Mitigation Control of Critical Faults in Production Systems

Jeferson A.L. de Souza, Diolino J. Santos Fo, Reinaldo Squillante Jr., Fabricio Junqueira, and Paulo E. Miyagi

University of São Paulo, São Paulo, Brazil
{jeferson.souza,diolinos,reinaldo.squillante,
fabri,pemiyagi}@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, and 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, implemented by fuzzy logic.

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 [1], [2], [3]. Given this new scenario, industrial processes and their control are becoming more complex. Additionally, organizations have focused on policies to achieve and to demonstrate people's safety and health, environmental management system, and controlling risks.

L.M. Camarinha-Matos et al. (Eds.): DoCEIS 2014, IFIP AICT 423, pp. 119–128, 2014.

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 equipment [4]. Although many studies have been presented for diagnosis and treatment of faults, a review of fault-tolerant reconfigurable control system can be found in [5], but 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 [6], (ii) human operators do not have zero risk of error and (iii) there is no computational software project developed that can predict all the possibilities [7].

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 faults, and to bring the process to a safe state. In this sense, some safety standards such as IEC 61508 [8], IEC 61511 [9] among others, guide activities related with a SIS Safety Life Cycle (SLC), such as design, installation, operation, maintenance, tests and others [10], [11].

According to IEC 61508, the term "fault" is defined as an abnormal condition that can cause a reduction or loss of the ability of a functional unit, and is defined two layers of SIS: the prevention layer and the mitigation layer. Recently, [12] proposes the implementation of a SIS prevention layer.

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 [13], and the *What-If* technique [14], 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 [15], [16]. The effect of every critical fault, or safety instrumented function (SIF), results in mitigation actions, determined by the *What-If* technique yet implemented.

Fuzzy logic is utilized for the generation of the control algorithm. It has the advantage of not using differential equations or complex mathematical models for determining the dynamic behavior of the system [17], and can therefore use the proposed mitigation actions, which in turn were the result of applying the techniques of risk analysis, for the determination of fuzzy control algorithms. Another advantage of fuzzy logic is the analysis of the parameter time derivative [18], thus contributing to an anticipatory action of the proposed mitigation layer. The generation of control codes for programmable logic controllers (PLC) can be made based on IEC 61131-7 [19], which deals with the conversion of the generated fuzzy logic algorithm to conventional PLC languages, based on IEC 61131-3. [20].

2 Relationship to Collective Awareness Systems

Recent political awareness with focus on sustainability and recycling, the use of resources and raw materials from renewable resources, along with the practices of waste management and emission control of pollutants, coupled with more rigid and punitive laws to production systems that do not meet the new regulations, results in new control systems in manufacturing plants.

In this context, a mitigation control layer is needed because, in addition to the market requirements of competitiveness, such policies result in a choosing collective awareness of choice by consumers for companies committed to focus on the environment and sustainability. Besides the increase in the complexity of the control systems for these new requirements, the proposed mitigation layer, based on IEC 61508, is precisely the preservation of men and the environment, just required for productive systems that wishing to adapt to these new practices of collective awareness recently observed.

3 Proposal of Layer of Mitigating Control System

3.1 Description of the Proposed Method

The proposed method is summarized by the following five steps, described on sections 3.1.1 to 3.1.5 below:

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, 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 fault mode. According to IEC 61508, such sensors must be independent of the BPCS. To avoid spurious faults and reading errors, it is recommended to use redundant architectures [11], 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 Construction of Models for Implementation of Control Algorithms

In this step will be used results of the *What-If* technique already implemented in section 3.1.3 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.

3.1.5 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 61131-3 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 [24] ST (Structured Text) for the implementation in conventional PLCs.

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. The PI&D of a turbo compressor uni tis shown in Fig. 1.

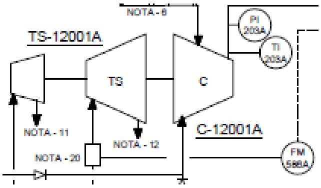


Fig. 1. P&ID of a compressor unit of the gas compression station

4.2 Application of the Proposed Method

We apply the proposed method, based on the SIS prevention layer proposed by [11] for the case of the 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 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 illustrates a FMEA for compressor, and Fig. 2 the FTA for the top event “High Temperature Lubricants Shaft”.

