MITIGATION CONTROL OF FAULTS IN CRITICAL PRODUCTION SYSTEMS

Jeferson A. L. Souza
Diolino J. Santos Fo
University of São Paulo , São Paulo, Brazil
jeferson.souza@usp.br; diolinos@usp.br

Paulo Eigi Miyagi
University of São Paulo , São Paulo, Brazil
pemiyagi@usp.br

Fabricio Junqueira
University of São Paulo , São Paulo, Brazil
fabri@usp.br

Reinaldo Squillante Jr
University of São Paulo , São Paulo, Brazil
reinaldo.squillante@usp.br

Edinei P. Legaspe
University of São Paulo , São Paulo, Brazil
edinei.legaspe@usp.br

Abstract. *The inherent complexity of critical production systems, coupled with policies to preserve people´s safety and health, environmental management, and the facilities themselves, and stricter laws regarding the occurrence of accidents, are the motivation to the design of Safety Control Systems that leads the mitigation functionality. According to experts, the concept of Safety Instrumented Systems (SIS) is a solution to these types of issues. They strongly recommend layers of risk reduction based on hierarchical control systems in order to manage risks, preventing or mitigating faults, or to lead the process to a safe state. Additionally some of the safety standards such as IEC 61508, IEC 61511, among others, guide different activities related Safety Life Cycle design of SIS. The IEC 61508 suggests layers of critical fault prevention and critical fault mitigation. In the context of mitigation control system, the standard provides a recommendation of activities to mitigate critical faults, by proposing control levels of mitigation. This paper proposes a method to implement the mitigation layer based on the risk analysis of the plant and the consequences of faults of its critical components. The control architecture, based on distributed and hierarchical control systems in a collaborative way, will make use of the techniques of risk analysis raised and mitigation actions, based on the knowledge of an expert, will be implemented by fuzzy logic. The mitigation layer therefore seeks to reduce the inherent risk in a process, and besides proposing the mitigation layer, this work aims to a further reduction of process risk on proposing an anticipatory mitigation action through temporal analysis of the evolution of the parameter used to measure the effect of the occurrence of a critical fault.*

Keywords*: Critical Systems, Mitigation Control System, Safety Instrumented System, Fuzzy Logic*

1. INTRODUCTION

In this first decade of the century XXI, many studies have indicated that automation processes are undergoing transformations that have been strongly influenced by the advance of technology and computing resources; becoming increasingly complex due to their dynamic and needed to address issues such as global market competitive production and technology used among other factors (Chen and Dai, 2004; Santos Fo, 2000; Wu *et al.*, 2008). Given this new scenario, industrial processes and their control are becoming more complex. Additionally, organizations have focused on policies to achieve and demonstrate people's safety and health, environmental management system, and controlling risks. Thus, industries should be consistent with their policies and objectives according to both the standards, Occupational Health and Safety Assessment Services – OSHAS 18001 (OSHAS, 2007), and ISO14001 (ISO, 2004), respectively.

In this context, any industrial system, as modern and innovative as can be, could be considered to pose a serious risk to people's health, the environment and to the costs of industrial equipment, in the event that a fault fails to be diagnosed and treated correctly (Sallak *et al.*, 2008). Although many studies have been presented for diagnosis and treatment of faults, a review of fault-tolerant reconfigurable control system can be found in (Zhang and Jiang, 2008), the accidents still occur. These issues are fully justified because there is no zero risk in process industries since: (i) physical devices do not have zero risk of failure, (ii) human operators do not have zero risk of error and (iii) there is no computational software projects developed that can predict all the possibilities. Thus, studies that aim to diagnose and

treat faults are inserted at this level of complexity that relies on restricting its state space for the control and treatment of a particular class of faults.

According to experts, the concepts of safety instrumented systems (SIS), is a solution to these types of issues and strongly recommend layers of risk reduction based on control systems organized hierarchically in order to manage risks by either preventing or mitigating failures, or to bring the process to a safe state. Additionally, these control systems must comply with the principles of sustainability so that in case of serious accidents, do not compromise the health of people, the environment and equipment (Summers and Raney, 1999). In this sense, some safety standards such as IEC 61508 (IEC, 2010), IEC 61511 (IEC, 2003a) among others, guide different activities related with a SIS Safety Life Cycle (SLC),such as design, installation, operation, maintenance, tests and others (Lundteigen and Rausand, 2009).

The term risk defines a metric for quantifying injury, environmental damage and economic losses; in reference to both probability of a fault occurrence and magnitude of the injury or loss (Bell, 2005). Due both industrial processes and their control are becoming more complex, and also the issues of sustainability, requirement specification for SIS is becoming more complex. Furthermore, according to IEC 61508 (IEC, 2010), the term "fault" is defined as an abnormal condition that can cause a reduction or loss of the ability of a functional unit. In this work, failures are classified into two groups: (a) non-critical faults that define risks to be "tolerated" and therefore automatically recovered by the Basic Process Control System (BPCS); hence, the industrial process can be regenerated in a controlled way to a normal state of operation, and (b) critical faults that define unacceptable magnitude of risks and must be either prevented or mitigated in order to avoid a catastrophic scenario, which may cause human fatalities and environmental damage. Therefore, the industrial process should be placed into a safe state via the degeneration of the process by layer of risk reduction or SIS.

