Applied Mathematical Sciences, Vol. 6, 2012, no. 36, 1747 - 1758

A Model of the Failure Detection Based on Fuzzy Inference System for the Control Center of a Power System

Sohrab Khanmohammadi[1] **, Kamran Rezaei**[2] **, Javad Jassbi**[1]
and Shabnam Tadayon[3]

[1] Department of Industrial Management, Science and Research Branch
Islamic Azad University, Tehran, Iran
[2] Department of Industrial Engineering, Tehran University, Tehran, Iran
[3] Department of Industrial Management, Science and Research Branch
Islamic Azad University, Tehran, Iran

Abstract

Power network stability requires a timely failure detection and operator reaction. The protection devices and operators have responsibilities for the failure detection in a power system. In other words, alarms being received from the protection devices are displayed to the operator by SCADA to respond to the respective appropriate and timely actions to be done. This article is a part of a risk assessment study on the alarm of power system control centers using the Failure Modes and Effects Analysis (FMEA) that seeks to assess the failure detection in power system. Failure detection evaluation is a subjective case and experts have usually problems with that. In this research, we identify factors that may influence the failure detection, so that experts could assess a failure detection score with an objective criterion. In this study a new definition for the detection scale is presented and relay performance probability is formulated from the viewpoint of the signal detection theory and the Bayes rule. In this paper we treat the effective factors as fuzzy variables and evaluate them using fuzzy inference system. The main advantages of the proposed fuzzy detection score are involving human reliability factors in addition to relay performance and modifying detection score.

Keywords: Failure Mode and Effects Analysis, Detection Score, Fuzzy Inference System, Control center of power system, Bayes rule

Introduction

FMEA is a preventative method that helps removing potential failures before they occur in a process, product or a system. This method has a main role in potential failure appearance and gives planned responses to failures. Therefore, FMEA is known as an effective environment for the risk management.

The risk assessment depends on three variables: Failure occurrence (O), Severity of consequences(S) and detection of failures (D). In this research, we focus on detection variable and prepare a specific model for the failure detection in a control center.

Detection probability (D) means probability to detect the failure mode/causes. There are two definitions for detection probability in FMEA:

- Probability that the failure to be detected prior to a customer.
- Probability that the failure to be detected by a customer prior to a disaster.

Table 1: Crisp ratings for detection of a failure (Wang, Chin, Poon, Yang; 2003)

Rating	Detection	Likelihood of detection by design control
10	Absolute uncertainty	Design control can not detect potential cause/ mechanism and subsequent failure mode
9	Very remote	Very remote chance the design control will detect potential cause/ Mechanism and subsequent failure mode
8	Remote	Remote chance the design control will detect potential cause/ Mechanism and subsequent failure mode
7	Very low	Very low chance the design control will detect potential cause/ Mechanism and subsequent failure mode
6	Low	low chance the design control will detect potential cause/ Mechanism and subsequent failure mode
5	Moderate	Moderate chance the design control will detect potential cause/ Mechanism and subsequent failure mode
4	Moderately high	Moderately high chance the design control will detect potential cause/ Mechanism and subsequent failure mode
3	High	High chance the design control will detect potential cause/ Mechanism and subsequent failure mode
2	Very high	Very high chance the design control will detect potential cause/ Mechanism and subsequent failure mode
1	Almost certain	Design control will detect potential cause/ mechanism and subsequent failure mode

Two definitions have important differences. Probability improvement of failure detection by customer is critical but it should be considered as the last solution. The little value for a rating means that the control devices will detect potential causes and subsequent failure mode prior to being received by a customer or the next operation. Number 10 for rating means the control devices cannot detect potential causes and subsequent failure mode. Thus, the company will be informed about the failure occurrence by a customer's complain.

Detection score had been criticized by researchers. One of its drawbacks is that the detection criterion is subjective and based on people's expertise. Rhee and Ishii

(2003) addressed the difficulty of traditional FMEA in consequences severity and detection determination and introduced a new methodology called, Life Cost-Based FMEA, which measured failure/risk in terms of cost. Kmenta and Ishii (2000) addressed a major problem with the conventional FMEA approach: The Detection index does not accurately measure a contribution to risk. Therefore they suggest organizing the FMEA around failure scenarios rather than failure modes. The other drawback is detection scale Table assumed that the received information is a signal. But the control devices may receive noise. Based on a Signal Detection Theory (SDT), there are four states.

