FOCUS ON SUCCESS: A SAFETY-II APPROACH ON OPERATIONAL MANEUVERS IN THE ITAIPU BINACIONAL HYDROPOWER PLANT

Juliano Couto Portela[1] and Lia Buarque de Macedo Guimarães[2]

[1] Universidade Federal do Rio Grande do Sul, Av Osvaldo Aranha, 99, Porto Alegre, Brazil

[1] jportela@itaipu.gov.br

[2] Universidade Federal do Rio Grande do Sul, Av Osvaldo Aranha, 99, Porto Alegre, Brazil

[2] liabmg@gmail.com

Abstract

Accidents in critical infrastructures, such as the Itaipu Binacional HPP, although rare, cause serious social and economic impacts in their area of influence. Therefore, they must be avoided even if a "normal" accident rate is expected due to the operation complexity. This paper investigates the conditions leading to operational failures in the Itaipu operation under the approach of Safety-II management related to Resilience Engineering, "in the many things go right", contrasting the Safety-I view, based on the retrospective analysis and "the few things went wrong". Guided by the structured opinions of the operational staff and inspired by the FRAM method, the study deals with the normal operation and variabilities of four typical operational maneuvers within the quadrants of a periodicity-complexity matrix. The results indicated that the same variabilities influence the operation regardless of the complexity or periodicity of the maneuver. A comparison between the analysis of the variabilities in a typical situation and the four operational failures occurred between 2006-2015 indicated that some variabilities act decisively in virtually all maneuvers. The results were discussed with the team members who proposed the adaptations to increase the operational safety of normal work.

1 INTRODUCTION

Accidents of big proportions in organizations of high sociotechnical complexity cause great social and economic impact. Chernobyl, (1986), Three Mile Island (1979), Sayano-Shushenskaya (2009), Fukushima (2011) and Deepwater Horizon (2010) are examples. In all, the variabilities that affected the operational process had become out of control, impacted vital functions of the process, and eventually lead to the fatal failures. In situations of minor failures, as in industry or health service, the reason for accidents normally is understood by the use of techniques that search for contributing factors to the damage, focusing on “what goes wrong” in an approach known as "Safety-I".

Even if subsequent analysis had been successful in pointing out the root causes of these accidents and established new safety standards, it’s clear that if the conditions that led to the accidents had been anticipated, they probably had been avoided. Achieving it requires a different approach to normal operation and a different way of thinking about safety. Rather than reactive, it should be proactive: perceiving the hazards of the process before they get out of control. This new approach, called "Safety-II", considers important focusing on adaptive capacity in order to maintain control over unforeseen disturbances or events (Lundberg & Johansson, 2015). In addition, security should not focus on the rare cases of failures because they do not explain why performance is almost always satisfactory and how it helps to meet organizational goals.

Itaipu Binacional has 14,000MW of installed power. It is the largest power generator of the world, having produced nearly 2.5 billion MWh since 1984. It is responsible for 17% of the Brazilian’s energy consumption and 75% of the Paraguayan’s. Therefore, shutdowns at Itaipu Binacional have the potential to cause loss of production and instability to both electrical systems. Thus, it is for the best interest of the societies that the organization assumes the proactive view provided by Safety-II guidelines. Based on the principle of equivalence between "successes" and "failures", this view assumes that both normal operation and accidents emerge from the same origin. By this approach, safety is a consequence of the way the complex system behaves, not a static property. Furthermore, adopting Safety-II practices meets the vision of sustainable production and high operational performance, represented by a sequence of world records of energy production, the last one achieved in 2016 (more than 103 million of MWh). This article presents the method used to address the “focus on success” in the Itaipu operation by analysing four maneuvers that represent the universe of maneuvers in a periodicity-complexity matrix. Next, it traces the normal operation of such maneuvers, the variabilities that influence each step of the chosen maneuvers, and then evaluates the impact of each maneuver step on the overall result (success or error). Finally, analyses the failures already occurred to verify the adherence of the study to the situations already experienced.

2 SAFETY-I AND SAFETY-II

By understanding safety as an absence of unwanted results in normal operation, the goal of the "traditional" safety management – Safety-I – is to maintain a safe condition where the number of unwanted outcomes is as small as possible (Eurocontrol, 2013). “New” accidents occur because their cause was not eliminated as it was unknown. Technological upgrades, changes in human or organizational resources can bring new causes (Patterson, Deutsch, 2015).

Safety-I thus promote a bimodal way of seeing work and activities: when how things work out is because the system works as it should and because as people work in the prescribed way, as one imagines; When they go wrong, it's because something goes wrong or it fails. Security is a quality that the system is sufficient to ensure that the number of potentially harmful events (Eurocontrol, 2013).