According to IEC 61508, there are two layers of SIS: the prevention layer and the mitigation layer. Recently, Squillante *et al.* (2011) proposes the implementation of a SIS prevention layer that models the diagnosis of critical faults, performs the treatment and coordination of faults, and accomplishes the integration and analysis of the generated models, performing its validation in compliance with IEC 61511. But some critical faults, depending on its consequence is severity, can lead the plant to a scenario that the prevention layer may not be enough to bring the system to a safe state or, depending on the magnitude of the fault, the system should treat the fault directly on the mitigation layer.

So far, the issue is the distinction between the treatment of a critical fault that should be addressed in prevention layer or directly in the mitigation layer or, in case that a fault being treated in the prevention layer, present an increasing evolution in it severity. In other words, the prevention layer is not enough to bring the system to a safe state, and an additional task must be performed to avoid a catastrophic scenario.

This work is initially proposed a systematic for modeling and validating layer of mitigation control within SIS. This approach considers the cause of the fault, its severity and its consequence for the system, through the application of risk analysis techniques such as *Failure Modes and Event Analysis* - FMEA, *Fault Tree Analysis* – FTA (Lewis, 1995; Modarres *et al*. 2010), and the *What-If* technique (Souza, 1995), based on a database of occurrence of faults or on knowledge of an expert or operator. The effects and the consequences of the occurrence of a critical fault, listed on the risk analyses study, are monitored and treated by the SIS sensors and actuators, respectively, independently of the BPCS devices, as predicts the IEC 61508. The effect of every critical fault, or safety instrumented function (SIF), will be monitored via SIS sensors and the action to mitigate each fault will be based on the *What-If* technique yet used, using fuzzy logic to implement the control algorithm (Zadeh, 1965; Lee, 1990, Popa *et al.*, 2008).

The mitigation layer contributes to a further reduction of the process risk, compared with a system in which only the preventive layer is present. This paper proposes a technique to implement a SIS mitigation active layer protection, based on IEC 61508 standard, using risk analysis techniques to evaluate the critical components and the severity of its faults, and purpose mitigation actions based on fuzzy logic algorithm . This result already contributes to a reduction in the process risk. However, an analysis of the temporal variation of the variable that indicates the effect of fault of a critical component will also be addressed, and may represent an anticipatory action of the mitigation SIS, contributing to a greater reduced process risk, in order to preserve people, the environment and equipment.

This paper is organized as follows: Section 2 presents the fundamental concepts of Risk Analysis techniques, such as FMEA, FTA and What-If technique, and the basis of Fuzzy Logic. Section 3 presents the proposal of a layer of mitigating control system and Section 4 presents the results. Finally, section 5 presents the conclusion and references.

2. FUNDAMENTAL CONCEPTS

This section introduces fundamental concepts of some risk analysis techniques, such as FMEA, FTA and What- IF technique, ending with the concepts of fuzzy logic.

Other risk analysis techniques, such as HAZOP (Hazard and operability) can be used (Cavalheiro *et al*, 2012). This paper proposes the techniques listed above because one technique complement each other, resulting in a better risk analysis study.

2.1 Risk Analysis Techniques

2.1.1 Failure Modes and Event Analysis – FMEA

The FMEA technique involves a detailed and systematic study of the possible faults of components or mechanical systems. The failure modes of each component are identified and the effects of these failures in the system are evaluated and proposed measures to eliminate, mitigate and control the causes and consequences of these faults (Lewis, 1995)

Thus one can outline what the critical components of the system, ie, which elements that under failure can cause the most serious consequences to the operators, the environment and to the equipment.

One should ponder five questions about the system as a basis for the development of a FMEA:

-How each system component can fail ? And what are its fault modes ?
-What are the effects of(s) fault(s) on the system ?
-How critical are these effects ?
-How to detect the fault ?
-What measures against these faults ? Avoid, prevent the occurrence, minimize its effects ?

It is usually presented in tabular form and/or in a risk matrix that takes into account the severity level associated with the occurrence of the fault versus the probability of occurrence.

As a disadvantage, the FMEA is a procedure centered on the component, for it falls short when multiple failure modes occur simultaneously, or when faults occur in various components.

2.1.2 Fault Tree Analysis – FTA

Methodology of deductive reasoning that part of an event, a specific fault of the system, called top event, and aim to determine the logical relations of component faults and human errors that can be associated with the occurrence of the top event. The analysis is performed by building a logic tree, starting from the top event for basic faults. Thus, we obtain a graph used to identify all potential causes originated all potential causes of failure (Modarres *et al*., 2010).

In a top-down approach, we can understand "how" the top event occurred. Already on a bottom-up approach, we can understand "why" the occurrence of the top event, as showed in the Fg.1 below:

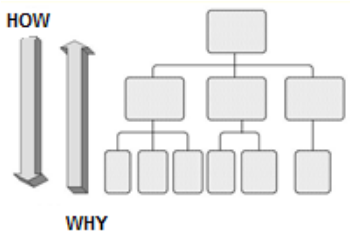


Figure 1. Up-Down and Bottom Up approach of a FTA.

