Journal of Dynamics, Monitoring and Diagnostics, 2025, 4, 44-52
https://doi.org/10.37965/jdmd.2025.717

ISTP
RESEARCH ARTICLE

A Novel Approach to Estimating Proof Test Coverage for Emergency Shutdown Valves using a Fuzzy Inference System

Steve Kriescher,[1] Roderick Thomas,[2] Chris Phillips,[1] Neil Mac Parthaláin,[3] and David J. Smith[4]

[1]Department of Chemical Engineering, Faculty of Science and Engineering, Swansea University, Swansea, Wales
[2]School of Management, Swansea University, Swansea, Wales
[3]Department of Computer Science, Aberystwyth University, Aberystwyth, Wales
[4]Technis, Tonbridge, UK

(Received 16 December 2024; Revised 19 February 2025; Accepted 13 March 2025; Published online 13 March 2025)

Abstract: Published proof test coverage (PTC) estimates for emergency shutdown valves (ESDVs) show only moderate agreement and are predominantly opinion-based. A Failure Modes, Effects, and Diagnostics Analysis (FMEDA) was undertaken using component failure rate data to predict PTC for a full stroke test and a partial stroke test. Given the subjective and uncertain aspects of the FMEDA approach, specifically the selection of component failure rates and the determination of the probability of detecting failure modes, a Fuzzy Inference System (FIS) was proposed to manage the data, addressing the inherent uncertainties. Fuzzy inference systems have been used previously for various FMEA type assessments, but this is the first time an FIS has been employed for use with FMEDA. ESDV PTC values were generated from both the standard FMEDA and the fuzzy-FMEDA approaches using data provided by FMEDA experts. This work demonstrates that fuzzy inference systems can address the subjectivity inherent in FMEDA data, enabling reliable estimates of ESDV proof test coverage for both full and partial stroke tests. This facilitates optimized maintenance planning while ensuring safety is not compromised.

Keywords: emergency shutdown valves; failure modes; effects; diagnostics analysis; fuzzy inference systems; proof test coverage

I. INTRODUCTION

The Control of Major Accident Hazards (COMAH) regulations [1], requires UK process plant and facility operators to demonstrate that safety instrumented systems are specified, designed, installed and maintained to minimise risks. Functional safety guidance, such as IEC 61508 [2] and IEC 61511 [3], are used for benchmarking within the COMAH regulations and has evolved to encourage the application of appropriate safety engineering activities in industries such as oil and gas, chemical and petrochemical.

A typical safety instrumented system (SIS) may consist of multiple safety instrumented functions (SIFs), each designed to protect a process plant or facility from potentially hazardous events. SIFs are designed to protect against specific hazardous events, for example, overfilling a storage tank or over pressurising a pipeline, hence preventing a loss of containment. These systems typically culminate in a shutdown of the process which prevents the flow of a hazardous material.

Sensors typically include process transducers (pressure, temperature, flow, level). Logic solvers typically include programmable logic controllers (PLCs) and/or hard-wired systems. Final elements typically include emergency shutdown valves (ESDVs), and/or contactors/relays (for pump motor stops). State-of-the-art sensors and PLCs feature onboard diagnostics, enabling the detection of some dangerous failures during operation. In contrast, ESDVs typically lack onboard diagnostic capabilities. The lack of diagnostic capability emphasizes the importance of proof testing ESDVs when compared with other components of a SIF.

An ESDV assembly consists of a series of components, all of which can fail preventing the valve from fully closing and shutting down flow in an emergency. The major components of an ESDV are as follows:

1) Solenoid operated valve (SOV) – a SOV is an electromechanical device which controls air supply to the actuator, upon receipt of an electrical signal from the logic solver and determines whether a valve is actuated (opened or closed) by providing pressured air to the valve actuator.
2) Actuator – an actuator, typically a pneumatically powered device, provides the force and motion required to open or close a valve, utilizing air supplied by the SOV. This movement is normally countered by a spring which holds the actuator in a normally closed or normally open position unless the actuator receives a pneumatic signal.
3) Valve – a valve is made up from several components, typically:

Corresponding author: Steve Kriescher (e-mail: s.a.kriescher.2139862@swansea.ac.uk).

- Body – the pressure containing part of the valve, which contains the com- ponents that contact the fluid.
- Bonnet – a closure component of the valve body that serves as a housing for the stem, providing a passage through which the stem moves.
- Obturator – a ball, disc, gate or plug that is positioned in the flow stream to permit or prevent flow with either linear or rotary motion.
- Stem – the connector from the actuator to the inside of the valve – transmits force to move the obturator
- Seat ring – the surface that the valve obturator contacts when the valve is closed, thus forming the seal.

Within these components there are subcomponents such as springs, bearings, and seals which can fail individually thus causing the failure of that component.

As part of ongoing maintenance, safety instrumented functions (SIFs) must be proof tested periodically to reveal dormant dangerous failures, i.e., failures which are neither self-evident nor detected by automatic diagnostics [3]. Proof testing in the context of process engineering is a form of planned preventative maintenance through which periodic functional tests are carried out on safety-related equipment such as safety instrumented systems. Preventative maintenance can be defined as time-based maintenance tasks that determine an asset's condition, that preserve the life of an asset, such as cleaning, adjustments, lubrication, and component replacement [4].

The interval at which a device is proof tested is based on the unavailability of the SIF, also known as the probability of failure on demand average (PFDavg). SIF SIL targets are determined prior to the specification and design phase as part of the hazard and risk assessment process.

