Proceedings of the 2016 Industrial and Systems Engineering Research Conference
H. Yang, Z. Kong, and MD Sarder, eds.

An Enhanced Hazard Analysis and Risk Assessment Method

David B. Kaber & Maryam Zahabi
North Carolina State University, Raleigh, NC, 27695-7906, USA

Abstract

Many system safety analysis (SSA) methods focus only on individual physical component failure. Some human reliability analyses (HRA) consider human-machine or human-automation interaction (HAI) in determining system failure rates; however, very few SSA methods account for interaction of components in hazard exposure. There is no SSA technique that provides the capability to quantify the impact of human/automation reliability on hazard exposure risk. The objectives of this study were to enhance the system hazard analysis (SHA) technique by introducing the concept of hazard risk bands and human/automation reliability classification using fuzzy sets, and to formulate a new risk-reliability score in a three-dimensional analysis space. Fuzzy sets are applicable in the systems safety domain as the classification of risk probability and severity are based on linguistic rather than numerical variables. The enhanced SHA technique yields a revised final mishap risk index, which is projected based on a composite assessment of HAI reliability at the time of system operation. The revised technique also supports broader control recommendations. The enhanced method was compared with human factors process failure modes and effects analysis (HF-PFMEA), which was considered to be the most similar HRA technique. The enhanced SHA approach provides comparable, if not more detailed, results.

Keywords
System hazard analysis, reliability analysis, fuzzy sets, human-automation interaction

1. Introduction

1.1. System Safety Analysis Methods
There are many formal system safety analysis (SSA) techniques documented in the literature (e.g. preliminary hazard list (PHL), preliminary hazard analysis (PHA), fault tree analysis (FTA)), which are primarily focused on individual physical component failures (e.g., defects, command faults) [1,2]. No existing SSA method provides the capability to quantify the impact of human/automation reliability on hazard exposure risk. Unfortunately, these methods have not made consideration of system aging, cumulative environment exposure, and degradations in fitness-for-duty and skills. Some SSA techniques do provide a basis for prioritizing use of engineering resources to control for specific types hazards exposure to equipment, facilities and human targets. For example, failure modes, effects, and criticality analysis (FMECA) identifies process failure modes, causes, negative effects, priority of risks, and recommended actions. It uses rating scales for quantifying outcome severity and occurrence of hazard exposure. FMECA also assigns rankings of likelihood of sensor or test technology success (i.e., the potential for revealing failures) and integrates a risk score with the detection ranking to yield a risk priority number (RPN). However, the RPN does not account for system aging and degradations in reliability.

System hazard analysis (SHA) is the only SSA method accounting for hazards due to interactions among components. This method is typically applied after a subsystem hazard analysis has mapped all potential piece-part, subassembly failure modes [2]. SHA is an inductive method that identifies sources of hazards and mechanisms (events) leading to negative outcomes with baseline risk assessment scores and revised scores considering recommended controls. The method is rare among formalized SSA techniques in terms of content.

1.2. Human Reliability Analysis Methods
Human reliability analysis (HRA) is defined as “any method by which human reliability is estimated” [3]. HRA plays an important role in many human-automation reliability assessments as part of complex systems. For example, astronaut performance is critical to the majority of NASA space missions and the reliability of human task performance needs to be estimated for accurate overall system and mission risk assessment. While reliable astronaut

performance leads to accomplishment of missions, human errors can result in damage to spacecraft and subsystems and, ultimately, incomplete missions [4].

In general, HRA techniques can be classified as the first and second generation [3]. The technique for human error prediction (THERP) is perhaps the best known of the first generation HRA methods. THERP classifies human errors as omissions or commissions. However, some studies have recommended use of second generation HRA methods for analysis of man-machine systems [5]. The most well-known second generation HRA methods include: a technique for human error analysis (ATHEANA) and the cognitive reliability and error analysis method (CREAM). These methods provide more of a theoretical human information processing basis for estimating task error rates; whereas, first generation methods were largely focused on observational data.