The advantage of FTA on the FMEA is a process FTA is centered on the symptoms of fault by this takes into account the combination of failure modes of various components in the fault top event, being connected by logical operators such as "and" and "or".

2.1.3 What- If Technique

This technique examines system responses from of equipment faults, human errors and abnormal process conditions. For the development of this technique, it is necessary to set up a team with knowledge about the process to be analyzed and its operation.

The team seeks to answer questions such: "**What** ...**If**...?". Example: " What if the relief valve did not open the specified pressure?"

These issues are developed in an attempt to identify the potential risks present in the process. As depends on the experience and knowledge of a system expert or operators, this technique is usually used to complement or assist the other risk analysis techniques (Souza, 1995).

2.2 Fuzzy Logic

Fuzzy logic is becoming very useful particularly on modeling non-linear systems or when using traditional modeling of differential equations becomes very complex, or even when modeling processes whose knowledge of the dynamic behavior is still not fully understood (Lee, 1990).

Fuzzy systems are knowledge-based or rule-based systems and the main goal of fuzzy logic is to mimic (and improve on) "human like" reasoning (Zadeh, 1996). Specifically, the key components of fuzzy systems knowledge base are a set

of IF-THEN rules obtained from human knowledge and expertise. The fuzzy systems are mostly multiple inputs to a single output. (Zadeh, 1965; Lee, 1990; Popa *et al.*, 2008).

Unlike Boolean logic, fuzzy numbers are contained in a closed interval between zero (0) and one (1), and therefore can take any value within this range. For example: 0.45 is a valid fuzzy number (Zadeh, 1965).

A way to represent fuzzy sets, i.e., human knowledge is through membership functions, that is a function in mathematical terms: given its domain, has the value of his image, but separated in each term belonging to the membership function. It can be expressed both in graphical form as a mathematical line segments.

In a summarized form, the value of an input variable undergoes a fuzzification process, which is a method that converts a real number to a fuzzy number. This fuzzy number is analyzed in an inference module from a set of rules defined by human knowledge of the dynamic behavior of the system, which will generate a fuzzy output. The next step is to perform the defuzzification of this output, resulting in a real number. A schematic diagram of the Fuzzy Controller is shown in Fig.2 below:

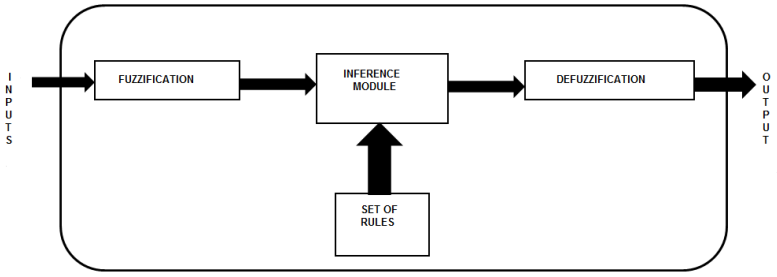


Figure 2. Schematic diagram of a Fuzzy Controller.

According to the input values, fuzzy logic performs operations between the inputs sets, such as t-norm and t-conorm. The most used is the t-norm, which makes an operation of minimum or intersection between the input sets, being represented by the **min** operator. The rules, as already stated, are formed by ranges between the sets. For example, a variable temperature can be defined by low or high. An average temperature may, on fuzzy logic, be considered "medium high" or "medium low" (Legaspe *et al*, 2012).

The human knowledge will therefore be the foundation for a set of fuzzy rules, formatted as "If (conditional)…Then (consequent)". All rules are processed in parallel, with the consequent being active with their degree of pertinence in the system output.

In the inference module we have the application of inference methods, such as Method Mandani Kang-Takagi-Sungeno (KTS). The inference method is the most commonly used method Mandani, which represents a simple mathematical model. Briefly, for a given input and applying the rule set to **min** or intersection operation of these sets, and output is determined by the set union or **max** of each rule entry. This output must go through a process defuzzification to be converted to a real number. A defuzzification process is, for instance, to calculate the centroid or center of mass, thus performing a weighted average of **max** values of output fuzzy sets.

The use of fuzzy logic in industrial systems is done by FCL – Fuzzy Control Language – defined by the standard IEC 61131-7 (IEC, 2000), which deals with fuzzy writing programs in industrial systems, e.g. making use of PLCs.

3. PROPOSAL OF LAYER OF MITIGATING CONTROL SYSTEM

The distributed and hierarchical control architecture in a collaborative way proposed can be represented according to Fig.3 below:

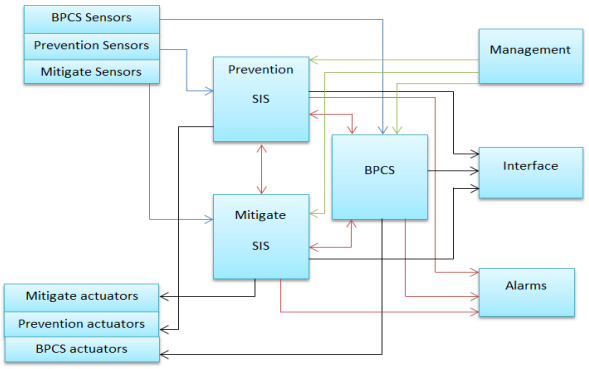


Figure 3. Control Architecture proposed for SIS Mitigation layer.