Table 2: Signal and noise detection (Source: Lee, 2008)

	Respond absent	Respond present
Stimulus present	Miss	Hit
Stimulus absent	Correct rejection	False Alarm

In the FMEA method, only "Hit" and "Miss" options are considered. The “Correct Rejection” and “False Alarm” are ignored. If the control devices function properly, they don’t response to noise and so it rejects (correct rejection). If control devices receive noise but act as signal, false alarm is sent. In this article, first we identify factors that influence a failure detection and then we will propose a failure detection framework based on Fuzzy Inference System (FIS) and the modify detection scale Table and will suggest a method to modify detection device probability. Finally, model validation and system results will be discussed.

Failure detection effective factors

Protective systems monitor the system conditions such as: voltage, current unbalance, current input and output power to or from transformer, transformer winding temperature and other quantities. If conditions are abnormal, the protective relay will feel that and line/protective equipments will be disconnected from the power system.

In systems which are controlled by human or machine, failure detection is important. In detection scale provided by the classic FMEA, it is assumed that received information from control devices is a signal. But control devices may receive noise. If control equipments operate properly, they could reject noise. If they cannot identify noise, they will send false alarm. In classic FMEA, if control devices identify a potential failure mode or cause, the score 1 will be assigned to detect factor and if control devices could not identify a potential failure mode or subsequent failure, the score 10 will be assigned to detect the factor. Detection scale does not consider “no response” option of detection devices. The focus of this research is an alarm system in the power system control center. Therefore there is another control for failure detection. The other control is an operator control. Operator tries to detect failures and control power network, using alarm system information. Alarm system performance and its characteristics may increase or decrease operator's control and an on time failure detection. Human Reliability Analysis helps studying this subject. Hacker (1998) defines human reliability analysis as human capability for accommodate to changing conditions on disturbance (Peka Peyy, 2000). The important methods for human reliability analysis are THERP, TESEO, HEART, PROF, INTENT and TRC. TESEO is designed by Bello and Colombari (1980) for assessing an operator failure rate in power plant control center (Laurids Boring; 2008). This method is an empirical technique that is used for operator's failure estimation and to calculate a Human Error Probability (HEP).

$$HEP = k_1.k_2.k_3.k_4.k_5 \tag{1}$$

k_1: Primary failure rate of work in progress

k_2 : Available time for work in progress

k_3: Operator's characteristics and training

k_4: Operator's fatigue

k_5 : Ergonomically characteristics

Other model named as TRC (Time reliability Correlation) was introduced for the reliability of power system operator and his response to the critical events. This problem is known as "the human-machine time related interaction". TRC database is a Human Cognitive Reliability (HCR) model (Laurids Boring; 2008). Alarm ambiguity/ transparency, multiple alarm for single failure, alarm grouping, number of alarms that display on CRT in a time unit are other factors that could influence primary failure rate of performing activity (k_1). In the following lines, we will explain every factor:

- Alarm ambiguity: To the extent that the alarm is more transparent, to the same extent, the probability of failure detection will increase.
- Multiple alarms for single failure: If a single failure has multiple alarms that are sent from several substations, the operator might be confused and his detection capability could decrease.
- Number of alarms display on CRT in a time unit: Increasing the number of alarm, the operator has a little time to manage alarms and then probability of failure detection may be reduced. If alarms average rate is reduced, probability of failure detection will be increased.

Other factor that may effect failure detection includes:

- Alarm repetition: Some alarms have a low value but are repeated in the short time intervals. Some alarm types includes: out of service alarms, alarms which are status indications rather than warnings, alarms due to faults which are awaiting maintenance, alarms from equipment undergoing maintenance or routing testing, alarms not appropriate in the current operating mode, alarms from the regular operation of on-off control systems, several alarms caused by one initiating event, etc. If an alarm to be repeated at different times, the operator sensitivity to alarm will be reduced.

- Alarm handling experience: successful/unsuccessful alarm handling provides a perception in operator about his capability. Operator may also expand his perception in various situations.