Another classification for HRA methods is quantitative vs. qualitative [6]. Qualitative methods attempt to identify the most likely errors while quantitative methods involve procedures to estimate human error probability (HEP). An example of quantitative methods is THERP. Another quantitative method is the standardized plant analysis risk-human reliability analysis (SPAR-H). It was first developed to estimate HEPs in nuclear power plant operations. Qualitative HRA methods include human factors process failure mode and effect analysis (HF-PFMEA) and action error analysis (AEA). HF-PFMEA identifies human error types as commission or omission. It considers the likelihood of human error (impossible, possible, and highly likely) as well as the consequence severity. It is also the only HRA method that is specifically designed for aerospace applications [4], including context-dependent information. Although the method supports an initial likelihood and severity assessment for hazard exposure, HRA does not involve determining a final risk score based on recommendation/implementation of hazard controls. Another qualitative HRA method is AEA, which involves enumeration of different system deviations from nominal operations, including actions that are too early, too late, or too long. [7]. The method also involves listing different errors in detail, such as actions applied to wrong objects, actions not taken, and actions in wrong order. Although we found some studies on advanced AEA [8], unfortunately the method itself is not well-defined in the literature.

1.3. Introduction to Fuzzy Sets

In classical set theory, an individual is either a member or not a member of a set and set boundaries are defined precisely. However, many real-word classification problems cannot be described using classical theory due probabilistic states of individuals. Fuzzy set theory allows partial membership of sets and is a more generalized set theory. A linguistic variable is defined as, "a variable whose values are words or sentences in a natural or artificial language" [9]. In the system safety literature, classifications of likelihood of hazard exposure (e.g., frequent, probable, occasional, remote, impossible) and severity of outcomes (e.g., catastrophic, marginal, negligible) and risk levels (e.g., unacceptable, undesirable, acceptable with review, acceptable without review) are also based on linguistic variables since their values are linguistic rather than numerical. Therefore, these variables can be better defined using fuzzy functions. The most common membership functions in fuzzy literature are triangular, trapezoidal, and Gaussian functions [10]. A triangular number, which is the simplest fuzzy function, is written by $A = (a_1, a_2, a_3)$ notation. The degree or grade of membership of any element x to a fuzzy set is represented by μ_x.

1.4. Motivation

The main goal of HRA methods is to identify HEP. None of the existing HRA techniques consider system reliability as a result of age and human-automation interactions (HAI). However, error classifications in HRA methods are more detailed than in SSA methods. Risk matrices, such as that included in MIL-STD 882B, are the most common tool by which to evaluate hazard exposure but little research has occurred to improve these matrices since their development. One limitation of current matrices is a lack of high resolution scales for ratings of severity and frequency of hazard exposure. The frequency of exposure scale includes levels of "improbable" (E), "remote" (D), "occasional" (C), "probable" (B), and "frequent" (A). The severity scale includes levels of "negligible" (IV), "marginal" (III), "critical" (II), and "catastrophic" (I). The overall risk index is numerical and ranges from a value of 20 ("acceptable without review") down to a value of 1 ("unacceptable"). Risk categories are defined based on threshold values and not overlapping risk bands.

The objectives of this study were to enhance the existing SHA technique by introducing the concept of overlapping hazard risk bands and a reliability classification using fuzzy sets. We also sought to formulate a new risk-reliability score in a three-dimensional analysis space considering the likelihood of hazard exposure, severity of potential outcomes, as well as levels of human-automation reliability. The organization of this paper follows a theoretical human factors research study which includes identification of research contributions, analytical support for our claims, and comparison with other existing methodologies.