The "management" box of the Fig.3 above can be represented by the SSCA – Safety Supervisory Control Architecture (Squillante *et al*, 2013).

3.1 Description of the proposed method

The proposed method is outlined in the flowchart shown in Figure 4 below, and the steps for its implementation are described in the following items. 3.1.1 to 3.1.2 are built from domain knowledge and/or database obtained from field experiments, record of past operation or computer simulation of plant under study.

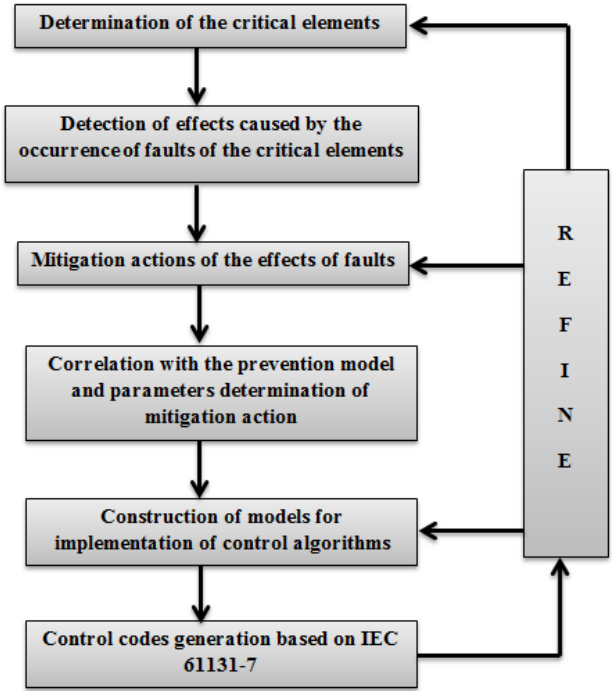


Figure 4. Flowchart of steps of the proposed method.

3.1.1 Determination of the critical elements

To determine the critical elements of the process under study we utilize the risk analysis techniques FTA, FMEA and What-If. The FMEA, to associate a severity level to the occurrence of fault of a component indicates which components must be monitored in the mitigation layer. Faulted components that pose risks to operators, the environment and equipment, besides violating the legislation are classified to maximum severity.

Furthermore, components which fault under no danger considerable not part of our analysis.

Because the FMEA to be centered on the component, combination of faults and a possible domino effect over other components may be analyzed by the FTA in conjunction to What-If technique. It is possible, according to Figure 3, to determine the how and the why of the fault, therefore rendering a more comprehensive study.

3.1.2 Detection of effects caused by the occurrence of faults of the critical elements

Each effect arising from the fault of a critical component must be monitored by a specific sensor for its failure mode. According to IEC 61508, such sensors must be independent of the BPCS. To avoid spurious failures and reading errors, it is recommended to use redundant architectures (Squillante *et al*,2013*)* , such as the criteria voting 2oo3 (two of three).

3.1.3 Mitigation actions of the effects of faults of critical elements

For each effect of a critical fault, detected by the SIS mitigation sensors, a mitigation action must be implemented by SIS mitigation actuators, controlled by the SIS mitigation control layer, aiming to preserve people, environment and equipment.

To determine de mitigation actions will make use of *What-If* technique, based on human knowledge and records of occurrence of faults, its effects and the actions proposed to mitigate its effects.

Some mitigation actions can be matched to faults occur in different components, but not necessarily input signals from SIS mitigation sensors are the same. That is, for different input signals, from different sensors, mitigation actions

may be the same. In this step, besides determination of the mitigation sensors can arrive at the conclusion that the sensors would be the same prevention. In this case, it is recommended doubling of signals from sensors for prevention PLC we use in our mitigation.

After this study and compilation of mitigation actions, will determine which actuators required for each mitigation action.

3.1.4 Correlation with the prevention model and parameters determination of mitigation action

As presented in Squillante *et al.* (2011), the SIS prevention layer is triggered when a process parameter exceeds a threshold. It is, therefore, a system of continuous variables. However, the approach taken was that, to overcome this threshold, indicating the occurrence of a critical fault, Squillante *et al.* (2011) performs a discrete event (Miyagi, 2007) approach for treatment and coordination of this critical fault. In our mitigation model, on the other hand, will take action to mitigate proportional to the absolute value of the control variable and also its temporal derivative.

This way, you can have a mitigation action if a fault occurs in the prevention layer by its own fault: fault of prevention sensors, actuators, hardware, and algorithm control or even due to an unforeseen scenario for project. Either prevention layer does not show enough to bring the system to a safe state, or if the trend parameter that monitors the occurrence of critical fault presents a very high value, the mitigation layer will be triggered by the prevention layer.

3.1.5 Construction of models for implementation of control algorithms

In this step of proposal will be presented control models for continuous variables of the process, making a correlation models addressed by prevention layer (Squillante *et al.*, 2011). In this step will be used results of the *What-If* technique already implemented in section 4.1.3 to determine the level or percentage of the measured variable values for activation layer of prevention and / or mitigation using the absolute value of the measured variable and its temporal variation or derivative of the measured parameter.