The proposed model for the failure detection score

This research concentrates on the risk assessment system in a control center. Failure detection is done in two stages: detection by relay, detection by operator.
For the estimation of failure detection by relay, relay performance history and success times of each relay should be identified. The relay reaction can be of four types: Proper failure detection (Hit), no detection of failure (Miss), false alarm, and a correct rejection of noise.

Finally, as stated, the alarm ambiguity, the number of alarms for a single failure, the alarm average rate, the alarm repetition, and the alarm management history are the types of influenced failure detections by an operator.

Methodology of a detection assessment

Fuzzy inference system (FIS) is based on If-Then rules, so, using rules, it could connect multiple input variables to output variable. FIS could be utilized as a forecasting model when input/output data has some uncertainties. Detection assessment methodology is based on FIS, therefore it provides a flexible way for recognizing their effective factors and modeling. Input variables are fuzzified by the fuzzy membership functions and they are imported to fuzzy inference engine. In a fuzzy inference engine, expert's knowledge about failure detection is converted into If-Then rules. Fuzzy inputs are assessed by fuzzy inference engine and finally output or detection score is defuzzified. In the suggested model, three fuzzy inference systems will be used.

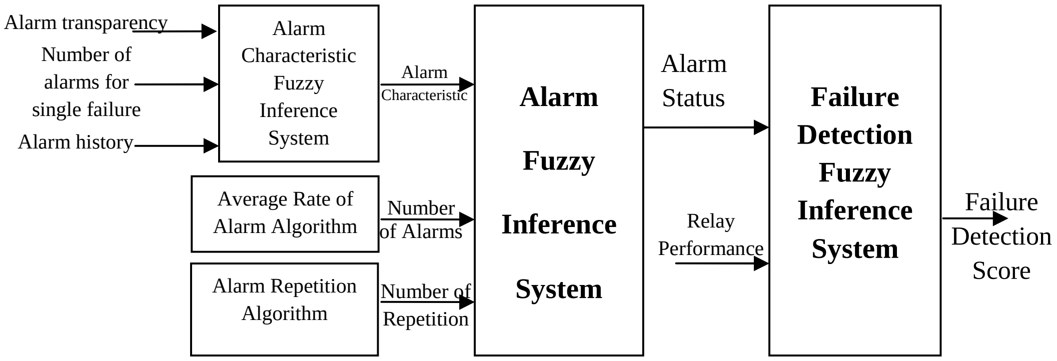

Alarm transparency
Number of alarms for single failure
Alarm history
Alarm Characteristic Fuzzy Inference System
Alarm Characteristic
Average Rate of Alarm Algorithm
Number of Alarms
Alarm Repetition Algorithm
Number of Repetition
Alarm Fuzzy Inference System
Alarm Status
Relay Performance
Failure Detection Fuzzy Inference System
Failure Detection Score

Figure 1: The suggested framework for the failure detection score

At the beginning, the input data should be fuzzified and their membership degree to be determined. For this purpose, the triangular membership function is used.

In order to show the two variables of Alarm status, the Relay Performance, also triangular membership function is used. The descriptive words which were used for describing these variables are: very low, low, medium high and very high.

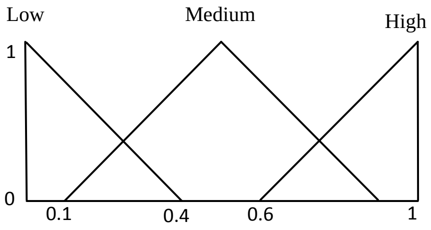


Figure 2: Input variables Fuzzy Membership Function

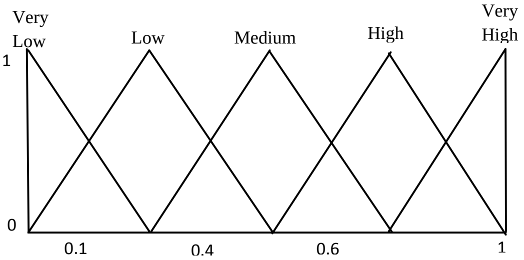


Figure 3: Fuzzy Membership Function of the variables of Alarm Status and Relay Performance

The output variable (Detection score) is also shown with the triangular fuzzy membership function and with descriptive words of very low, low, medium, high and very high.