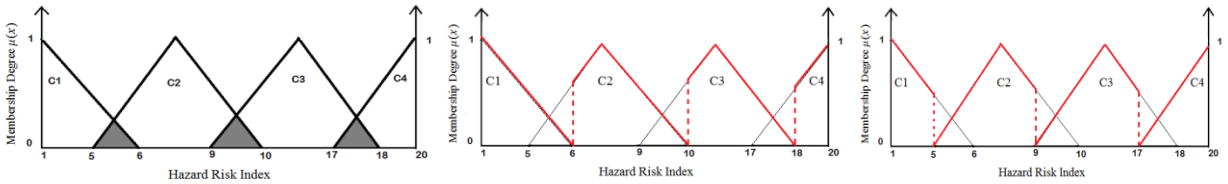
2. Research Contributions

2.1. Overlapping Risk Bands in SSA

In MIL-STD 882B, risk categories are defined discretely by threshold values. Such certainty of classification of risk scores is not logical, based on subjective ratings of severity and frequency of hazard exposure that underlie the scores. To address this issue, we proposed the use of triangular fuzzy functions to represent overlapping risk categories as part of the assessment method. Based on the hazard risk categories (C) of the military standard, we defined fuzzy membership functions (C_1, C_2, C_3) and they are presented in Table 1, including range and median values. Figure 1a provides a graphical representation of the overlapping risk bands and specific hazards can fall in either of the risk functions (see the shaded areas) depending on the grade of membership. Decisions about threshold risk values should depend on the analyst's approach to the risk assessment. For example, if the analyst wants to take a conservative approach, any risk value between 5 and 6 would be considered unacceptable (i.e., the hazard would belong to C_1). However, in a risky approach, the same hazard risk value might be categorized as undesirable (or belonging to C_2). Conservative and risky approaches for all risk bands are shown in Figure 1, plates b and c.

Table 1: Fuzzy risk categories

Criterion	Unacceptable	Undesirable	Acceptable with review	Acceptable w/out review
Triangular Fuzzy Number	$C_1 = (1,1,6)$	$C_2 = (5,7.5,10)$	$C_3 = (9,13.5,18)$	$C_4 = (17,20,20)$



(a) (b) (c)

Figure 1: (a) Overlapping fuzzy risk bands; (b) Conservative approach; (c) Risky approach

2.2. Reliability Classification

In order to define a 3D risk-reliability scale, reliability values should be mapped into several classes. The classification shown in Table 2 can be used for reliability of man-machine systems [11]. However, "high" (H), "medium" (M), and "low" (L) reliabilities are linguistic variables and can be better defined using fuzzy functions. Related to this, continuous random variables have extensive use in reliability analysis for description of system survival times, system loads, and repair rates. [12]. Since reliability is better defined using continuous functions, such as exponential and normal (Gaussian) functions, any fuzzy classifications of reliability should also follow this structure. Figure 2 shows reliability categories using fuzzy membership functions. The "low" reliability category was defined using a negative exponential function. As the reliability of the system increases, the likelihood of having a low reliability will decrease. The "medium" reliability category was defined using a normal distribution. As the reliability level of a system approaches a value of 0.7, the system is more likely to have moderate reliability. Finally, the "high" reliability category was defined using an exponential function. As the system reliability increases, the likelihood of having high reliability will increase. Consequently, this proposed fuzzy classification for reliability supports a bathtub-shaped failure curve [12]. Reading from the right of the figure to the left side, the initial high failure rate can be attributed to design faults or operator mistakes, leading to decreases in HAI reliability (i.e., the decreasing trend of reliability from 1.0 to 0.8). The mid-section of the curve includes the lowest likelihood of membership but the most nearly constant failure rate (i.e., reliability ranging from 0.8 to 0.6). Finally, the last part of the bathtub shape (at the left side of the figure) is usually caused by system fatigue or component aging, which results in a drastic decrease in HAI reliability (i.e., an increase in the likelihood of reliability levels from 0.6 to 0).