Table 1. Proposed FMEA for temperature increase of the lubricating oil of shaft bearing 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 Torque		Speed Control Condensate Excess			

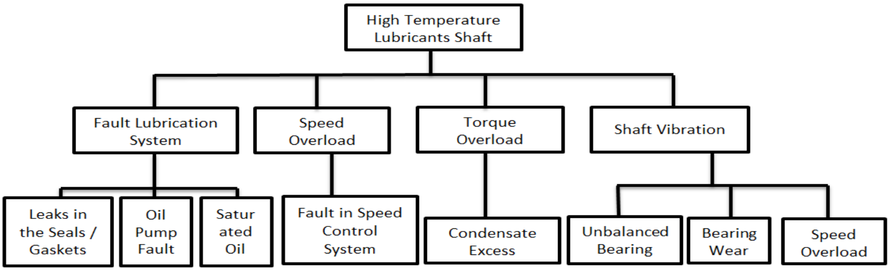


Fig. 2. Suggested FTA for the top event “High Temperature Lubricants Shaft”

Both FMEA and FTA found that an effect of occurrence of fault in the 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 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 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 [11] should 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 compressor, beside the action of shutdown from the prevention layer, suggested action to mitigate the effects is the forced cooling of the 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 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.

4.2.4 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. Fig. 3 illustrates the proposed model for temperature:

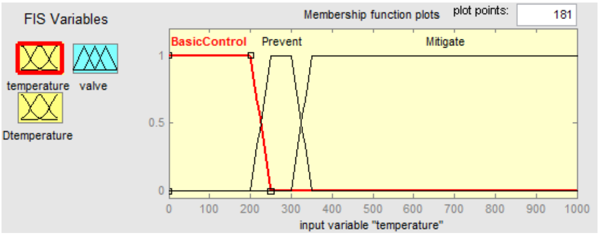


Fig. 3. Fuzzy Membership functions for temperature

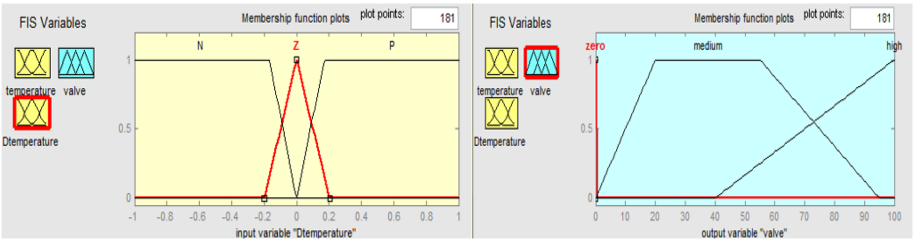


Fig. 4. and Fig. 5. Membership functions to temperature derivative and percentage of valve opening

According to the membership functions adopted in the Fig. 3 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.4 and Fig.5 illustrate the above.

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

Table 2. Fuzzy rules for mitigation layer

If	**Temperature**	**Operator**			
1	*Mitigate*				*High – 100% open*
2	*Basic Control*				*Zero - Closed*
3	*Prevent*	*And*	*P*		*Medium – 50%*
4	*Mitigate1*	*And*	*N*		*Medium – 50%*

The output signal, or the proportional action of mitigation, here designated by proportional valve opening, can be seen by the generated surface on Fig.6.

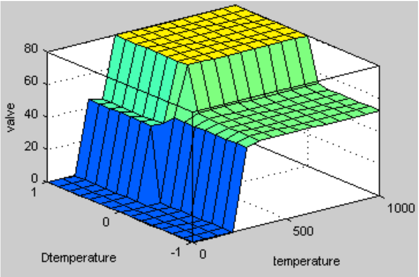
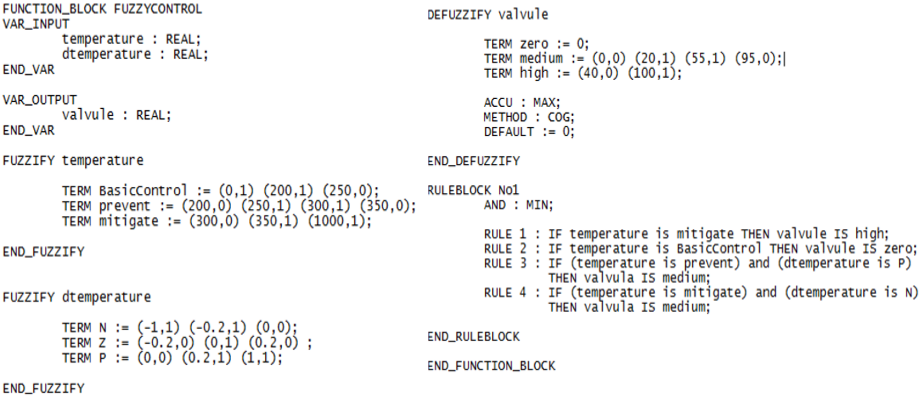


Fig. 6. Surface generated by the fuzzy algorithm by the fuzzy rules defined for the mitigation model

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.