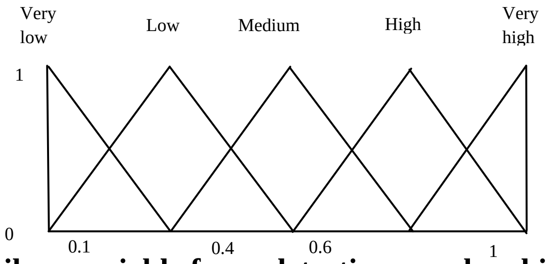


Figure 4: Failure variable fuzzy detection membership function

Also, to assign a proper linguistic score to relay performance variables (Figure 1), the Bayes rule is used. As later stated, four states may occur for detection equipment (Table 2): Miss, hit, correct rejection and false alarm. In traditional detection scale table, score 1 indicates control devices can detect occurrence of a failure mode and its causes and score 10 indicates control devices can't detect occurrence of failure mode and its causes. In this scale, miss and hit states are considered and correct rejection and false alarm have been ignored. First, we will modify the Table of failure detection score. In this table (table 3), four states are considered.

To assign a proper score to relay performance (figure 1), Bayes rule is used. As stated earlier, relay may perform in four states: hit, false alarm, miss, correct rejection. In following formula, posterior probability of four states is calculated in formulas 2, 3, 4 and 5.

Table 3: A suggested detection probability scale Table

Rank	Detection capability	Detection probability control devices
10	certainty	Control devices can not detect occurrence/nonoccurrence of failure mode and its causes
9	Remote	There is a very remote chance for occurrence/nonoccurrence of failure mode and its causes
8	Relatively remote	There is a relatively remote chance for occurrence/nonoccurrence of failure mode and its causes
7	Very low	There is a very low chance for occurrence/nonoccurrence of failure mode and its causes
6	Low	There is a low chance for occurrence/nonoccurrence of failure mode and its causes
5	Moderate	There is a moderate chance for occurrence/nonoccurrence of a failure mode and its causes
4	Relatively high	There is a relatively high chance for occurrence/nonoccurrence of a failure mode and its causes
3	High	There is a high chance for occurrence/nonoccurrence of a failure mode and its causes
2	Very high	There is a very high chance for occurrence/nonoccurrence of a failure mode and its causes
1	Certainty	Control devices can detect occurrence/nonoccurrence of a failure mode and its causes

$$P(A_1|B_1)=\frac{P(B_1|A_1)\times P(A_1)}{P(B_1|A_1)\times P(A_1)+P(B_1|A_2)\times P(A_2)} \quad (2)$$

Formula (1) is the posterior probability of A_1 given B_1 or correct rejection (Hit).

In this equation:

A_1: Response

A_2: No response

B_1 : Stimulus present

$P(A_1|B_1)$: posterior probability of A_1 given B_1 (Hit probability)

$P(A_1)$: Relay response probability

$P(A_2)$: Relay no response probability

$$P(A_1|B_2) = \frac{P(B_2|A_1) \times P(A_1)}{P(B_2|A_1) \times P(A_1) + P(B_2|A_2) \times P(A_2)} \tag{3}$$

$P(A_1|B_2)$: posterior probability of A_1 given B_2 (false alarm probability)

$P(B_2|A_1)$:conditional probability of having response(A_1) if the stimulus is absent (B_2)

$P(B_2|A_2)$:conditional probability of having no response (A_2) if the stimulus is absent (B_2)

$$P(A_2|B_1) = \frac{P(B_1|A_2) \times P(A_2)}{P(B_1|A_1) \times P(A_1) + P(B_1|A_2) \times P(A_2)} \tag{4}$$

$P(A_2|B_1)$: posterior probability of A_2 given B_1 (Miss probability)

$$P(A_2|B_2) = \frac{P(B_2|A_2) \times P(A_2)}{P(B_2|A_1) \times P(A_1) + P(B_2|A_2) \times P(A_2)} \tag{5}$$

$P(A_2|B_2)$: posterior probability of A_2 given B_2 (Correct rejection probability)

On the other hand:

$$P(A_1|B_1) + P(A_1|B_2) = 1 \tag{6}$$

$$P(A_2|B_1) + P(A_2|B_2) = 1 \tag{7}$$

That means:

$$P(A_1|B_1) + P(A_1|B_2) + P(A_2|B_1) + P(A_2|B_2) = 2 \tag{8}$$

"Correct performance (Hit)" and "correct rejection" are proper relay performance and probability aggregation determines the correct detection and no detection status by control devices. For example, if probability is equal 0.4, then relay correct response probability will be 0.2.