Table 2: Reliability classification

Category	**Low**	**Medium**	**High**
Reliability	0.6000 or less	0.6001 to 0.8000	0.8001 or more

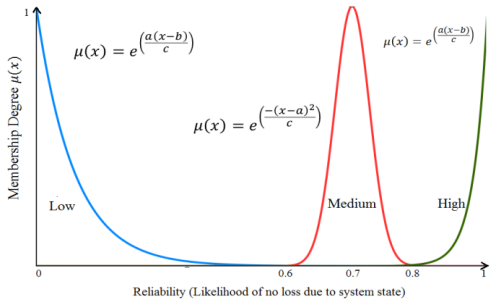
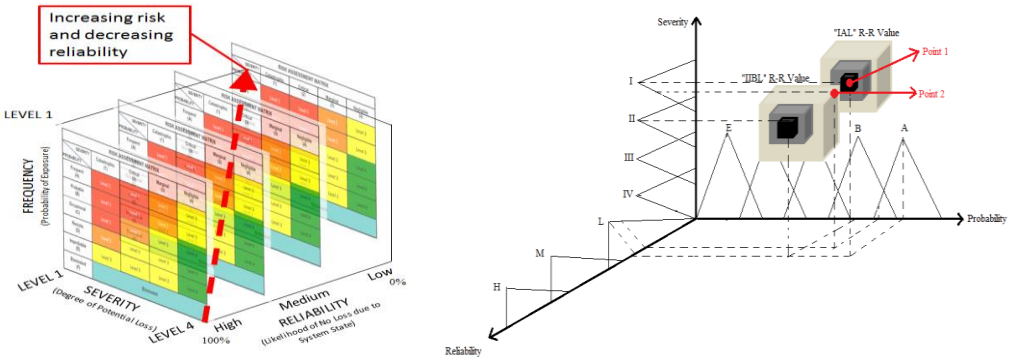


Figure 2: Fuzzy reliability classification

2.3. A Three-Dimensional Risk-Reliability Space

The addition of reliability values to SSA allows for definition of a three-dimensional (3D) risk-reliability (R-R) modeling space (or location of multiple risk planes along the dimension of system reliability). This model is shown in Figure 3 (a). Among other factors, reliability can represent system age. Such 3D analysis spaces can be defined for a human operator or automation/robot. The range of severity, frequency and reliability values may vary among servers. In addition, the rate of change in anyone dimension relative to another may also vary among servers. Referring again to Figure 3(a), following the convention of MIL-STD 882B-E, lower values for severity and frequency are considered riskier, and increasing risk occurs with degraded system reliability. This 3D R-R space can also be described using fuzzy classification (see Figure 3 (b)). For example, if a hazard probability was estimated to be frequent with a degree of membership = 1, its severity was determined as catastrophic with a degree of membership = 1, and estimation of a composite HAI reliability level was "low" with the degree of membership = 1, then the R-R value for this hazard would be classified as "IAL" (see Point 1 in Figure 3(b)). However, any uncertainty in any of the dimensions would lead to a composite degree of membership < 1, which would indicate that the R-R value could be categorized, for example, as either "IIBL" or "IAL", depending on analyst's approach (see Point 2 in Figure 3(b)). Therefore, fuzzy classification of R-R values could lead to recommendation of a broader set of potentially appropriate safety controls for each hazard. It is important to note that R-R classification can be uni-dimensional, bi-dimensional, or 3D depending on crisp or fuzzy classification of the likelihood of hazard exposure, severity of outcomes, and system reliability level. Figure 3(b) shows a scenario in which all dimensions are fuzzy. In addition, for simplicity of the graph, we assumed triangular fuzzy functions for all dimensions. However, as noted above, reliability can also be described using exponential and normal membership functions.



(a) (b)

Figure 3: (a) A 3D Risk-Reliability analysis space; (b) Fuzzy classification applied to the R-R space