Parameters considered in the PFDavg calculations include equipment dangerous undetected failure rates (λ_{DU}), proof test interval (PTI), proof test coverage (PTC) and mission time (MT). PFDavg is defined as follows:

$$PFDavg = PTC \times \lambda_{DU} \times \frac{PTI}{2} + (1 - PTC) \times \lambda_{DU} \times \frac{MT}{2} \quad (1)$$

Proof test coverage (PTC) is calculated from the sum of the revealed dangerous undetected failure rates (Revealed λ_{DU}) and the sum of the total dangerous undetected failure rates (Total λ_{DU}), expressed as a percentage:

$$PTC = \frac{Revealed\,\lambda_{DU}}{Total\,\lambda_{DU}} \quad (2)$$

Mission time (MT) is the period between when the SIF (or device) is placed into service and when it is replaced or completely refurbished to "as-new" condition.

The purpose of proof testing is to reveal potentially dangerous failures, which are not revealed by on-board diagnostics. In the case of ESDVs, diagnostics are limited or often unavailable and therefore reliance on effective proof testing is essential. There are several different ESDV proof test regimes, as shown below [5], which will have varying PTC:

(1) Partial stroke test – the valve is typically moved from 5% to 20% [6–8], online (under process operating conditions).
(2) Full stroke test – the valve moved to its fully closed (or open) position, offline (not under process operating conditions).
(3) Full stroke test at process operating conditions – as per test (2) with the valve online.
(4) Full stroke test and leak test – with the valve offline.
(5) Full stroke test at process operating conditions and leak test – as per test (4) with the valve online.

The partial stroke test (1) and the full stroke test (2) are the most common types and the focus of this study.

The variation in proof test methods seen industrially is due to the limitations of the plant design and its operation; for example, it may be disruptive or impractical to test ESDVs when the process is operating, so an offline test may be carried out or a partial test when the plant is online. Due to these constraints, proof tests are typically imperfect.

Estimating credible values of PTC is essential for determining proof test intervals. Inaccurate predictions can result in test frequencies that are either insufficient, compromising safety, or excessive, leading to unnecessary cost penalties. Green and Bell [9] emphasize the importance of accurately specifying proof test intervals, as this plays a critical role in the PFDavg calculations for safety instrumented systems. As highlighted in a study by Tokarski [10], inadequate maintenance and testing account for over 30% of major accidents in the oil and gas industry.

The full stroke test as described in (2) above allows for full movement of the valve but does require the process to be offline, which can be a disadvantage. Figure 1 below presents PTC estimates for this type of test, provided by several industry experts and organizations. These estimates are derived using several different techniques including semi-quantitative (based on point scoring systems); quantitative (based on failure modes and effects analysis and industry data); and qualitative (based on assessor experience and judgement).

The resultant PFDavg can differ significantly, therefore affecting the safety integrity level, when applying the upper and lower values of PTC. This shows the extent of variability and lack of consensus with wide-ranging estimates of PTC for this type of proof test, from 35 to 90% (a mean of

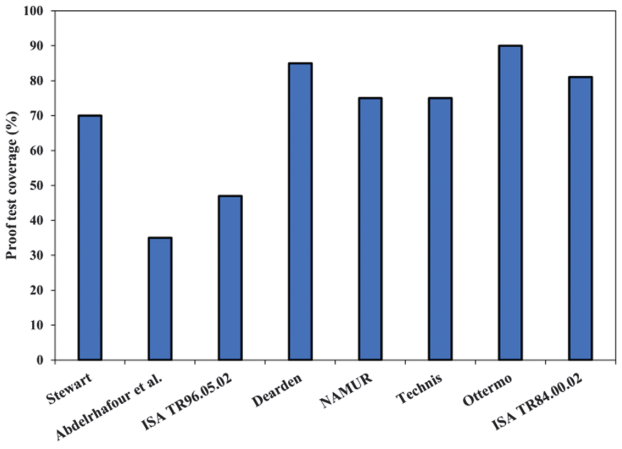

Fig. 1. Published Full stroke test PTC estimates. Stewart [5], Abdelrhafour *et al.* [11], ISA TR96 [12], Dearden [13], NAMUR [14], Technis [15], Ottermo [16], ISA TR84 [17].

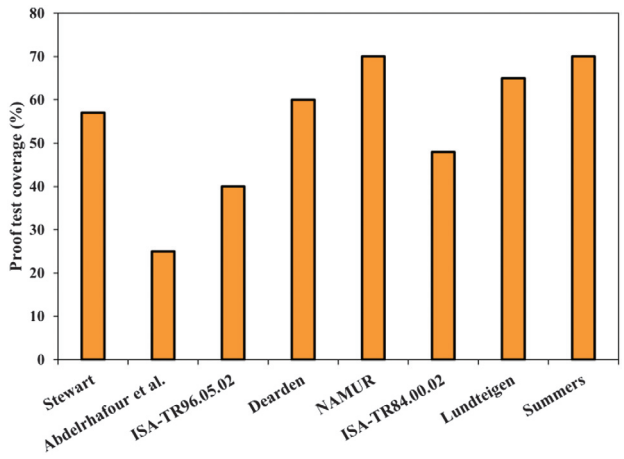

Fig. 2. Published Partial stroke test PTC estimates. Stewart [5], Abdelrhafour *et al.* [11], ISA TR96 [12], Dearden [13], NAMUR [14], ISA TR84 [17], Lundteigen [18], Summers [19].

approximately 70%). It is noted that the estimates provided by Abdelrhafour *et al.* [11] and ISA-TR96.05.02 [12] appear to be particularly low, 35% and 47% compared to others. The point scoring system used in the evaluation by Abdelrhafour *et al.* [11] assumes valve seat inspection or testing and since this is not part of the test considered as part of this study, the resulting estimate is low. Regarding ISA-TR96.05.02 [12] the relatively low estimate of PTC may be due to the valve specification that requires tight shutoff (TSO), which is not a requirement of the ESDV in this study.

