Reliability Engineering and System Safety 180 (2018) 425–433

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Failure modes, mechanisms and effect analysis on temperature redundant sensor stage

M. Catelani, L. Ciani*, M. Venzi

Department of Information Engineering (DINFO), University of Florence, Via S. Marta 3, Florence 50139, Italy

ARTICLE INFO

Keywords:
FMEA
FMECA
FMMEA
Failure mechanism
Safety instrumented system
SIS
Sensors
Temperature transmitter
Condition monitoring
Diagnosis

ABSTRACT

This paper focuses on failure analysis using two techniques developed from Failure Mode and Effect Analysis (FMEA), one of the most used methodologies to determine causes and consequences of failures: Failure Mode, Effect and Criticality Analysis (FMECA) and Failure Modes, Mechanisms and Effect Analysis (FMMEA). In this paper their combination is shown to optimize the benefits of both and overcome their drawbacks. This approach ensures high efficiency throughout equipment design and guarantees suitable maintenance policies. It has been applied in a redundant architecture based on temperature sensors included in a Safety Instrumented System for Oil&Gas application.

1. Introduction

The reliability and maintenance policy, adopted in the design and operational period in order to minimize the downtime and preserve the system functionality, influence the functional profile of any system [1]. Failure Mode Effect and Criticality Analysis (FMECA) in taken into account as an effective methodology to enhance the system functional profile. While Failure Modes Mechanisms and Effects Analysis (FMMEA) that focuses on mechanisms of the failures and assists in updating the maintenance policies to cope with operational profile.

The paper analyzes a new approach introduced to overcome the drawback of traditional FMECA and FMMEA, and test it on a complex system used in safety loop operation.

A safety loop (i.e., Safety Instrumented System) is a process involving three stages (sensor, logic solver and actuator) in order to detect a failure, elaborate the collected data and perform a corrective action [2]. Safety instrumented systems (SIS) are used in Oil&Gas industry to detect hazardous events, and to perform required safety actions to maintain or bring the process back to a safe state [3].

Fault diagnosis is mandatory (in particular for Oil&Gas applications) where products are forced to endure extreme process and environmental conditions [4–6].

2. Failure Mode, Effect and Criticality Analysis (FMECA)

FMECA was, firstly, introduced, in 1950s, by U.S. military and it was developed and applied by NASA, in 1960s, to verify reliability of space programs. By 1990s, many international standards were published for different applications of FMECA. Nowadays, it becomes one of the most powerful methods used for risk assessment and maintenance management [7].

FMECA is one of the most used techniques for failure analysis in particular during design stage of new systems. This method is an inductive analysis method that starts from the lowest level (single component) and continues analyzing the upper hierarchical level.

FMECA is composed of two separates analysis, the Failure Mode and Effects Analysis (FMEA) and the Criticality Analysis (CA) [8–11]. The first analysis list:

- the probable item failure modes;
- causes of these failure modes;
- the effects of failure on local level and global level (i.e., referred to the effect of each breakdown on the equipment and the whole system respectively);
- the corrective actions suggested to prevent each failure.

In order to achieve a priority ranking of the identified failure modes

* Corresponding author.
E-mail address: lorenzo.ciani@unifi.it (L. Ciani).

https://doi.org/10.1016/j.ress.2018.08.013
Received 28 February 2018; Received in revised form 17 August 2018; Accepted 26 August 2018
Available online 27 August 2018

Table 1
Rules for the criticality index assessment.

Criticality Index	Influence Factor	Rating
Severity **S**	Effects of the failure on the system, on the operator and on the environment	1 2 3 4 5 6 7 8 9 10 **Low Max**
Occurrence **O**	Probability that a failure will happened (failure rate)	1 2 3 4 5 6 7 8 9 10 **Low Max**
Detection **D**	Possibility of diagnose the failure	1 2 3 4 5 6 7 8 9 10 **Max Low**

and effect the second analysis (Criticality Analysis) is performed. This ranking is obtained using a quantitative index, Risk Priority Number (RPN), given by [12]:

$$RPN = S \cdot O \cdot D \tag{1}$$

Where:

- Severity S defines the strength of failure impact on the system. It can assume integer values belong to the interval [1; 10] where 10 represents the worst scenario.
- Occurrence O is the probability that a failure mode will happened, therefore it is strongly linked to the failure rate of the equipment. It can assume integer values belong to the interval [1; 10] where 10 is associated to the most probable failure mode.
- Detection D indicates the possibility of diagnose the failure mode before its effects are manifested on the system. It can assume integer values belong to the interval [1; 10] where 10 is associated to the least diagnosable event.