2.4. Risk-Reliability Score

In order to quantify the 3D R-R space, there is a need to further define the R-R value. In the systems safety literature, risk is a two-dimensional construct, which is quantitatively defined as the product of severity and frequency. Frequency by definition should represent the number of times system hazard exposure is expected to occur. However, the term does not capture the probability of loss given exposure (P(L|E)). Considering Equation 1,

the frequency term can be expanded to address the conditional P(L|E). Following the MIL-STD 882B-E convention of risk classification (i.e., lower risk is "worse"), the probability component of the equation should be inverted. Therefore, the R-R value can be written as Equation 2. For example, if a severity of a hazard is estimated to be "catastrophic" and the probability of this hazard is assumed to be "frequent", then the risk of the hazard (based on the MIL-STD-882B) is equal to 1 (with membership in the fuzzy risk category C_1). Assuming a system reliability (combined human and automation reliability, which can be serial or parallel) of 0.95 (a "high" (H) reliability classification), the overall R-R value can be calculated using Equation 2, which would result in a final value of 0.95. (The R-R value for this hazard would be classified as "1AH" in the 3D R-R space.)

$$\text{FREQ} = \text{Exposures} / \text{Time} * P(L \mid E) \xrightarrow{P(L \mid E) = (1 - \text{Reliability})} \text{FREQ} = \text{Exposures} / \text{Time} * (1 - \text{Reliability}) \quad (1)$$

$$\text{R-R} = \text{Severity} * \text{FREQ} = \text{Severity} * (\text{Time} / \text{Exposure}) * \text{Reliability} \quad (2)$$

2.5. Enhanced SHA Method

Considering the new R-R value, we proposed an enhanced SHA approach to include classification of human error types due to degraded capacity (for each specific hazard). The method integrates human reliability/capacity values, which should be estimated based on validated cognitive and physical performance measures. The enhanced SHA also considers automation reliability values, which should be estimated based on prior mission data or manufacturer tests. A composite HAI reliability value can be calculated based on individual server reliabilities and system type. An example of the enhanced SHA worksheet is shown in Figure 4.

System: H-R Subsystem/Function: Payload ops.		System Hazard Analysis					Analyst: Kaber, D. B. Date: 10/29/14							
No.	TLM	Hazard	Cause(s)	Human Error Type	Effect(s)	IMRI	RISK	HR	AR	System Type	SR	R-R	Controls	FMRI
HAI-1	Human-robot collision	Heavy payload robot contacts human	(1) Soft control (sensor) failure; (2) degraded astronaut situation awareness	Commission (occupying same location in work cell as robot)	Astronaut head trauma and loss of consciousness; Body blow and internal bleeding; Tear in space suit, loss of atmosphere, death due to suffocation; damage to manipulator system; loss of payload	1D	8	0.95	0.95	Parallel	0.998	7.98 (1DH)	Implement redundant sensor array; provide astronaut training on precautions in robot work cell	1E-1D
							At time of material handling operation							
							Includes: hazards, causes, human errors, effects, IMRI, risk score, HRA, ARA, system type, SRA, R-R score, controls, and FMRI							

Figure 4: Enhanced SHA worksheet. (Note: TLM = Top level mishaps (taken from a preliminary hazard list); IMRI = Initial Mishap Risk Index (based on MIL-STD-882-E); HR = estimated Human Reliability level at stage of system operation; AR = estimated Automation/robot Reliability level; SR = the calculated overall System Reliability level based on HR, AR and the System Type; R-R = the composite Risk-Reliability score for the system (in the defined 3D space); FMRI = Final Mishap Risk Index (with a return to reference MIL-STD-882-E).

3. Discussion

3.1. Comparison of Enhanced SHA Approach with HF-PFMEA

Based on the review of literature on HRA methods, we noted that the objective of such methods is basically to calculate HEP. None of the existing techniques, save HF-PFMEA and AEA, consider the severity of hazard outcomes along with the probability of exposure as a basis for calculating risk score. Therefore, we identified the HF-PFMEA and AEA as the two closest HRA methods to our enhanced SHA approach. However, the AEA method was not a well-defined technique; whereas, HF-PFMEA has been identified in HRA guidelines as a method specifically designed for aerospace applications. A side-by-side comparison between the worksheet columns of the HF-PFMEA and our enhanced SHA approach is shown in Table 3. In general, the enhanced SHA approach provides a broader range of analysis capability as compared with the existing second generation HRA tool.