Figure 2 illustrates the wide range of published proof test coverage (PTC) estimates for a partial stroke test, as observed for the full stroke test.

A description of the ESDV components (SOV, actuator and valve) assessed using the FMEDA technique is provided below. The ESDV is fail safe, close on demand. For the application considered minor seat leakage is acceptable to achieve a safe state, i.e., there is no requirement for tight shut-off (TSO).

A. SOLENOID OPERATED VALVE (SOV)

A pneumatic 3/2 direct acting SOV. Configured as fail safe closed, i.e., on loss of signal the SOV returns to its vent (safe) position.

B. ACTUATOR

A pneumatic scotch-yoke, spring return type actuator. Configured as fail safe, i.e., on loss of air supply the actuator will return to its safe state, hence returning the valve to its closed position.

C. VALVE

A full bore, trunnion mounted ball valve with static seat rings and springs.

II. THE FUZZY-FMEDA APPROACH

A failure modes, effects, and diagnostics analysis (FMEDA) is a technique originally developed to determine the diagnostic coverage of electronic equipment, identifying electronic component failure modes and their effects on the system and whether failures are detected or not by diagnostics [20]. The technique requires component failure rates to be assigned to failure modes, which allows the distribution of failures and the overall diagnostic coverage to be determined. In comparison a failure modes, effects, and criticality analysis (FMECA) is a semi-quantitative method used to identify failure modes, assess their effects, and prioritize them based on severity, occurrence and detectability to determine risk priority numbers (RPN) allowing component failure criticalities to be identified. It is widely used for general risk assessment and system reliability improvement. Whereas FMEDA is a quantitative extension of FMECA, specifically used in functional safety to evaluate component failure rates and diagnostic coverage.

The FMEDA technique as described by Stewart [5] can also be used to determine the proof test coverage for mechanical systems such as ESDVs. Similarly, Easton [21] and Green and Bell [9] agree that FMEDA is an appropriate tool for this purpose. Furthermore, Lundteigen [18] suggests the use of a FMEA type study to determine proof test coverage of partial stroke testing valves and following the work undertaken by Bukowski [22] estimates of proof test completeness can be determined using FMEDA and evaluating what dangerous undetected failures can be revealed from specific proof test procedures.

The FMEDA technique requires the human judgement of the assessor, in particular the selection of appropriate component failure rate and the identification of failure modes. The opinion of human experts can vary significantly and have a significant vagueness attached to the descriptions of component failure. As highlighted by Dearden [13], there are also uncertainties in the failure rates and identification of the failure modes in any given context, making any attempt to determine precise percentages of PTC very challenging. Likewise, research undertaken by Isenburg [23] suggests that the lack of mechanical component failure rate databases leads to subjectivity, which ultimately impacts the outcome of the assessment.

It was evident from data collected from industry experts that there is a wide-ranging opinion on mechanical component failure rates. Table I highlights the variation in failure rates for ESDV components provided by seven FMEDA experts (Datasets #1 to #7). The range of failure rates vary from 1 to 220 FIT. FIT is the number of failures that can be expected in one billion (10^9) device hours of operation. The FIT values are color coded to present a 'heat map'. Green indicates the lowest values, yellow represents the mid-range values, and red signifies the highest values.

Data sources included published databases developed by exida [24] and Technis [25]. The exida component reliability database (CRD) provides a list of valve assembly components, potential failure modes, an overall component failure rate and a distribution of failure rate for specific failure modes. Component failure rates are provided with variations based on environmental conditions. The exida failure modes were used as a basis for the FMEDA. The Technis database, FARADIP FOUR, provides a list of valve assembly components and associated failure rates, whereby the distribution of failure rates for specific failure modes are subject to expert judgement.

Table I. FMEDA expert failure rate data

Component	Failure mode	Failure mode type	Dataset #1	Dataset #2	Dataset #3	Dataset #4	Dataset #5	Dataset #6	Dataset #7
Sleeve bearing	Bind	FTC	22	110	50	56	2	40	10
Poppet w/seals	Bind	FTC	36	220	30	45	1	32	6
Spring	Settle	FTC	104	165	40	45	1	32	16
Spring	Break	FTC	26	55	40	45	1	32	24
Piston rod	Break	FTC	20	19	30	13	11	13	5
Piston rod	Deflect	DOP	20	38	130	26	21	26	5
Yoke (includes guide block/bar)	Break	FTC	36	19	30	13	11	13	15
Yoke (includes guide block/bar)	Bind	DOP	36	150	70	52	43	52	15
Cylinder body	Fracture	FTC	3	19	30	13	11	13	12
Cylinder body	Fracture	DOP	3	19	20	13	11	13	12
Piston	Bind	DOP	8	150	160	104	86	104	16
Piston	Fracture	FTC	4	19	90	13	11	13	8
Piston seals	Bind	FTC	12	75	70	52	43	52	16
Tie rod	Break	FTC	3	19	30	13	11	13	5
Tie rod	Deflect	DOP	3	37	70	26	21	26	5
Spring	Settle	FTC	104	57	70	39	32	39	16
Spring	Break	FTC	26	19	30	39	32	39	24
Stem bush/bearings	Bind	FTC	47	73	43	24	22	7	45
Stem bush/bearings	Bind	DOP	47	73	43	48	44	15	45
Valve body	Bind	DOP	5	19	40	12	11	4	12
Valve body	Bind	FTC	5	19	20	12	11	4	12
Seat ring/spring A	Bind	FTC	23	55	40	24	22	7	6
Seat ring/spring A	Major leak	LCP	45	91	105	121	110	37	15
Seat ring/spring B	Bind	FTC	23	55	40	24	22	7	6
Seat ring/spring B	Major leak	LCP	45	91	105	121	110	37	15
Stem	Bind	FTC	27	73	20	73	66	22	15
Stem	Bind	DOP	27	73	20	73	66	22	15
Stem	Break	LCP	18	73	65	12	11	4	8
Obturator (ball)	Bind	FTC	25	19	43	12	11	4	6
Obturator (ball)	Bind	DOP	25	37	43	24	22	7	6
Obturator (ball)	Break	FTC	25	19	43	12	11	4	6
Obturator (ball)	Major leak	LCP	76	145	65	73	66	22	39
Trunnion bush/bearings	Bind	FTC	47	73	43	48	44	15	15
Trunnion bush/bearings	Bind	DOP	47	73	43	48	44	15	15
Total Dangerous Failure Rate			1021	2248	1808	1369	1040	786	491