Hollnagel (Vanderhaegen, 2015), by explaining there is a distinction between the Work-As-Done and Work-As-Imagined, where the latter is generally considered in a Safety-I approach, considers a mistake thinking of human beings as machines capable of responding in infinite ways to infinite possibilities. In short, in the approach of Safety-I mainly refers to the evaluation of the lack of security rather than the presence of security. However, the number of failures or accidents is much smaller than the number of successes in normal operation. In fact, Figure 1 shows the number of well-succeeded operational maneuvers selected for the study performed by the Itaipu operation in the period 2006-2015 and the failures resulting in loss of energy production, reliability or damage to equipment during that time. It can be observed that the failures represent 0.025% of the universe, while the successful maneuvers represent 99.975%. This is adherent to what is shown in (Eurocontrol, 2013).

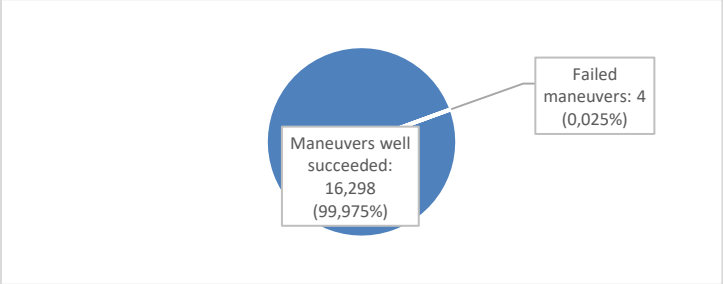

Figure 1 *Well-succeeded x failed maneuvers considered in the study between 2006-2015*

The contemporary security approach, called Security-II, is based on the principle of equivalence between successes and failures as well as fine-tuning performance, which makes performance always variable. Even in a normal operation, a certain variability can propagate from function to function, ultimately leading to an unexpected result, or non-linear effects (Hollnagel et al, 2015). Therefore, both normal operations and eventual accidents emerge from functions whose results are influenced by the variabilities present in any successful or failed operation. The extent of such variabilities (and their monitoring) is that will define the operation outcome. Security is, therefore, an emergent property that involves the operation of a complex system being a consequence of the way the system behaves, not a static property.

In short, Safety-II is based on a simple principle: one must understand and support the much that works (Patterson, Deutsch, 2015) instead of investing effort and resources in the few occasions when things go wrong. Focusing on success instead of focusing on failure implies that human actions are performed on real situations, subjected to high variability. According to this view, one must avoid treating failures as unique events, but see them as the expression of the variability of performance in the daily routine. Things that went wrong have worked well many times before, and will work out many other times in the future. In other words, when the error occurs, one should begin by understanding why the action is usually correct rather than looking for specific explanations to the failure (Hollnagel et al, 2015).

3 METHOD

Although safety management according to the precepts of Safety-II is still incipient, there are methods that can present an approach to the "focus on success". None of them, however, is specific to Safety-II. They are approaches that can be adapted to reach this goal in at least one criterion (Eurocontrol, 2013).

Reviewing some of the methods (Eurocontrol, 2013), the FRAM was chosen to serve as an inspiration for the study from a conceptual point of view, for it reflects the view of Safety-II and Resilience Engineering (Hollnagel et al, 2014). Inspired by the FRAM, the study mapped the functions of typical maneuvers of the Itaipu

Binacional operation, their variabilities, and interfering conditions on normal operation.

Due to the significant number of maneuvers executed by the Itaipu operational team, each one with several steps with different levels of complexity and attention, a matrix of four quadrants was created with categories "complexity" and "periodicity", where four maneuvers represent the universe for the purpose of this study. The periodicity refers to the number of times the maneuver was performed during the period. The complexity refers to the number of steps to be taken and the number of factors (vulnerabilities/noises) to influence its success. One of the criteria for choosing the maneuver was that it should cause an impact on the energy production or safety of human resources, facilities or the surroundings of the plant if unsuccessful.

In order to: - choose the maneuvers representing the four quadrants of the periodicity-complexity matrix; - determine the variabilities that influence each step of the chosen maneuvers; - evaluate the impact of each step of the maneuver on the overall result – success or failure –, interviews were conducted with 31 technicians and 8 engineers of the operation team. The results are shown in the Table 1.