4.2.5 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. 7.



```
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
```

Fig. 5. 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.

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

References

1. Chen, C., Dai, J.: Design and high-level synthesis of hybridcontroller. In: Proc. of IEEE Intern. Conf.of Networking, Sensing & Control (2004)
2. SantosFilho, D.J.: Aspectos do Projeto de Sistemas Produtivos. PHDThesis, Escola PolitécnicadaUniversidade deSãoPaulo, Brazil (2000)
3. Wu, B., Xi, L.-F., Zhuo, B.-H.: Service-oriented communication architecture for automated manufacturing system integration. Int. J. Computer Integrated Manufacturing 21(5), 599–615 (2008)
4. Sallak, M., Simon, C., Aubry, J.: A fuzzy probabilistic approach for determining safety integrity level. IEEE Transaction on Fuzzy Systems 16(1), 239–248 (2008)
5. Zhang, Y., Jiang, J.: Bibliographical review on reconfigurable fault-tolerant control systems. Annual Reviews in Control 32, 229–252 (2008)
6. Summers, A., Raney, G.: Common cause and commonsense, designing failure out of your safety instrumented systems (SIS). ISA Transactions 38, 291–299 (1999)
7. Miyagi, P.E.: ControleProgramável–Fundamentos do controle de sistemas a eventos discretos. Editora Edgard Blucher Ltda, SãoPaulo, SP, Brazil (2007)
8. IEC,I.E.C., Functional safety of electrical / electronic / programmable electronic safety-relatedsystems (IEC61508) (2010)
9. IEC,I.E.C., Functionalsafety-safety instrumented systems for the process industry sector-part 1(IEC 61511) (2003a)
10. Lundteigen, M.-A., Rausand, M.: Architectural constraints in IEC61508: Do they have the intended effect? In: Reliability Engineering and System Safety, pp. 520–525. Elsevier SciencePublisher Ltd. (2009)
11. Bell, R.: Introduction to IEC61508. In: Proceedings of ACS Workshop on Tools and Standards, Sydney, Australia (2005)
12. Squillante Jr., R., Santos Filho, D., Riascos, L., Junqueira, F., Miyagi, P.: Mathematical method for modeling and validating of safety instrumented system designed according to IEC61508 and IEC61511. In: InCobem 2011 (2011)
13. Modarres, M., Kaminskiy, M., Krivstov, V.: Reliability Engineering and Risk Analysis: apractical guide, 2nd edn. CRCPress (2010)
14. Souza, E.A.: O treinamento industrial e a gerência de riscos–uma proposta de instrução programada.Master Thesis, Universidade Federal de Santa Catarina, Brazil (1995)
15. Squillante Jr., R., Fo, D.J.S., de Souza, J.A.L., Junqueira, F., Miyagi, P.E.: Safety in supervisory control for critical systems. In: Camarinha-Matos, L.M., Tomic, S., Graça, P. (eds.) DoCEIS 2013. IFIP AICT, vol. 394, pp. 261–270. Springer, Heidelberg (2013)

16. Cavalheiro, A., Santos Fo, D., Andrade, A., Cardoso, J.R., Bock, E., Fonseca, J., Miyagi, P.E.: Design of supervisory control system for ventricular assist device. In: Camarinha-Matos, L.M. (ed.) Technological Innovation for Sustainability. IFIP AICT, vol. 349, pp. 375–382. Springer, Heidelberg (2011)
17. Popa, D.D., Craciunescu, A., Kreindler, L.: API-Fuzzy controller designated for industrial motor control applications. In: ISIE IEEE International Symposium on Applications, Industrial Eletronics (2008)
18. Legaspe, E.P., Dias, E.M.: Open source fuzzy controller for programmable controllers. In: 13th Mechatronics Forum Biennial International Conference (2012)
19. IEC,I.E.C., Programmable Controllers IEC 61131-7: Fuzzy Control programming (2000)
20. IEC,I.E.C., Programmable controllersIEC61131-part 3: Programming languages (2003b)