The results of this study will form the basis of fuzzy algorithms for mitigation control layer.

3.1.6 Control codes generation based on IEC 61131-7

For each mitigation action determined by the fuzzy control algorithm, the next step is to convert the generated control algorithm for a language of IEC 61131 to implement in the Safety PLC for mitigation.

The IEC 61131-7 deals with the implementation of fuzzy algorithms in FCL (Fuzzy Control Language), based on IEC 61131-3 (IEC, 2003) ST (Structured Text) for the implementation in conventional PLCs. Below it is shown an application example of implementation of fuzzy algorithm using structured text, as standard instructions.

4. EXAMPLE OF APPLICATION

To illustrate the method proposed, an application example for critical faults to be mitigated by SIS Mitigation layer in a natural gas compression station is presented. Natural gas is a mixture of highly flammable hydrocarbons. To be extracted from the environment must be pressurized in compressor stations to its carriage due to consumer centers.

4.1 Process Description

The natural gas station has one or more natural gas supply lines, called suction, from a gas pipeline which transports this natural gas. At the station entrance, natural gas goes through filters equipment before being compressed by the turbo compressor machine. A portion of this gas is directed to the utility unit. The utility unit accounts for controlling the gas temperature and pressure for use in the compression station, such as fuel gas for the turbo-compressor machine, gas heaters and gas power generators. After the natural gas is compressed by turbo compressor machine, it is sent back to the gas pipeline through discharge lines, called headers. Figure 5 shows a Process and Instrumentation Diagram (P&ID) of a turbo compressor of the gas compression station:

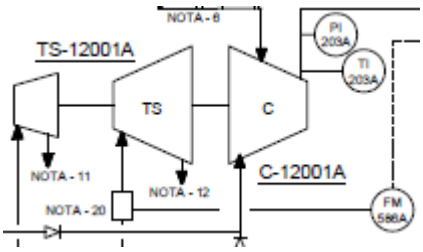


Figure 5**.** P&ID of a turbo compressor unit of the gas compression station.

4.2 Application of the proposed method

We apply the proposed method, based on the SIS prevention layer proposed by (Squillante *et al.*, 2011) for the case of the turbo compressor gas compression station. A more elaborate study should be done, considering all critical components indicated by the application of FMEA and FTA techniques. This work presents an example for a system component, in order to exemplify the application of the proposed method.

4.2.1 Determination of the critical elements

Applying the FMEA technique can be seen that the turbo compressors are critical to effectively our system, because they operate under high temperature, pressure and speed, in addition to use as fuel the compression fluid itself, which is natural gas, just explosive. A fault in this equipment certainly put under unacceptable risk operators, the environment and the equipment itself, besides violating government standards for safety. Hence its severity is maximum, and must be entered in our mitigation layer. Table 1 below illustrates a FMEA for turbo compressor:

Table1. Proposed FMEA for temperature increase of the lubricating oil of shaft bearing turbo compressor

Component	Potential Fault Mode		Potential Effects of Fault	Potential Causes of Fault	Deteccion - Control	Recommended Actions	Severity Associated
Turbo Compressor	Lubrication		Increase in temperature of the lubricating oil bearing	Saturated Oil	Temperature Sensors	Shut-Down (Preventive) Dioxide Carbon (Mitigate)	10
	Damage	Oil Pump					
		Shaft Speed control		Bearing Wear Hardware / Software			
	Overload	Speed		Speed Control			
		Torque		Condensate Excess			

To understand how and why a turbo compressor fail, the FTA based on fault history or knowledge of an expert (using the What-If technique), you can have the following structure, shown in Fig. 6 below:

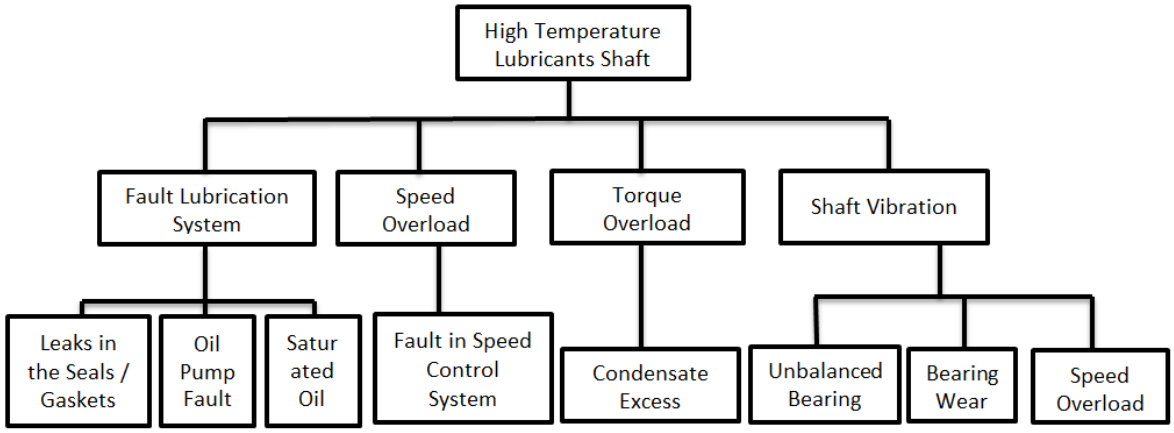


Figure 6. Suggested FTA for the top event "High Temperature Lubricants Shaft"

Both FMEA and FTA found that an effect of occurrence of fault in the turbo compressor is to increase the temperature on the cooling fluid turbine shaft, being able to have also an increase in temperature of the working fluid in the discharge line. We will perform our study on the mitigation system as a function of monitoring the temperature parameter for this component. Other effects can be measured as changes in discharge pressure coming from a lower performance of the turbo compressor operating under fault.