$$P_{CorrectDetection} = \frac{P(A_1|B_1) + P(A_2|B_2)}{2} \tag{9}$$

The Correct detection probability ($P_{CorrectDetection}$) is converted into a linguistic term using Fig 3. If $P_{CorrectDetection}$ is equal to zero that means relay performance is “very bad” and if $P_{CorrectDetection}$ is equal 1, the relay performance is “very good”. Figure 5 is the three dimension perspectives of rules. X and Y dimensions show the relay performance and alarm status and Z dimension shows a detection score.

Experts have proper experience and knowledge about a system behavior. Multiple experts with different knowledge and expertise are selected to construct If-Then rules. Building a fuzzy if–then rule base is thought to be tedious and critical to fuzzy FMEA (Wang etal,2009). Braglia et al. (2003), Tay and Lim (2006), Pillay and Wang (2003), are used rule reduction techniques to reduce sizes of rule base (Wang etal,2009). On the other hand, Similarity technique looks for rules that antecedent part is similar then consequence part should adjust. Lee, Chen and Liu (2002) have represented methods for fuzzy rule inconsistency resolution and fuzzy rule insertion for fuzzy neural networks. By using these methods, rule inconsistencies are detected and removed. They have used trapezoidal LR-type membership function. In this research, we apply similarity and rule reduction concepts to this aims: First, similar rules are removed from rule base or merge together. Therefore, the quickness of inference increases. Second, if antecedent part has a relative similarity, consequence part should have a relative similarity. For examining rules similarity, we prepare a simple algorithm. The algorithm compares rules in pairs. Input variable membership functions compare in pairs by formula 10.

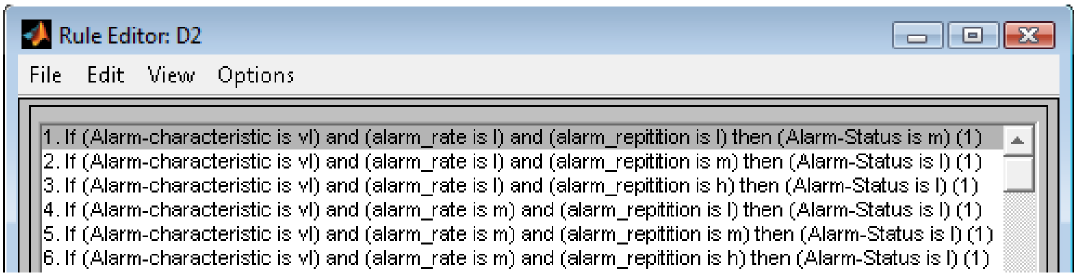
$$Sim_i = \frac{Min(\mu_A(x), \mu_B(x))}{Max(\mu_A(x), \mu_B(x))} \qquad (10)$$

Then the general antecedent similarity is calculated as Formula 3:

$$SimTotal = \sum_{i=1}^{n} Sim_i \times W_i \qquad (11)$$

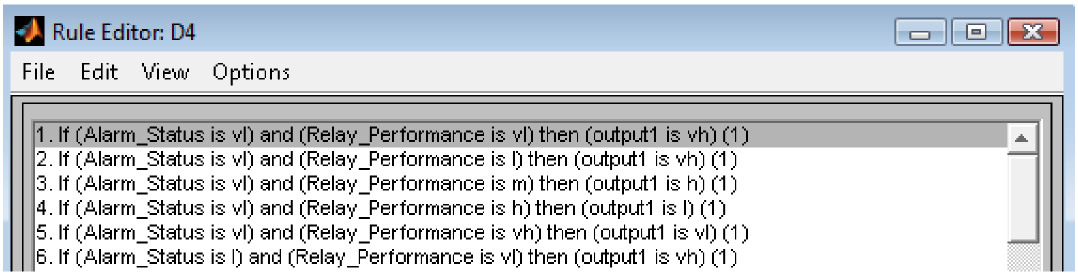
W_i : If input variables have weight, this weight should be multiplied by similarity score. If variables have the same weights, the score one is assigned to weights.