Inference systems are effective for handling subjective, imprecise, or vague information. They can also address inconsistencies in data, ensuring more reliable analysis and decision-making [26]. Such a system is a Fuzzy Inference System (FIS) which maps information from a given crisp input to an output using membership functions and fuzzy logic. A set of IF-THEN rules are used to map the input to the output membership function which is then de-fuzzified to produce a crisp value. The inputs of the FMEDA (component failure rate and probability of revealing the failure) shall then be used as inputs to the FIS to generate an FIS output. The FIS outputs for each line of the FMEDA can then be used to determine a PTC estimate accounting for the implicit uncertainty in the FMEDA data, hence the Fuzzy-FMEDA approach.

III. FAILURE MODES, EFFECTS, AND DIAGNOSTICS ANALYSIS (FMEDA)

A. APPLICATION

The FMEDA technique was used to determine the causes and modes of failure of the various components within the ESDV assembly. The inputs to a FMEDA include the following:

- Equipment datasheets.
- Safety requirements specification.
- Schematic drawings (identifying component parts).
- Proof test requirements.
- Component failure rate data.

It will be necessary to understand the safe and dangerous failure modes of the equipment and specifications such as seat leakage classification. Each component part is assessed to determine how it can fail (failure mode) and what impact the failure (failure effect) has on the operation of the system, i.e., will the failure effect be safe, dangerous or have no effect. There are three dangerous failure mode types associated with an ESDV namely fail to close (FTC), delayed operation or slow to close (DOP) and leak in the closed position (LCP). A failure rate is then assigned to the failure mode of the component, which is likely to be a distributed value from the overall component failure rate as there is usually more than one type of failure mechanism. The final part of the assessments includes consideration of whether the failure mode will be revealed during the proof test and the reliability of the verification method of the proof test, as described below [18]:

Revealability - to what degree is the failure mode reveal-able during a proof test, e.g., a partial stroke test (PST) will reveal a smaller percentage of the delayed operation (DOP) failure mode compared to a full stroke test (FST).

Reliability - to what degree are the proof test results dependable, such that the revealed results reflect the valve condition, e.g. the reliability of the limit switches indicating fail to close (FTC) failure mode.

The product of the component failure rate (for each failure mode), its revealibility and the test reliability provides a 'weighted' revealed dangerous undetected failure rate. The resultant PTC is calculated from the sum of the weighted revealed dangerous undetected failure rates (Revealed λ_{DU}) and the sum of the total dangerous undetected failure rates (Total λ_{DU}) using PTC formula (1).

IV. FUZZY-FMEDA FOR ESTIMATING PROOF TEST COVERAGE

Possibilistic or fuzzy reasoning is based upon fuzzy set theory [27] which is a generalization of classical set theory. In fuzzy set theory, membership can be defined in the interval [0,1]. Fuzzy logic is a many-valued logic and an extension of classical logic and is built on fuzzy set theory. Fuzzy reasoning offers the ability to reason using imprecise, human-defined concepts (e.g. 'a fairly tall man') and therefore is often referred to as 'computing with words', hence can be utilized for the sorts of imprecise descriptions applied to valve failure. It has enjoyed application to a wide variety of problems relating to: control, knowledge representation and modelling, and more generally to decision systems that can handle vagueness in data. A fuzzy inference system (FIS) uses the process of fuzzification to model the input domain of the problem, under consideration, thus mapping crisp values from the real-world into linguistic variables.

A. FUZZY INFERENCE SYSTEMS

Fuzzy inference is the process of mapping from a given set of inputs to an output using fuzzy logic as the inference step. This mapping provides a basis from which decisions can be made, or by which patterns can be recognized by firing various associated rules. The actual process of fuzzy inference involves several components that are described in the membership functions, linguistic variables, and the rule base.

Broadly speaking there are two different approaches to fuzzy inference: Mamdani inference [28] and Takagi-Sugeno-Kang or TSK inference [29]. The Mamdani approach has been widely adopted and is generally the most popular method for FIS. However, as system complexity increases, there is a corresponding increase in computational complexity and TSK is often employed to reduce this overhead. In this work, however, a Mamdani approach is employed.

Mamdani inference was initially proposed [28] as an approach to create a control system by synthesizing a set of linguistic control rules derived from human expert opinion. In such an approach, the output of each rule is a fuzzy set. As Mamdani systems have more intuitive and easy-to-understand rule bases, they lend themselves well to application in the area of expert systems, where the rules are derived from human expert knowledge, e.g. medical diagnosis. Figure 3 outlines the general approach to the Mamdani inference system, which is described in detail below.