Table 1. *Maneuvers considered in the study – period 2006-2015*

Maneuver	Periodicity	Complexity	Total of maneuvers
Select generating units to conventional control	LOW	LOW	553
Separation of generating units for ANDE	LOW	HIGH	27
Reversal of speed regulator pumps	HIGH	LOW	10,400
Start and stop of generating unit	HIGH	HIGH	5,322
TOTAL			**16,302**

4 RESULTS AND DISCUSSION

4.1 Variabilities

The variabilities that influence these four operational maneuvers were also obtained through the interviews with the professionals. It was verified that, regardless of the complexity and periodicity of the maneuver, 16 variabilities, grouped into 6 categories, are common to the four types of maneuvers, as shown in Table 2.

Table 2. *Variabilities that influence the operation*

Category	Variability
Operator	Knowledge/experience
	Ability to adapt to unexpected situations
	Necessity to confirm each step with another operator
Communication	Communication equipment availability
	Operator/Supervisor reports each step
	Quality of operational communication (eg. clear and objective communication between O&M)
Human Resources	Availability of human resources
	Hierarchy in the execution of step
Operational Instruction	Quality of the operational instruction
	Current operational restrictions
Maneuver Environment	Situations that take the operator's attention (e.g. telephone/alarm)
	Urgent / emergency situations or concomitant work
	Similarity with another maneuver environment
Maneuver equipment	Normal operation of the maneuver equipment
	Availability of the computerized systems
	Tacit peculiarities of the equipment (not described in any instructions)

From the start to the end of the maneuver, several steps are performed. For the purpose of the study, there are two types of steps: 1) *Key step*: central function from which the purpose of the maneuver is achieved. An error in a key step most probably causes an error in the maneuver itself. Examples: breaker closure, unit synchronization. It is similar to the *functional resonance* of the FRAM method; 2) *Relevant step*: although it is not a key step, it contributes to the normal flow of the maneuver in a decisive way; a failure in this step can influence the key step, and therefore cause error in the maneuver. Examples: trigger starting preparation, confirm voltage bar without voltage before switch closure;

Table 3 shows the 7 steps of one of the maneuvers (Select generating units to conventional control) with some of the variabilities – see Category “Operator” in Table 2 – to illustrate how the general table was assembled. It was considered less important to understand the technical meaning of each step than to understand how each variability influences each step. The “X” implies that the variability influences the step.

Table 3. *Example of maneuver steps and variabilities*

	Maneuver step	Key step (functional resonance)?	Operator – Knowledge/ experience	Operator - Ability to adapt to unexpected situations	Operator - Necessity to confirm each step with another operator
1	Request to the dispatch center to turn off the Automatic Control of Generation	N			
2	Set reference power in the Turbine Joint Control	S	X	X	X
3	Confirm that the voltage value is zero in the Joint Control	S			
4	Set reference voltage in the Voltage Joint Control	S	X	X	
5	Select generating units, transmission lines and voltage bars from Scada 1 to conventional	S	X	X	X
6	Confirm the switch key 43JCS in the Joint Control in the "conventional" position	N			
7	Switch generating units on conventional panel to the same position as in the digital system	N	X	X	

For example, it was considered that the "Operator Knowledge" variability does not influence the "Request to the dispatch center to turn off the Automatic Control of Generation" step, as the knowledge is not relevant to the outcome of this step. On the other hand, it was considered that "Ability to adapt to unexpected situations" influences the "Set reference voltage in the Voltage Joint Control" step because, if there is an unexpected situation at the time of this maneuver - for example, disturbance in the electrical system - the Operator must be able to adapt the maneuver to this situation.

Based on the evaluation of the operation team, the question "which variabilities in Table 2 influence this step?" was asked for each of the steps. The overall result is shown in Table 4, which gives an overview of the specific variabilities for each of the four quadrants of the matrix complexity-periodicity.

Table 4. *Variability frequencies on the maneuver key steps*

LOW COMPLEXITY		HIGH COMPLEXITY	
Maneuver environment – Similarity with another maneuver environment	85%	Maneuver environment – Urgent / emergency situations or concomitant work	76%
Maneuver environment – Situations that take the operator's attention (e.g. telephone/alarm)	62%	Maneuver equipment – Normal operation of the maneuver equipment	74%
Instruction – Current operational restrictions	62%	Maneuver environment – Situations that take the operator's attention (e.g. telephone/alarm)	74%
Instruction – Quality of the operational instruction	54%	Human Resources – Availability of human resources	67%
Operator – Knowledge / experience	46%	Operator – Necessity to confirm each step with another operator	64%
Operator – Ability to adapt to unexpected situations	46%	Instruction – Current operational restrictions	64%
LOW PERIODICITY		**HIGH PERIODICITY**	
Maneuver environment – Situations that take the operator's attention (e.g. telephone/alarm)	93%	Maneuver equipment – Normal operation of the maneuver equipment	61%
Human Resources – Availability of human resources	85%	Operator – Knowledge / experience	57%
Instruction – Quality of the operational instruction	85%	Maneuver environment – Similarity with another maneuver environment	57%
Operator – Necessity to confirm each step with another operator	81%	Maneuver environment – Urgent / emergency situations or concomitant work	50%
Instruction – Current operational restrictions	78%	Maneuver environment – Situations that take the operator's attention (e.g. telephone/alarm)	50%
Maneuver environment – Similarity with another maneuver environment	74%	Instruction – Current operational restrictions	50%