For comparing consequence part, formula 10 could be used. To carry out this algorithm, we provide a program in Matlab software and program outputs write in Excel file format. Then, similar rules are detected. Some similar rules that have redundancy, is removed from rule base. Finally, for three fuzzy inference systems, expert's knowledge is converted to 91 If-Then rules. As stated above, we use similarity algorithm (formula 10) to determine inconsistent rules and modify them. The format of rules framed in the research is shown in figures 5 and 6.



1. If (Alarm-characteristic is vl) and (alarm_rate is l) and (alarm_repitition is l) then (Alarm-Status is m) (1)
2. If (Alarm-characteristic is vl) and (alarm_rate is l) and (alarm_repitition is m) then (Alarm-Status is l) (1)
3. If (Alarm-characteristic is vl) and (alarm_rate is l) and (alarm_repitition is h) then (Alarm-Status is l) (1)
4. If (Alarm-characteristic is vl) and (alarm_rate is m) and (alarm_repitition is l) then (Alarm-Status is l) (1)
5. If (Alarm-characteristic is vl) and (alarm_rate is m) and (alarm_repitition is m) then (Alarm-Status is l) (1)
6. If (Alarm-characteristic is vl) and (alarm_rate is m) and (alarm_repitition is h) then (Alarm-Status is l) (1)

Figure 5: Format of If-Then rules for 'Alarm fuzzy inference system'



1. If (Alarm_Status is vl) and (Relay_Performance is vl) then (output1 is vh) (1)
2. If (Alarm_Status is vl) and (Relay_Performance is l) then (output1 is vh) (1)
3. If (Alarm_Status is vl) and (Relay_Performance is m) then (output1 is h) (1)
4. If (Alarm_Status is vl) and (Relay_Performance is h) then (output1 is l) (1)
5. If (Alarm_Status is vl) and (Relay_Performance is vh) then (output1 is vl) (1)
6. If (Alarm_Status is l) and (Relay_Performance is vl) then (output1 is vh) (1)

Figure 6: Format of If-Then rules for 'Failure detection fuzzy inference system'

As shown in Figure 7, each input variable tends toward zero, the possibility of failure non detection will increase.

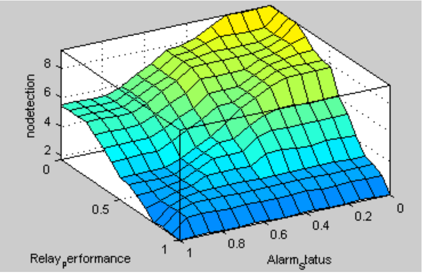


Figure 7: A graphical representation of input variables and a detection score

Model verification

Model verification is done from two points of view: structural, behavioral. For model examination from structural view, conceptual model is examined by experts and mathematical model using similarity algorithm is checked. For a model validation from behavioral view, extreme condition test is used.

Model examination by experts: To identify factors that influence detection score, we reviewed researches and interview with experts. Then, to verify suggested model, a questionnaire was prepared and questionnaire validation and reliability are examined. For examining questionnaire validation, questionnaire was distributed among five experts. Finally, one question was modified. In the next step, for examining questionnaire reliability, Cronbach's Alpha was used. Cronbach's (alpha) is a coefficient of reliability. It is commonly used as a measure of the internal consistency of a psychometric test score. Results showed questionnaire reliability (0.838). Finally, the questionnaire was distributed among 16 experts. Received answers showed expert acceptance to alarm transparency, number of alarms for single failure, alarm history, average rate of alarm and alarm repetition and relay performance factors.

Extreme condition test: The purpose of this test is to know whether the system in extreme conditions produces appropriate and desired responses and adjust outputs with a necessary sensitivity. Therefore, input variables including ‘alarm ambiguity’, ‘number of alarms for single failure’, ‘alarm history’, ‘average rate of alarm’ and ‘alarm repetition’ are adjusted in extreme conditions. By the way, in the cases which do not provide expected response, they are determined and related rules are modified. Finally, “operator’s readiness” and “network status” were tested. Output variable is ranged from 1 to 10. In Table 4, results of extreme condition test for “Failure Detection FIS” are shown.