4.2.2 Detection of effects caused by the occurrence of faults of the critical elements

For the effects of faults listed in the previous step, we have temperature sensors coolant axis of turbo compressors, independently of the BPCS. Such sensors will be designated TAT 211 – Temperature Axis Turbine – for each unit present in the natural gas station. So we have the TAT 211 A, TAT 211 B, TAT 211 C and TAT 211 D as input signals our mitigation PLC. Again, a redundant architecture of these sensors as well as the implementation of algorithms for detecting spurious faults (Squillante *et al*, 2013) must be implemented.

4.2.3 Mitigation actions of the effects of faults of critical elements

To mitigate the effects caused by the occurrence of a fault in the turbo compressor, beside the action of shutdown from the prevention layer, suggested action to mitigate the effects is the forced cooling of the turbo compressor, if preventive layer is not sufficient or if the temporal variation of temperature proves too high.

Will be used both carbon dioxide cylinders large that are already installed in natural gas station, and have the purpose of fire combat if an outbreak of fire. The release of carbon dioxide is currently done manually, through the action of fire brigade teams, specially trained for this purpose. The proposal would be the installation of pipelines leaving the cylinders to turbo compressors with proportional valves connected to the outputs of mitigation´s Safety PLC. As the intensity of mitigation action, the valve would release the carbon dioxide in the same proportion. Figure 7 below show the carbon dioxide cylinders already installed in the gas compression station:

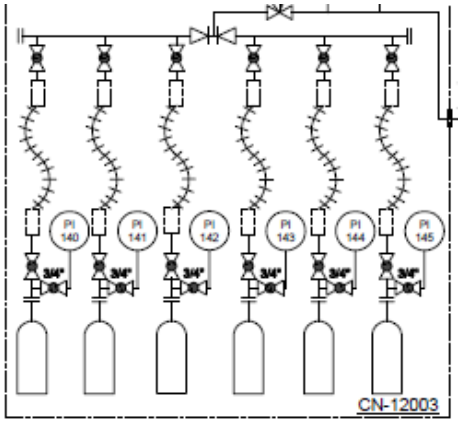


Figure 7. P&ID of carbon dioxide cylinders of the gas compression station.

4.2.4 Correlation with the prevention model and parameters determination of mitigation action

In the prevention model, sensors TIT 209 for units A, B, C and D are responsible for monitoring the temperature deviation of turbo compressors discharge. Such sensors are used in our model for mitigating the effect may indicate a fault or unforeseen hidden in our risk analysis. As the IEC 61508 requires that the monitoring devices must be independent, is used to signal duplicators on mitigation PLC.

4.2.5 Construction of models for implementation of control algorithms

From mitigation proposals have the construction of the control algorithms implemented by fuzzy logic, from the What-If technique already implemented, based on the expertise of a specialist.

To illustrate the algorithm, the expert reports that 150% of the temperature set point would be unacceptable to the turbo compressor. So we adopted a range of 110% to 130% for the prevention layer. Above 120% mitigation layer already comes into operation in a proportional action. Note that the temporal variation in temperature is part of the algorithm´s control input, beyond the absolute value of the parameter. Figure 8 below illustrates the proposed model for temperature:

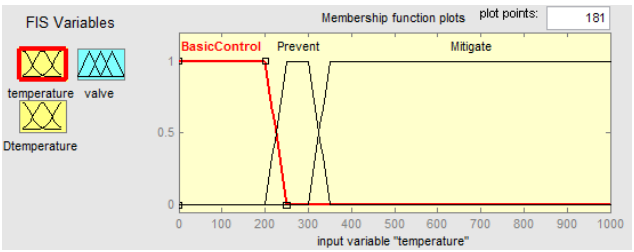
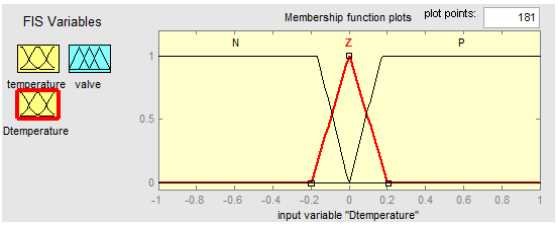
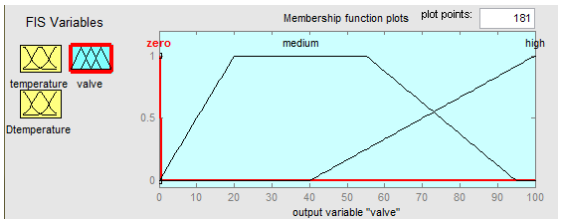


Figure 8. Fuzzy Membership functions for temperature

According to the membership functions adopted in the Fig. 6 above, has three regions for temperature: Basic Control, Prevent and Mitigate. The input of time derivative of temperature was set to three values: zero, positive and negative.