Broadly speaking there are three primary components to any FIS:

Fuzzification - the process of mapping crisp real-world values onto fuzzy linguistic variables.

Inference engine - fires the fuzzy IF-TEN rules according to the fuzzy input in order to derive a consequent (output). In particular, the fuzzy if-then rules are used to evaluate linguistic values and map them to an output fuzzy set using the firing strength.

Defuzzification - this step converts the output or consequent of the inference engine to a crisp value.

B. FIS DESIGN

The FIS was developed using MATLAB's Fuzzy Logic Toolbox. The objective of FIS design was to allow estimation of proof test coverage (PTC) for both full stroke and partial stroke tests.

The universe of discourse for the component failure rate fuzzy set was defined based on the range of failure rates derived from the seven datasets.

To determine the most appropriate FIS design a number of different membership functions types were experimented with, employing a varying number of membership functions, ranging from three to seven. It is worth noting that while various types of fuzzy membership functions can be employed, triangular and trapezoidal functions have proven sufficient for most real-world applications [30].

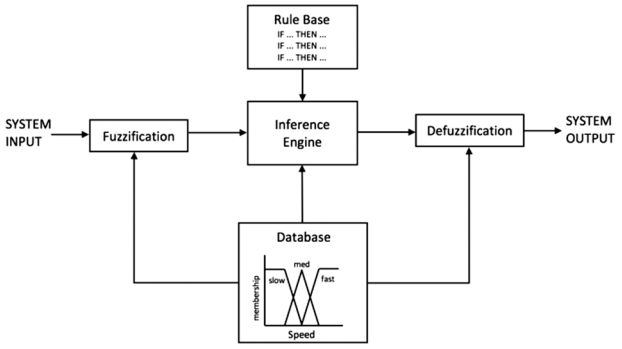

Fig. 3. Mamdani fuzzy inference system.

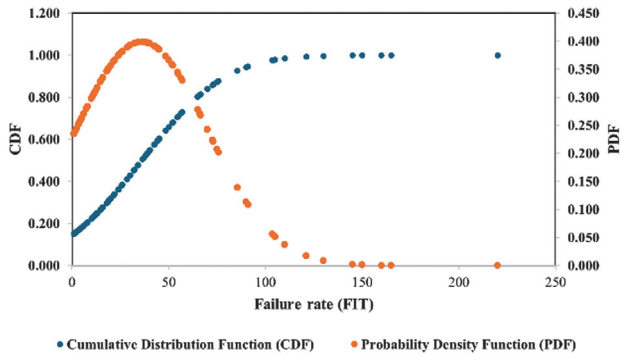

Fig. 4. Component failure rate distribution curves.

However, Gaussian membership functions were also explored to identify the most suitable type for this specific application.

The distribution of failure rates was also analyzed to determine the partitioning of the membership functions. The combined failure rate data for all datasets exhibited a right-skewed distribution, indicating that most values fell within the lower end of the 0 to 220 FIT range. Figure 4 illustrates the distribution of failure rate data. Figure 5 illustrates the partitioning of the component failure rate membership functions based on this distribution.

Regarding probability of revealing failure, for a full stroke test (FST) a value of 1 was employed and for the partial stroke test (PST) varying values for revealing delayed operation (DOP) and fail to close (FTC). A probability of 0.5 was used for DOP and FTC which covered the lower end of the range and values of 0.7 (DOP) and 0.8 (FTC) the mid-range.

C. DESIGN VALIDATION

To identify the most suitable FIS design, the coefficient of determination (R-squared or R^2) and root mean square error (RMSE) were calculated for each dataset by comparing the observed values from FMEDA with the expected values from the FIS. Synthetic datasets (Datasets #8 to #10) were generated from existing datasets to expand the range of data utilized for validation purposes. The design that proved most suitable, based on R^2 and RMSE values, utilized trapezoidal membership functions and is detailed in the next section. Table II illustrates the average R^2 and RMSE values for the best performing FIS design for a full stroke test (FST) and partial stroke test (PST). The high R^2 values and low RMSE values demonstrate that the FIS model fits the data well.

Table II. Average R^2 and RMSE values for the best performing FIS design

	FST	PST (0.7, 08)	PST (0.5, 0.5)
R^2	0.97	0.92	0.96
RMSE	5.8	9.5	5.0

D. IMPLEMENTATION

1. FUZZIFICATION. The fuzzification process maps the component failure rate and the probability of revealing the failure inputs into their respective fuzzy subsets. The linguistic variables for these inputs are defined based upon the values of the input domains. The partitioning of the component failure rate was based on the FMEDA data from seven experts, as discussed above. The probability of revealing the failure was also based on the FMEDA data and partitioned in equal increments from 0.5 to a probability of 1, this range was sufficient to cover both full stroke and partial stroke tests. The overlaps between adjacent membership functions permit smooth interpolation of the inputs

In terms of fuzzy-FMEDA, for component failure rate and probability of revealing the failure, trapezoidal membership functions were employed as shown in Figs. 5 and 6, respectively. The scaling describes the range of input values and their corresponding membership to each of the fuzzy linguistic labels and their respective fuzzy subsets. The y-axis represents the degree of membership to a fuzzy subset, so an input value that is in the middle of a subset has full membership of that category.