From Table 4, we can draw some conclusions:

a) The "maneuver environment" is significant in all situations of complexity and periodicity;

b) The "knowledge/experience", despite its central importance, does not appear as a main variability in the maneuvers of high complexity and low periodicity;

c) Most of the steps are affected by "Similarity with another maneuver environment "; it is usual in plants with several generating units that each environment where the operator performs the maneuver is exactly equal as the adjacent, except for the operational identifications;

d) The category "instruction" affects significantly the low complexity and low frequency maneuvers;

e) In the case of low periodicity maneuvers, many of the variabilities affect almost all the steps. The

main variability is the “Situations that take the operator's attention”. This is because as the maneuver is rarely executed, the operator tends to turn all the attention to the execution, and all the attention-taking conditions influence the normal operation;

f) In maneuvers of high complexity, the two variabilities that most affect the functions ("Maneuver environment - Urgent / emergency situations or concomitant work" and "Normal operation of the maneuver equipment") are external variabilities, so the operation has no much to do as a concrete action to decrease their influence on the maneuver, but emphasize the importance of the experience as well as the knowledge management as a way to increase the operation capacity of adaptation and response to eventual disruption, one of the primal precepts of RE.

4.2 Comparison between the variabilities raised and actual failures

Although Safety-II emphasized the analysis of success rather than failures, it was understood important to confront the results obtained with the four operational failures occurred between 2006 and 2015. The variabilities that influenced each one are summarized in Table 5.

The first operational process failure, occurred in 2010, was made in a maneuver of low complexity and high periodicity. The analysis indicated process failures in 5 out of 6 steps. There was a coincidence between the activation of an alarm and an unrelated work on the equipment, where the latter required special attention of the operator. When analysing the alarm in front of the equipment, the operator missed the comprehensive understanding of the operational situation, performing an undesired maneuver of pump transfer.

Second failure, occurred in 2008, was made in a maneuver of high complexity and low periodicity. The analysis indicated process failures in 2 out of 17 steps. In the occasion, the generating unit U9A should be switched off for maintenance. However, at the same time, the dispatcher asked to shut down the U03 along with the U9A in order to meet electrical systems demands. Upon entering the digital system screen to open the U9A circuit breakers, the operator was induced by the information that U03 should be also stopped. Thus, mistakenly the operator accessed the control panel of the U03 instead of the U9A and opened the circuit breakers with U03 still at full power, causing load rejection in the U03.

Third failure, occurred in 2014, was made in a maneuver of high complexity and high periodicity. In this, failure was found in 3 of the 22 steps. The generating unit U09 should start and synchronize to the electrical system. In order to run the start-up sequence automatically, it would be necessary for an operator be locally on the unit’s local control panel to switch the control mode to automatic. Since the local operator wasn’t found, the operator in the Control Room decided to perform the maneuver even so. With concomitant work in progress in the control room, the maneuver was performed by a single operator. In this process, the U09 circuit-breaker was closed out of ideal synchronization conditions, resulting in mechanical and electrical damage to the unit.

Fourth failure, occurred in 2014, was made in a maneuver of high complexity and high periodicity. In this, failure was found in 3 of the 22 steps. During the stopping process of generating unit U05 to meet electrical system requirements, the operator mistakenly transferred the power supply selection of the unit U04 instead of U05. It was necessary to stop the U04, which was operating normally at the time.

Without taking the frequencies into account, Table 5 shows the variabilities that influenced the four operational process failures between 2006 and 2015.