As for output, which is proportional to the valve opening was also set to three positions: zero or closed valve, high or 100% open and medium, open at 50%. Fig.9 and Fig.10 below illustrate the above:





Figures 9 and 10. Membership functions to temperature derivative and percentage of valve opening.

The rules of the fuzzy algorithm, according to What-If technique are as follows in Tab.2:

Table 2. Fuzzy rules for mitigation layer.

IF	TEMPERATURE	OPERATOR	DTEMPERATURE	THEN	VALVE
1	*MITIGATE*				*HIGH – 100% OPEN*
2	*BASIC CONTROL*				*ZERO - CLOSED*
3	*PREVENT*	*AND*	*P*		*MEDIUM – 50%*
4	*MITIGATE1*	*AND*	*N*		*MEDIUM – 50%*

The fuzzy algorithm applied to our model is presented in Tab. 3 below:

Table 3. Fuzzy Set.

FUZZY MODEL	MANDANI
AND METHOD	MIN
OR METHOD	MAX
IMPLICATION	*MIN*
AGGREGATION	*MAX*
DEFUZZIFICATION	*CENTROID*

The output signal, or the proportional action of mitigation, here designated by proportional valve opening, can be seen by the generated surface on Fig.11 below:

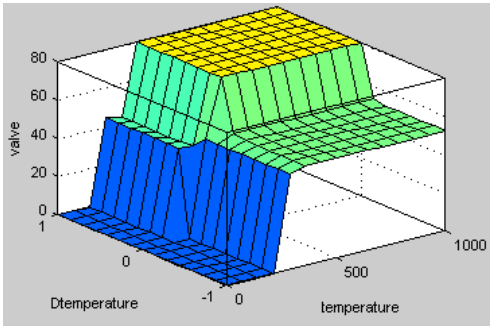


Figure 11. Surface generated by the fuzzy algorithm according to the fuzzy rules defined for the mitigation model.

We can see from the graphs of anticipatory mitigation action due to the temporary increase of the measured variable. This results in better efficiency of the system, thus contributing to a further reduction of the inherent process risk.

4.2.6 Control codes generation based on IEC 61131-7

From the algorithms based on fuzzy logic implementation has the control codes to Safety PLC for mitigation, considering the anticipatory model, as shown in Fig. 12 below:

```
FUNCTION_BLOCK FUZZYCONTROL
VAR_INPUT
        temperature : REAL;
        dtemperature : REAL;
END_VAR

VAR_OUTPUT
        valvule : REAL;
END_VAR

FUZZIFY temperature

        TERM BasicControl := (0,1) (200,1) (250,0);
        TERM prevent := (200,0) (250,1) (300,1) (350,0);
        TERM mitigate := (300,0) (350,1) (1000,1);

END_FUZZIFY


FUZZIFY dtemperature

        TERM N := (-1,1) (-0.2,1) (0,0);
        TERM Z := (-0.2,0) (0,1) (0.2,0) ;
        TERM P := (0,0) (0.2,1) (1,1);

END_FUZZIFY
```

```
DEFUZZIFY valvule

        TERM zero := 0;
        TERM medium := (0,0) (20,1) (55,1) (95,0);|
        TERM high := (40,0) (100,1);

        ACCU : MAX;
        METHOD : COG;
        DEFAULT := 0;

END_DEFUZZIFY

RULEBLOCK No1
        AND : MIN;

        RULE 1 : IF temperature is mitigate THEN valvule IS high;
        RULE 2 : IF temperature is BasicControl THEN valvule IS zero;
        RULE 3 : IF (temperature is prevent) and (dtemperature is P)
                 THEN valvula IS medium;
        RULE 4 : IF (temperature is mitigate) and (dtemperature is N)
                 THEN valvula IS medium;

END_RULEBLOCK

END_FUNCTION_BLOCK
```

Figure 12. Control code generated, implemented in FCL (Fuzzy Control Language) according to IEC 61131-7.

5. CONCLUSIONS

A method for the implementation of mitigation layer in critical industrial systems was proposed, based on the IEC 61508 and IEC 61511 standards, which recommend layers of risk reduction based on cooperative and hierarchical control prevention and mitigation of critical faults. Based on the results of applying the risk analysis techniques can be evaluated, due to the effects of their faults, what the critical elements present in the process. Based on the knowledge of an expert and making use of the What-If technique already deployed, implement corresponding mitigation actions using fuzzy logic, becoming such an algorithm in industrial PLCs languages based on IEC 61131-7. This layer proposal, coupled with the prevention layer, contributes to reduce the inherent risk in the process and adding to the temporal analysis of the variable associated with the effect of a critical component fault results in anticipatory mitigation action, resulting in a higher process risk reduction.