Table 1 shows the factor that influence the criticality index and the rules to assess the rating to each one. Table 2 explains how the O, S and D values should be assigned and the meaning of each score.

According to these considerations, the RPN index can assume value in [1; 1000] and the higher RPN indicates the necessity to resolve the failure mode with maximum priority and speed. The main drawbacks connected with FMECA are [13–14]:

- it is limited to the design phase
- only failure modes are considered regardless of the mechanisms of these modes
- failure rates are not constant
- large sensitivity to small changes of criticality index
- duplications resulted from several combinations of different factors that lead to same RPN

In literature there are several formulae for RPN calculation in order to change the priority ranking assessment such as ERPN - Exponential Risk Priority Number, which substitutes the multiplication function with an exponential function of Severity, Occurrence and Detection [15], and URPN which is based on UGF - Universal Generation Function [16]. Anyway, in this study the standard RPN ranking procedure was used since it is suitable for Oil&Gas applications.

The following assumptions have been made for FMECA assessment:

- series configuration
- working in the useful life section of the bathtub curve that describes the failure rate function (i.e., constant failure rate)
- propagation of failures is not relevant
- stress levels comparable to the Ground Fixed classification of MIL-HNBK-217F

In [17] a different method is proposed to model failure behavior using qualitative data based on the judgment of experts in case data are not sufficient. Different configurations are taken into consideration (not just series) and also the costs of corrective actions. In this paper the series configuration is preferred anyway because the worst-case is still necessary in Oil&Gas critical applications.

Table 2
Complete Rules for the criticality index assessment.

S	O	D	Score
Insignificant	Improbable	Automatic detection with warning	1–2
Marginal	Remote	Automatic detection without warning	3–4
Critical	Occasional	Detected by the operator	5–6
Very critical	Probable	Impossible to detect by the operator	7–8
Catastrophic	Frequent	Impossible to detect	9–10

3. Failure Modes Mechanisms and Effect Analysis (FMMEA)

The center of advanced life cycle engineering at the University of Maryland recently has improved FMEA procedure by introducing the FMMEA [18]. FMMEA does not investigate the failure mode causes but it considers the mechanisms of these failures and tries to improve the maintenance activities. Thus, unlike FMECA method, FMMEA approach prioritizes the failure mechanism and the maintenance policies in order to cope with the operational profile. The failure mode is a manner in which a failure manifests itself in the system and failure mechanisms are the processes by which physical, electrical, chemical and mechanical stresses induce failures individually or in combination [19]. It aims to the proper selection of the failure mechanism parameters in order to determine the proper failure precursors for a health monitoring for the system. In general, a precursor is a change in a measurable variable that can be associated with subsequent failure [20].

FMMEA is developed on the basis of both FMEA and CA techniques, and it does not investigate the failure mode causes. Instead, it focuses on the mechanisms of these failures. Afterwards, Criticality analysis is evaluated through RPN by considering occurrence and severity of each mechanism (Section 2).

This way FMMEA enhances the value of FMECA by identifying the high priority failure mechanisms and helps create a plan to mitigate the effects: after all potential failure modes, causes, mechanisms, and models are identified for each element, the prioritization is made based on the life-cycle environmental and operating conditions.

In order to identify the possible failure mechanisms of the equipment, the FMMEA procedure is applied at the end of the design phase, and the steps necessary to implement the approach are shown in Fig. 1.

The first step is to identify the life cycle (including transportation, handling, installation, and operation of the equipment in the system). The Life cycle must take into account some limits, such as temperature, relative humidity and pressure in environmental field, or mechanical stress, voltage and current in operational field.

As can be seen in Fig. 1 the FMMEA is developed on the basic of FMECA approach, since after the first step, where it is necessary to study the system, the method focuses on identify failure modes and failure causes. Then, the failure mechanisms' parameters are identified which are crucial to determine the physics to failure model and monitored failure precursor. Physics of a failure model defines the connection between the time to failure, products' environmental and operational conditions [21]. For that reason, this approach prioritizes the failure mechanism analyzing both monitoring precursors to failures and physics to failure modeling. Generally, these two assessment can be used simultaneously or separately based on the capability to monitor the pre-defined failure mechanisms parameters.

The step of prioritize mechanisms contains several sub-steps such as [22]:

- evaluating failure susceptibility
- assign occurrence of mechanisms
- assign severity level of mechanisms.