Table 5. *Summary of the variabilities that influenced the four failures*

Failure 1: 2010 occurrence **(Low complex/High periodic)**	***Failure 2: 2008 occurrence*** **(High complex/Low periodic)**	***Failure 3: 1st 2014 occurrence*** **(High complex/High periodic)**	***Failure 4:2nd 2014 occurrence*** **(High complex/High periodic)**
Maneuver environment *– Situations that take the operator's attention (e.g. telephone/alarm)*			
Maneuver environment *– Urgent / emergency situations or concomitant work*		***Maneuver environment*** *– Urgent / emergency situations or concomitant work*	
	Maneuver environment *– Similarity with another maneuver environment*		***Maneuver environment*** *– Similarity with another maneuver environment*
	Operator *– Necessity to confirm each step with another operator*	***Operator*** *– Necessity to confirm each step with another operator*	***Operator*** *– Necessity to confirm each step with another operator*
Operator *– Knowledge / experience*			
Maneuver equipment *– Normal operation of the maneuver equipment*	***Maneuver equipment*** *– Normal operation of the maneuver equipment*	***Maneuver equipment*** *– Normal operation of the maneuver equipment*	
		Human Resources *– Availability of human resources*	

Although totally different in circumstantial terms, some similarities that corroborate conclusions drawn from Table 4 can be noted:

a) The "maneuver environment" is important in all situations of complexity and periodicity;

b) The "operator knowledge" is not a main variability to influence maneuvers of high complexity and low periodicity. In fact, the reports pointed out that in the cases of faults 2, 3 and 4 the operators were fully aware of the operational procedure;

c) Most of the steps are affected by the variability "Similarity with another maneuver environment". In the case in question, in two of the four failures it was present;

d) The category "instruction" affects more significantly the low complexity / periodicity maneuvers.

e) In low periodicity maneuvers, many variabilities affect practically all steps. The main variability affecting normal operation comes from situations that get the attention of the operator.

f) The analysis of the reports has proved that malfunctioning of the maneuvering equipment and concomitant emergency / work situations are basic failure conditions. The operation should maintain the priority of its knowledge management systems and training to decrease their influence on the results of the maneuvers.

5 FINAL CONSIDERATIONS

This study applied precepts of Safety-II in a set of four maneuvers categorized in high and low complexity and periodicity performed by the operation of the Itaipu Binacional HPP, inspired by the FRAM method, in order to understand which variabilities influence the normal operation. Maneuvers were detailed in steps; for each, it was pointed the variabilities that act on them and it was concluded which variability most influences the normal operation. By this, variabilities that influence the operation are common to all studied maneuvers.

The results were compared to the reports of the four operational process failures occurred between 2006 and 2015. The conclusion is that although it is fragile to say that the four maneuvers represent the whole universe of more than five hundred maneuvers executed by the Itaipu operation, they provide valuable inputs to the study by allowing pertinent conclusions comparing what was verified in the study with the actual cases of failure. Some of that are: a) some variables act decisively in practically all maneuvers. Among them, the category maneuver environment, the need to confirm the steps of the maneuver with another operator, situations that draw attention from the operator and the similarity with another operating environment. The operator knowledge was not mapped as a fundamental variability present in the failures.

Comparisons between normal operation and failure cases proved success and failure come from the same source, which is adherent of the Resilience Engineering principles. Once identified the maneuver functions, it was possible to understand which would be the most important variabilities that influence normal operation, providing subsidies to the organization to the decision-taking before an event of failure.

The main contributions of this work for the development of the discipline are:

a) The confirmation that the same variabilities influence the operational steps, regardless of the complexity of the periodicity of the maneuver.

b) The reports of the four failures corroborated fundamental aspects of the study;

c) The Resilience Engineering and Safety-II approaches are adherent to the real cases found.

REFERENCES

M. Patterson and E. S. Deutsch, “Safety-I, Safety-II and Resilience Engineering,” Curr. Probl. Pediatr. Adolesc. Health Care, vol. 45, no. 12, pp. 382–389, 2015.

J. Lundberg and B. J. E. Johansson, “Systemic resilience model,” Reliab. Eng. Syst. Saf., vol. 141, pp. 22–32, 2015.

EUROCONTROL, “From Safety-I to Safety-II: A White Paper,” Netw. Manag., pp. 1–32, 2013.

F. Vanderhaegen, “Erik Hollnagel: Safety-I and Safety-II, the past and future of safety management,” Cogn. Technol. Work, vol. 17, no. 3, pp. 461–464, 2015.

E. Hollnagel, R. L. Wears, and J. Braithwaite, “From Safety-I to Safety-II: A White Paper,” Netw. Manag., p. 43, 2015.

E. Hollnagel, J. Hounsgaard, and L. Colligan, FRAM – the Functional Resonance Analysis Method - A handbook for the practical use of the method, 1st ed., no. june. Middelfart, Denmark, 2014.