations while working directly on the third effectively. Without the proper lines of sight available to monitor all of your train cars at once, a problem could be missed and continue on for a longer period of time.

Implementing a poka yoke system of signals would provide the operator the opportunity to monitor each station quickly and simultaneously from a distance. Counters or filling gauges which monitor the amount of fuel that has been pumped into the train car versus the amount of fuel to be pumped could be displayed in areas that will not block the operator’s line of sight from one train car to the next. Visual controls to indicate normal operating conditions, and information displays could be placed in locations that would allow operators to have at-a-glance-monitoring of all of the train cars from any position on the platform.

B. Overflow and Over Filling

Over filling is a concern in both the train and the truck filling sections of the distribution center. Intuitively, working with oil products and fuel poses many potential hazards, any of which may be involved with a major system failure. Overflow is related to the risk of unclear lines of sight, and solutions mentioned above would also apply. Other possible solutions are discussed below.

---

1 A Japanese term meaning "sign" or "card". It is a system used to signal the need for movement, production, or supply of a unit in a factory.

2 A mistake proofing system that stops production whenever defects or machine malfunctions are detected.
The completion of the installation of DANLOAD into all the truck filling stations would reduce the chance of overfilling. Currently, only half of the stations in the truck platform have implemented the DANLOAD system. DANLOAD is equipped with built-in automation that can detect potential problems and automatically shut down flow to the tank. However, the train system has not implemented any automated system and continues to use the manual filling device. The manual system has frequent breakdowns which make it difficult to keep track of the filling process. These machines have a numeric turning dial that counts down from the entered amount to zero. Sometimes when the machine reaches 000000, it turns over and starts again at 999999 and continues on its way back down to 000000. When this happens, the machine does not shut off and gives the operator a false sense of where the machine is in terms of the filling process. Overfilling has occurred via this sequence of events. These machines need to be a more reliable system for assessing the amount of fuel that has been pumped into the train cars.

C. Improper Grounding

The grounding of the train cars and trucks is performed before each car is filled with fuel. This grounding sequence involves clamping grounding vice to the bottom of the train and on specific locations on the truck. Although this procedure is always carried out, there is no way to determine if a clean and strong ground has been established.

Incorporate some visual indicator that a clean ground has been reached when the clamp is put on the train car. This indicator could be as simple as a light upon the proper grounding. The filling system could also have a mechanism performing tests to make sure a clean ground is established before initiating the filling process. If no clean ground is determined, the process will not continue. This potential solution is also effective during filling, in case the grounding has been lost for one reason or another. The DANLOAD system, according to the operators, has that ability, but does not show if you achieved a clean ground or not. The system was never tested for this kind of problem.

D. Loss of Knowledge

Loss and transfer of knowledge is one of the major problems inside the Depot. Due to the monthly rotation each operator, except the one whom always works on the train, has to leave their current sector to one of the other seven in the Depot. Another paper has described all the advantages and disadvantages of the current rotation system use in the Depot [12]. The Depot does not have updated procedures that are followed by the operator, this causes a problem when they face an event that is not routine. When the operators face any non-routine event, they need to draw on external sources of knowledge. The lack of knowledge build up and transfer from the rotation system is one impediment. Another problem is that procedures often are not up to date or complete and do not provide support for non-routine events.

Mechanisms to expand the knowledge about how to handle non-routine events and to transfer this knowledge to operators who may have to act quickly and under stress are needed. Upgrading the procedure system to include frequently updated information could help collect and transmit knowledge. The change of the current rotation system, as proposed in [12], could help to turn it into a more adaptive system that can form experts on all the Depot’s sectors.

E. Closing the Main Valves in the Trains Platforms

The closing valves are located on the West side of the distribution center in the train filling section. When these valves are closed the flow of fuel products is stopped. The valves should be open only during work hours. However, these valves are difficult to close because a great deal of force is required to perform this action, and closing the valves takes close to four minutes to perform.

If an accident were to occur resulting in a fire or explosion of some kind, closing these valves is necessary to contain the consequences and prevent feeding the accident. The location of these shut-off valves is not directly in the path that the operator would take to escape the danger. All of these factors mean that people would be unlikely to perform this critical action should a fire break out or if there is acute danger of an explosion. But the plans and procedures assume that operators will take this action.

There are many possibilities to resolve this gap. Some involve eliminating the task through valve design. For example, if the valves always reverted to a closed position when fuel is not being pumped through them, the operator would perform an action every time he wants fuel and not every time he doesn’t want fuel. Another approach is to provide a control so that the operator only needs to push a button which is positioned as part of the exit process. As always though in a resilience approach, any change can introduce new capabilities and potentially new complexities which will trigger adaptation to meet production and other pressures. For example, if a change in valve design led to frequent interruptions in flow, monitoring of filling could inadvertently become more difficult or disrupt the production process so much that workarounds occurred which defeated the safeguard.