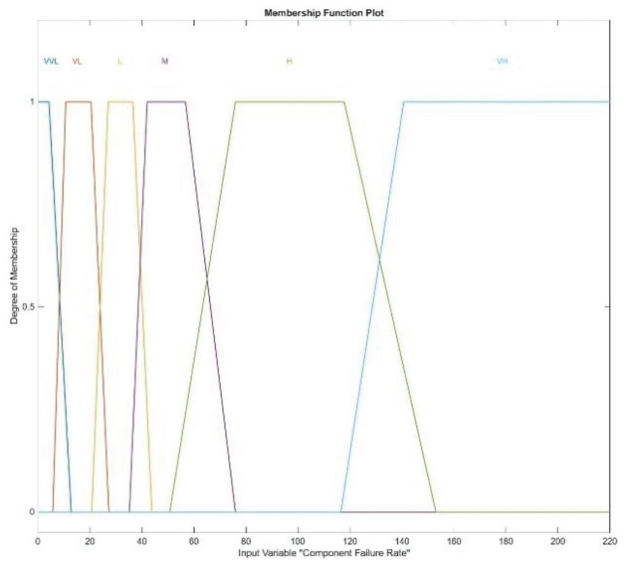

Fig. 5. Input membership functions: component failure rate.

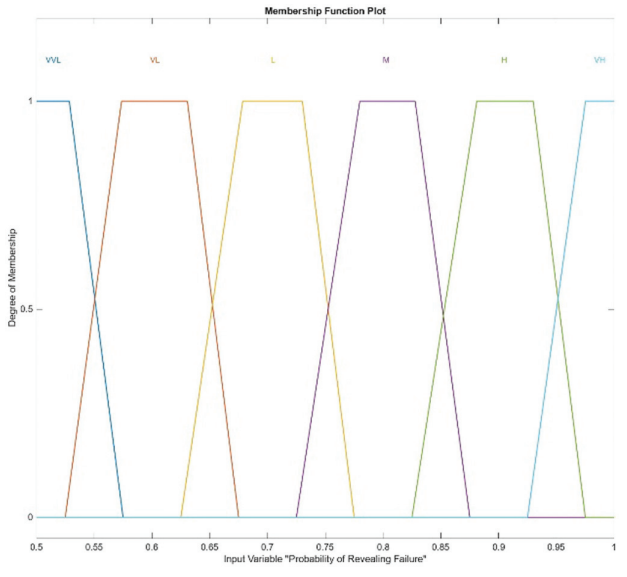

Fig. 6. Input membership functions: probability of revealing the failure.

Table III. Sample of IF-THEN rules

	Rule
1	If Component Failure Rate is VVL and Probability of Revealing Failure is VVL then Weighted Revealed Failure Rate is VVL
2	If Component Failure Rate is VL and Probability of Revealing Failure is VVL then Weighted Revealed Failure Rate is VVL
3	If Component Failure Rate is L and Probability of Revealing Failure is VVL then Weighted Revealed Failure Rate is VL
4	If Component Failure Rate is M and Probability of Revealing Failure is VVL then Weighted Revealed Failure Rate is L
5	If Component Failure Rate is H and Probability of Revealing Failure is VVL then Weighted Revealed Failure Rate is M
6	If Component Failure Rate is VH and Probability of Revealing Failure is VVL then Weighted Revealed Failure Rate is H
7	If Component Failure Rate is VVL and Probability of Revealing Failure is VL then Weighted Revealed Failure Rate is VVL
8	If Component Failure Rate is VL and Probability of Revealing Failure is VL then Weighted Revealed Failure Rate is VVL
9	If Component Failure Rate is L and Probability of Revealing Failure is VL then Weighted Revealed Failure Rate is VL
10	If Component Failure Rate is M and Probability of Revealing Failure is VL then Weighted Revealed Failure Rate is L

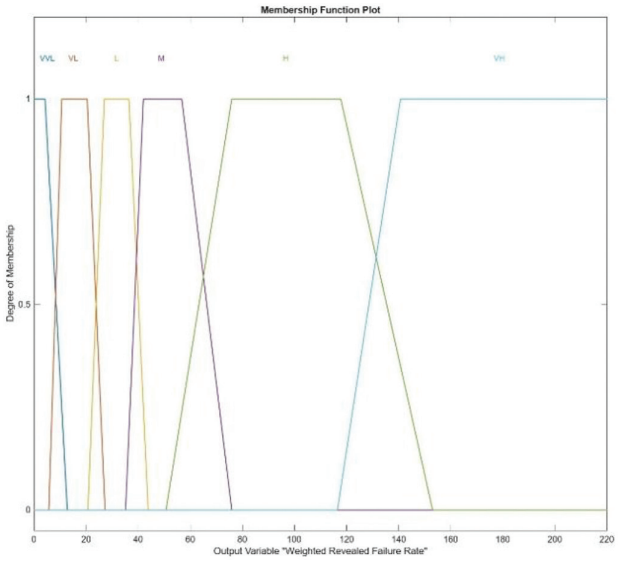

Fig. 7. Output membership functions - weighted revealed failure rate.

Any input can be fuzzified by mapping the component failure rate value and the probability of revealing the failure assessment value to the corresponding antecedent input. The membership degrees for the corresponding fuzzy sets can then be ascertained.

2. RULE BASE. Table III illustrates a sample of the 42 IF-THEN rules that were developed based on observations from the data.

3. PARTITIONING OF THE OUTPUT AND DEFUZZIFICATION. Figure 7 illustrates the corresponding set of consequents along with the membership functions for the output. Defuzzification of the output is conducted using the most used method, the centre-of-gravity method (COG). This method determines the centre of area of the fuzzy output set and returns the corresponding crisp value.