Table 4: Results of extreme condition test for detection model

Alarm Status	Relay performance	Detection Score
0	0	9.2
0.5	0.5	5
1	1	0.8

An illustrative example

The following Table shows some failure modes. In six right columns, input variables are listed. Using the proposed model, the detection score (D) is obtained.

Table 5: An illustrative example for detection score

Alarm ambiguity	Alarm history	Alarm unique	Average rate of alarm	Alarm onrepetiti	Relay performance	Failure detection
Low	Bad	Low	Moderate	Low	Very good	1.72
Low	Bad	Low	Moderate	Low	Bad	7.75
Low	Bad	Low	Moderate	Low	Very bad	9.2
High	Moderate	Moderate	High	Low	Moderate	5.5
High	Good	ghHi	High	High	Very bad	7.8
Low	Bad	Low	High	High	Very bad	9.2
Moderate	Moderate	Moderate	Low	High	Bad	7.2

Conclusion

FMEA is a systematic method which determines and prevents failures in process and product before they occur. Its goal is to prevent defects, improve safety and satisfy customer (Mc Dermott, 2009). FMEA has difficulties in exact assessment of risk factors (O, S, D). This article represents a method based on fuzzy inference system to assess detection variable. First, factors that influence failure mode detection are identified. Then a model is suggested based on a fuzzy inference system. The detection scale score is modified and relay performance is calculated using the Bayes theory. Next, model validation is reviewed from two points of views. Finally, an illustrative example is presented. The model strengths include:

- To assess the detection variables, the ‘alarm status’ and ‘relay performance’ are considered together. The ‘alarm status’ affects operator failure rate. Therefore, we have combined operator failure factors in control center with relay performance. This is a new work in failure detection assessment and risk assessment for a control center.
- We have identified factors that influence the failure detection and have provided a model to determine D score. By the way, an exact method is presented for D assessment.
- To determine the relay performance score, we apply signal detection theory concept and Bayes rule. This method have changed classic view of FMEA to detection score and Hit, false alarm, Miss and Correct rejection probabilities are calculated. Therefore, a mechanism is presented to evaluate correct relay response probability and more exact criteria for response assessment are provided.

Acknowledgements. The work described in this article was financially supported by Khorasan Regional Electric Company (KREC).

References

1. A. Pillay, J. Wang, Modified failure mode and effects analysis using approximate reasoning , Reliability Engineering and System Safety, 79 (2003), 69–85.
2. H. M. Lee, J. M. Chen, C. L. Liu, Inconsistency Resolution and Rule Insertion for Fuzzy Rule-Based Systems, Journal of Information Science and Engineering, 18(2002),187-210
3. K. M. Tay, C. P. Lim, Fuzzy FMEA with a guided rules reduction system for prioritization of failures, International Journal of Quality & Reliability Management, 23(2006), 1047-1066.
4. M. D. Lee, BayesSDT: Software for Bayesian inference with signal detection theory, Behavior Research Methods, 40 (2008),450-456
5. M. L. Bransby, J. Jenkinson, The Management of Alarm Systems, Bransby Automation Ltd & Tekton Engineering, Norwich, 1998
6. M. Braglia, M. Frosolini, R. Montanari , Fuzzy criticality assessment model for failure modes and effects analysis, International Journal of Quality & Reliability Management, 20 (2003), 503-524.
7. P. Pekka, Reliability Analysis Methods for Probabilistic Safety Assessment, Technical Research Centre of Finland, 2000.
8. R. E. McDermott, R. J. Mikulak, M. R. Beauregard, The Basics of FMEA, CRC Press Taylor & Francis Group, New York, 2009
9. R. Laurids Boring, Human Reliability Analysis in Cognitive Engineering and System Design, Sandia National Laboratories, New Mexico, 2008.
10. S. J. Rhee, K. Ishii, Life Cost-Based FMEA Incorporating Data Uncertainty, Proceedings of DETC2002 ASME2002 Design Engineering Technical Conferences, Quebec, 2002.
11. S. Kmenta, K. Ishii, Advanced FMEA Using Meta Behavior Modeling for Concurrent Design of Products and Controls, Proceedings of DETC ’98 1998 ASME Design Engineering Technical Conferences, Atlanta, 1998.
12. Y. M. Wang, K. S. Chin, G. K. K. Poon, J. B. Yang, Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean, Expert Systems with Applications, 36(2009).

Received: October, 2011