VI. GENERATING FUTURE INCIDENTS

One of the objectives of Resilience Engineering is to anticipate incidents that have not happen yet. The team generated one case of a future incident scenario which could be used to design and test improvements and changes. The potential incident scenario was created based on the interviews and observations that took place in the train

---

3The new digital fueling mechanism linked to a database of truck drivers, compartment numbers and capacity relating to each truck.
system area of the Depot and that revealed particular events that contribute to the risk of overfilling.

The common operations procedures on the trains platforms are performed by three “operator one” and one foreman, responsible for supervision. Each operator is responsible for filling three or four cars depending on the demand. The operator is obligated to watch the filling in his other stations from a distance of about 20 feet, since he does not receive any information about other stations.

The possible situation occurs in a normal day of work in the train platforms of BR. Operator A, a male “operator one” who is monthly rotated, is working at four cars at the same time as he usually does. He starts by presetting the fuel amount in the first car, and as soon as he is done he heads to the second car. He continues this route until he gets to his fourth car. This is when something happens in the first car, but is not noticed by the operator who continues his job. The first car is still being filled, even though its counter already reached zero. The problem is that the counter reset to 99999, which kept the filling process going. This turns into an overfilling problem as soon as the cars reaches its full capacity and stars spilling fuel over the car. By the time the operator A realizes there has been overfilling the problem has turned into a fire. BR safety procedures have emergencies escape routes that should be followed by the operator in cases like this. The four operators following the procedures exit the train platforms. When reaching the stairs that lead to the exit of the train section, they pass a sign warning them to close the main valves on the platforms. These valves are located in the other direction away from the exit route (and the valves can take as long as four minutes to close). Will operators notice the sign or remember to detour to close the valves? Will operators place personal safety as the first priority in this situation (the interviews indicated that operators are unlikely to go back)? How does the fire cascade if the valves are not closed manually? A cascade of consequences is made more realistic by the recent Buncefield fuel depot fire near London in December of 2005.

The future incident design probes the resilience or brittleness of the organization, training, equipment and procedures as a system. The first question is how do operators notice and recover before overfilling occurs? When we trace the knowledge and mindset of the current operators, the standard practice is to preset all the cars with less than their capacity, and then do the final portion serially and manually. This tactic appears to dodge the risk of overfilling despite the limited means to assess the status of the filling process, but the scenario design challenges this workaround by creating circumstances where the counter resets (as was identified in the observations and interviews and is related to the knowledge gaps that can occur given the rotation system). One might ask: why is he filling four at once? But production pressure leads to tactics such as parallel filling given a limited number of cars and turnaround targets.

The second part of the scenario focuses on a goal conflict or double bind. Someone could say: “Why did no one close the valves? There was a sign there!” the goal conflict is hidden in part because the effectiveness of the emergency response plan is not tested realistically (gaps where people assume that since there is a plan for handling an emergency, the plan is effective are more common that we would like—consider FEMA’s Katrina response or examine your own plans restoring your personal computer from back up).

Note how the scenario is built by targeting gaps between the system as designed and the actual difficulties of operations. The scenario combines gaps in ways that seem likely to overwhelm the normal mechanisms for adaptation. And the scenario reveals how seemingly minor difficulties can contribute to effects that have major consequences. The scenario can be used to assess the effects of potential design changes. And the scenario can serve as a base that can be modified to capture other aspects of operations.

Other examples of future incident scenarios could be developed, not only on the trains, but also on the truck platforms. An evolving set of such scenarios is a basic tool PETROBRAS could use to identify brittle points and add resilience to their operations.

VII. CONCLUSION

PETROBRAS has begun to pioneer the development of Resilience Engineering methodologies. PETROBRAS sees the resilience approach as a means to enhance safety management inside a highly technical organization. This paper describes the work of only one of multiple groups that have begun to apply resilience concepts. The project also has the goal of developing engineers who can amplify resilience techniques throughout the companies operations.

ACKNOWLEDGMENT

Our group would like to thank Ms. Anelise Welter, Ms. Lucimara Balardin and Mr. Cleyton Vargas with the Ergonomics and Design Department (UFRGS) for their commitment and help through initial analyses and data collection on the project. The authors would also like to thank Mr. Marques, former manager of BR Distribuidora, who made it possible to access the information on the Depot.

REFERENCES