V. FMEDA AND FUZZY-FMEDA RESULTS

Table IV illustrates the proof test coverage (PTC) estimates based on FMEDA and FIS (fuzzy-FMEDA) for full stroke test (FST) and partial stroke tests (PST).

VI. DISCUSSION

The proof test coverage (PTC) for the full stroke test suggests that there is only a 3% difference between the FMEDA and FIS versions for the datasets within this study. This would likely have minimal impact on the PFDavg or the proof test interval. However, due to the limited validation data in this research, particularly the number of expert datasets, it remains possible that other FMEDA data could produce FIS PTC values that differ significantly from those of FMEDA. However the results of the PTC of the partial stroke test of FIS, in some cases, were 22% greater than the FMEDA probability of revealing failure = 0.7 (FTC) and 0.8 (DOP), for Dataset #8. The significance of this is that applying these findings to the PFDavg calculations could lead to a reduction in the frequency of partial stroke testing and/or allow for an extension of the full stroke test interval.

Although PST can improve the testing strategy and improve operational efficiency, it should not typically replace FST in safety-critical applications. Instead, it is often used in conjunction with FST to provide a more comprehensive assessment of valve health and functionality. The potential outcome of these results is a reduction in ESDV proof testing overhead, leading to maintenance cost savings for operating companies.

The fuzzy-FMEDA results indicate a 100% improvement in both test intervals, which could extend the typical partial stroke test interval from six months to one year and the usual full stroke test interval from one year to two years.

VII. CONCLUSIONS

This paper has presented a novel approach to estimating ESDV proof test coverage using a fuzzy inference system as a means of dealing with the uncertainty of the data in the FMEDA approach and reconciling the judgement of experts.

The approach described in this paper has the potential to resolve some of the problems associated with the FMEDA technique. As well as quantitative data, a fuzzy inference system can also handle qualitative, ambiguous and imprecise or vague data.

Fuzzy-FMEDA offers a distinct advantage over other inference techniques such as Bayesian methods, Monte Carlo simulation and machine learning by effectively managing uncertainty in expert-driven functional safety analysis. Compared to Bayesian methods, which depend on prior distributions that may be subjective or hard to justify, fuzzy-FMEDA

Table IV. FMEDA and FIS (Fuzzy-FMEDA) proof test coverage results

	Full Stroke Test									
	Dataset #1	**Dataset #2**	**Dataset #3**	**Dataset #4**	**Dataset #5**	**Dataset #6**	**Dataset #7**	**Dataset #8**	**Dataset #9**	**Dataset #10**
FMEDA PTC	82%	82%	81%	77%	71%	87%	84%	77%	77%	82%
FIS PTC	81%	83%	81%	76%	72%	88%	84%	80%	77%	83%
	Partial Stroke Test with probability of revealing a failure = 0.7 (FTC), 0.8 (DOP)									
	Dataset #1	**Dataset #2**	**Dataset #3**	**Dataset #4**	**Dataset #5**	**Dataset #6**	**Dataset #7**	**Dataset #8**	**Dataset #9**	**Dataset #10**
FMEDA PTC	60%	61%	60%	57%	54%	65%	62%	57%	57%	60%
FIS PTC	70%	58%	61%	59%	61%	76%	80%	79%	54%	57%
	Partial Stroke Test with probability of revealing a failure = 0.5 (FTC), 0.5 (DOP)									
	Dataset #1	**Dataset #2**	**Dataset #3**	**Dataset #4**	**Dataset #5**	**Dataset #6**	**Dataset #7**	**Dataset #8**	**Dataset #9**	**Dataset #10**
FMEDA PTC	41%	41%	41%	38%	36%	44%	42%	38%	38%	41%
FIS PTC	43%	41%	44%	40%	37%	42%	36%	38%	40%	47%

allows uncertainty to be expressed in linguistic terms, reducing reliance on potentially biased priors. Unlike Monte Carlo simulation, which demands well-defined probability distributions and significant computational resources to model uncertainty, fuzzy-FMEDA accommodates vague expert opinions without requiring precise probabilistic inputs. Additionally, while machine learning techniques can uncover complex patterns, they require large training datasets, which are often unavailable in safety-critical industries, and they lack interpretability which is a key requirement for regulatory acceptance. In contrast, fuzzy-FMEDA provides an interpretable, expert-driven approach that captures the nuances of expert opinions without over-reliance on historical data or probabilistic assumptions, making it a robust and practical tool for functional safety related analysis.

The fuzzy-FMEDA proof test coverage results suggest that the FIS approach supports further optimisation of emergency shutdown valve maintenance by integrating full and partial proof tests, extending proof test intervals, and enhancing plant uptime without compromising safety.

DATA AVAILABILITY

The data that support the findings of this study are available on request from the corresponding author.

ACKNOWLEDGEMENTS

SK would like to thank Dr. William Goble (exida) for kindly providing a copy of the Component Reliability Database (CRD) Handbook and the Failure Modes, Effects and Diagnostic Analysis (FMEDA) training in support of this research.

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] HSE. *A Guide to the Control of Major Accident Hazards Regulations (COMAH) 2015 (L111)*. London: HSE, 2015.

[2] International Electrotechnical Commission. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 1: General Requirements (IEC Standard No. 61508:2010)*. Geneva: International Electrotechnical Commission, 2010.

[3] International Electrotechnical Commission. *Functional Safety - Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements (IEC Standard No. 61511:2016)*. Geneva: International Electrotechnical Commission, 2016.

[4] R. Thomas and D. J. Rees, "Progress in predictive asset maintenance management," *Int. J. Condition Monitoring Diagn Eng. Manage.*, vol. 24, pp. 39–45, 2021.