3.2. Advantages and Limitations

Current assessments of the frequency of system hazard exposure are "fully-loaded" and assume hazard exposure to be equal to certain loss. However, if different outcomes (losses) are specified for a single system hazard exposure, each outcome should have a separate likelihood estimate. The defined R-R values resolve this issue by capturing likelihoods of hazard exposure, degrees of potential loss, and probability of system loss. The values can be used to

predict system vulnerability levels at future points in time at which degradations in human and/or automation reliability might occur. In addition, R-R values can be used to further differentiate hazards with different severities of outcome (e.g., catastrophic vs. critical) and support broader control recommendations. For example, the trend of human and automation reliability/capacity against frequency of exposure and severity of outcome may be non-linear; therefore, the trend of R-R value will be non-linear.

The enhanced SHA approach also has some limitations that might cause difficulties in applying the technique. For example, the new method does not provide a structured approach for translating R-R values to hazard controls for degraded human or automation states. This issue needs to be addressed in any further revision of the methodology. In addition, there is a need to define overlapping ranges of R-R values for fuzzy classification of system hazard exposures according to MIL-STD categories (e.g., "unacceptable"). Beyond this, there is a need to further validate the integration of fuzzy sets and the SHA approach through analysis of real world applications.

Table 3: Comparison of HF-PFMEA and enhanced SHA approach in terms of analysis content

Item	Section	HF-PFMEA	Enhanced SHA
1	TLM	No	Yes
2	Hazards	Yes (based on guide words and process parameters)	Yes
3	Causes	Yes (based on performance shaping factors)	Yes
4	Human error type	Yes	Yes
5	Effects	Yes (based on the worst effect of errors)	Yes
6	Hazard likelihood	Yes (based on the likelihood of the worst effect)	Yes
7	Severity	Yes	Yes
8	Initial risk index	Yes	Yes
9	Controls	Yes	Yes
10	Human reliability	Yes (based on likelihood of error)	Yes
11	Automation reliability	No	Yes
12	Parallel/series system selection	No	Yes
13	System reliability	No	Yes
14	Risk-Reliability score	No	Yes
15	Final risk index	No	Yes

References

1. Bahr, N., 1997, System Safety Engineering and Risk Assessment: A Practical Approach. Boca Raton, FL: CRC Press.
2. Ericson, C. A., 2005, Hazard Analysis Techniques for System Safety. New York: Wiley.
3. Swain, A. D., 1990, "Human reliability analysis: Need, status, trends and limitations," Reliability Engineering & System Safety, 29(3), 301-313.
4. Chandler, F., Chang, Y., Mosleh, A., Marble, J., Boring, R., & Gertman, D., 2006, "Human reliability analysis methods: selection guidance for nasa," NASA Office of Safety and Mission Assurance, Washington, DC, 123.
5. Kim, I. S., 2001, "Human reliability analysis in the man–machine interface design review," Annals of nuclear energy, 28(11), 1069-1081.
6. Embrey, D., 2004, "Qualitative and quantitative evaluation of human error in risk assessment," Human factors for engineers. Landon: IET, 151.
7. Suokas, J., 1982, "Safety analysis of a liquefied gas storage and loading system," Journal of Occupational Accidents, 4(2), 347-354.
8. Bligård, L. O., & Osvalder, A. L., 2014, "Predictive use error analysis–Development of AEA, SHERPA and PHEA to better predict, identify and present use errors," Int. J. of Indus. Ergo., 44(1), 153-170.
9. Zadeh, L. A., 1975, "The concept of a linguistic variable and its application to approximate reasoning," Information sciences, 8(3), 199-249.
10. Chen, G., & Pham, T. T., 2000, "Introduction to fuzzy sets, fuzzy logic, and fuzzy control systems," CRC press.
11. Meister, D., 1964, "Methods of predicting human reliability in man–machine systems," Human Factors: The Journal of the Human Factors and Ergonomics Society, 6(6), 621-646.
12. Lewis, E. E., & Lewis, E. E., 1987, Introduction to reliability engineering (Vol. 2). New York et al.: Wiley.