A refinement of this method can be accomplished by inserting a larger set of terms for de derivative membership function, such as PS (Positive Short), PM (Positive Medium) and PH (Positive High) and adopting the same procedure for negative derivative. Intermediate values of the actuator, eg 30% may be associated with these new values, which will surely determine new fuzzy rules in the algorithm. Other mitigation actions can be proposed, and this model must be implemented for the other critical elements of plant. Such elements may have other parameters that indicate the fault component and also other mitigating actions.

6. ACKNOWLEDGMENTS

The authors would like to thank the Brazilian governmental agencies CNPq, FAPESP, and CAPES for their financial support to this work.

7. REFERENCES

Bell, R., 2005. “Introduction to IEC 61508”. In Proceedings of ACS Workshop on Tools and Standards. Sydney, Australia.

Cavalheiro, A.C.M. “Design of supervisory control system for ventricular assist device”. In *IFIP Advances in Information and Communication Technology,* Lisboa, Portugal, p. 375-382, 2012.

Chen, C. and Dai, J., 2004. Design and high-level synthesis of hybrid controller. *In Proc. of IEEE Intern. Conf. of Networking, Sensing & Control.*

IEC, I.E.C., “Programmable Controllers IEC 61131-7: Fuzzy Control programming”, 2000.

IEC, I.E.C., 2003a. “Functional safety - safety instrumented systems for the process industry sector - part 1 (IEC 61511)”

IEC, I.E.C., 2003b. “Programmable controllers IEC 61131- part 3: Programming languages”, 2003.

IEC, I.E.C., 2010. “Functional safety of electrical / electronic / programmable electronic safety-related systems (IEC 61508)”.

ISO14001, I.O.f.S., 2004. “International standard for environmental management systems”.

Lee, C. C.: “Fuzzy logic in control system: fuzzy logic controller Part 1”. In *IEEE Transactions n System, Man and Cybernetic,* Vol 20, nº2, p. 404-418, 1990.

Legaspe, E.P., Dias, E.M., "Open source fuzzy controller for programmable controllers". In *13th Mechatronics Forum Biennial International Conference, 2012.*

Lewis, E.E., 1995. *Introduction to Reliability Engineering.* 2º Ed., John Wiley&Sons.

Lundteigen, M.-A.; Rausand, M. Architectural constraints in IEC 61508: Do they have the intended effect ? *Reliability Engineering and System Safety,* pp. 520-525, Elsevier Science Publisher Ltd., 2009.

Miyagi, P.E., 2007. *Controle Programável – Fundamentos do controle de sistemas a eventos discretos*. Editora Edgard Blucher Ltda, São Paulo, SP, Brazil.

Modarres, M., Kaminskiy, M., Krivstov, V., 2010. *Reliability Engineering and Risk Analysis: a practical guide*. 2º Ed., CRC Press.

OSHAS18001, 2007. "International standard of occupational health and safety assessment services".

Popa, D. D., Craciunescu, A, Kreindler, L.: "A PI-Fuzzy controller designated for industrial motor control applications". In *ISIE IEEE International Symposium on Applications,* Industrial Eletronics, 2008.

Sallak, M.; Simon, C.; Aubry, J., A fuzzy probabilistic approach for determining safety integrity level, *IEEE Transaction on Fuzzy Systems,* vol 16, n. 1, pp. 239-248, 2008.

Santos Filho, D.J. 2000. *Aspectos do Projeto de Sistemas Produtivos*. PHD Thesis, Escola Politécnica da Universidade de São Paulo, Brazil.

Souza, E.A., 1995. *O treinamento industrial e a gerência de riscos – uma proposta de instrução programada.* Master Thesis, Universidade Federal de Santa Catarina, Brazil.

Squillante Jr, R.; Santos Fo, D.J.; Souza, J.A.L.; Junqueira, F,; Myiagi, P.E. "Safety in Supervisory Control for Critical Systems". *IFIP International Federation for Information Processing (DoCEIS 2013),* vol 394, pp. 261-270, ISBN: 978-3-642-37290-2, DOI: 10.1007/978-3-642-37291-9 2013.

Squillante Jr, R., Santos Filho, D., Riascos, L., Junqueira, F., Miyagi, P., 2011. "Mathematical method for modeling and validating of safety instrumented system designed according to IEC 61508 and IEC 61511. In *Cobem* 2011.

Summers, A.; Raney, G. Common cause and common sense, designing failure out of your safety instrumented systems (SIS). In: *ISA Transactions,* vol 38, pp. 291-299, 1999.

Wu, B; Xi, L.-F; Zhuo, B.-H. Service-oriented communication architecture for automated manufacturing system integration. *International Journal of Computer Integrated Manufacturing,* vol 21, n. 5, pp. 599-615, 2008.

Zadeh, L. A.: Fuzzy Logic = Computing with Words. In *IEEE Transactions on Fuzzy Systems,* Vol 4, nº 2, p. 103-111, 1996.

Zadeh, L. A.: *Fuzzy Sets. Information and Control*, Vol 8, p. 338-353, 1965.

Zhang, Y; Jiang, J. Bibliographical review on reconfigurable fault-tolerant control systems, *Annual Reviews in Control,* vol 32, pp. 229-252, 2008.

Zhang, Y; Jiang, J. Bibliographical review on reconfigurable fault-tolerant control systems, *Annual Reviews in Control,* vol 32, pp. 229-252, 2008.

8. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.