[5] L. Stewart, "How final element proof test can affect your SIF," *Proceedings of the 29th European Safety and Reliability Conference*, Hannover, Germany, 2019. https://doi.org/10.3850/978-981-11-0745-0-0478-cd.

[6] P. Gruhn, J. Pittman, S. Susan Wiley, and T. LeBlanc, "Quantifying the impact of partial stroke valve testing of safety instrumented systems," *ISA Trans.*, vol. 37, no. 2, pp. 87–94, 1998.

[7] S. Doddi, "Understand partial-stroke testing," *Control Eng. J.*, vol. 67, no. 3, pp. 7–8, 2020.

[8] Safety and SIS, "Partial Valve Stroke Test (PVST)," 2020. https://safetyandsis.com/partial-valve-stroke-test/.

[9] D. Green and R. Bell, "Proof Testing . . . A key performance indicator for designers and end users of Safety Instrumented Systems," Symposium Series No 162, Hazards 27, Birmingham, UK, 2017. Retrieved from https://www.icheme.org/media/15519/paper-67.pdf

[10] E. Tokarski. *The Safety Professional's Role: In Support of Industrial Facilities Operations and Maintenance*. Bloomington, IN: Xlibris. 2013.

[11] M. Abdelrhafour, N. Bajaj, and S. Boily, "Proof Test Procedure Effectiveness on Safety Instrumented Systems," 2012 Safety Control Systems Conference IDC Technologies. Edmonton, Canada, 2012. Retrieved from https://vdocuments.mx/idc-conference-2012-proof-test-procedure-effectiveness-on-safety-instrumented.html.

[12] International Society of Automation. *In-Situ Proof Testing of Automated Valves (ISA Standard No. ISA-TR96.05.02-2022)*. Durham, NC: International Society of Automation, 2022.

[13] H. T. Dearden. *Functional Safety in Practice (3rd ed.)*. North Charleston, SC: CreateSpace, 2020.

[14] NAMUR, "Flexible proof testing of field devices in safety instrumented systems (NA 106)," NAMUR. 2018. Retrieved from https://infostore.saiglobal.com/en-us/standards/NAMUR-NA-106-2018-1135947 SAIG NAMUR NAMUR 2683920/.

[15] Technis, "Guidelines on Assessing Proof Test Coverage (T996)," Technis, 2020. Retrieved from https://www.technis.org.uk/guidelines.html.

[16] M. Ottermo, S. Hauge, and S. Habrekke *Reliability Data for Safety Instrumented Systems PDS Data Handbook*. Trondheim: SINTEF, 2021.

[17] International Society of Automation. *Safety Integrity Level (SIL) Verification of Safety Instrumented Functions (ISA Standard No. ISA-84.00.02-2022)*. Durham, NC: International Society of Automation, 2009.

[18] M. A. Lundteigen and M. Rausand, "Partial stroke testing of process shutdown valves: How to determine the test coverage. *J. Loss Prev. Process Ind.*, vol. 21, no. 6, pp. 579–588, 2008.

[19] A. E. Summers, "Partial stroke testing of block valves," In *Instrument Engineers Handbook*. Houston, TX: SIS-TECH, 2006.

[20] W. M. Goble and A. C. Brombacher, "Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems," *Reliab. Eng. Syst. Saf.*, vol. 66, no. 2, pp. 145–148, 1999.

[21] B. J. Easton, "Impact of imperfect proof testing on the performance of safety instrumented functions," *Proceedings of the 31st European Safety and Reliability Conference*, 2021, pp. 744–751. Retrieved from https://doi.org/10.3850/978-981-18-2016-8.

[22] J. V. Bukowski and I. van Beurden, "Impact of proof test effectiveness on safety instrumented system performance," *Proceedings of the 2009 Annual Reliability and Maintainability Symposium*, 2009, pp. 157–163, Retrieved from https://doi.org/10.1109/RAMS.2009.4914668.

[23] J. Isenburg, "Mechanical components for functional safety applications (SIL): Standardisation urgently needed," *Industrial Valve Summit 2022 Conference*, 2022. Retrieved from https://www.valvecampus.com/abstract/mechanical-components-for-functional-safety-applications-sil-standardization-urgently-needed/.

[24] exida. *Component Reliability Database (CRD) Handbook Volume 2 - Mechanical Components*, 5th Edition. Gaithersburg, MD: Signature Book Printing, 2021.

[25] Technis, "FARADIP.FOUR Database," Technis. 2023. Retrieved from https://www.technis.org.uk.

[26] S. Wang, Y. Chang, T. Wu, Z. Han, and Y. Lei, "Attribute-driven fuzzy fault tree model for adaptive lubricant failure diagnosis," *J. Dynamics, Monitoring Diagnostics*, vol. 3, no. 3, pp. 207–215, 2024.

[27] L. A. Zadeh, "Fuzzy algorithms," *Inf. Control*, vol. 12, no. 2, pp. 94–102, 1968.

[28] E. H. Mamdani, "Application of fuzzy algorithms for control of simple dynamic plant," *Proc. Inst. Electr. Eng.*, vol. 121, no. 12, pp. 1585–1588, 1974.

[29] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control. Systems, man and cybernetics," *IEEE Trans. on, SMC*, vol. 15, no. 1, pp. 116–132, 1985.

[30] O. A. M. Ali, A. Y. Ali, and B. S. Sumait, "Comparison between the effects of different types of membership functions on fuzzy logic controller performance," *Int. J.*, vol. 76, pp. 76–83, 2015.