Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 865241, 17 pages
http://dx.doi.org/10.1155/2014/865241

Research Article

Adaptive Failure Identification for Healthcare Risk Analysis and Its Application on E-Healthcare

Kuo-Chung Chu and Lun-Ping Hung

Department of Information Management, National Taipei University of Nursing and Health Sciences, No. 365, Mingde Road, Beitou District, Taipei City 11219, Taiwan

Correspondence should be addressed to Kuo-Chung Chu; kcchu@ntunhs.edu.tw

Received 20 January 2014; Accepted 4 March 2014; Published 16 April 2014

Academic Editor: Young-Sik Jeong

To satisfy the requirement for diverse risk preferences, we propose a generic risk priority number (GRPN) function that assigns a risk weight to each parameter such that they represent individual organization/department/process preferences for the parameters. This research applies GRPN function-based model to differentiate the types of risk, and primary data are generated through simulation. We also conduct sensitivity analysis on correlation and regression to compare it with the traditional RPN (TRPN). The proposed model outperforms the TRPN model and provides a practical, effective, and adaptive method for risk evaluation. In particular, the defined GRPN function offers a new method to prioritize failure modes in failure mode and effect analysis (FMEA). The different risk preferences considered in the healthcare example show that the modified FMEA model can take into account the various risk factors and prioritize failure modes more accurately. In addition, the model also can apply to a generic e-healthcare service environment with a hierarchical architecture.

1. Introduction

With the trend of information overload, humans face more and more challenges in their activities and have to deal with them [1, 2]. Although most industries incorporate automation techniques into production processes to deal with the challenges, the risk of failure always exists in processes where humans are involved. Moreover, in many industries, such as the aerospace, automobile, and healthcare sectors, human safety is the primary concern; hence, risk management is a hot topic in such industries. Strategies used to manage risk include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

Certain aspects of many risk management standards have been criticized because they do not achieve a measurable reduction in risk, even though confidence in the estimates and decisions based on the standards is raised. Risk management can be defined as the identification, assessment, and prioritization of risks followed by the coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events [3] or to maximize the realization of opportunities. Various industries (e.g., manufacturing and aviation) have long used this risk assessment process to evaluate system safety, and healthcare organizations are now using it to evaluate and improve the safety of patient care services. The risk management field is no different from any other area of management where standards proliferate. It is necessary to highlight some of the most important terms used in the field of risk management and provide examples of how they are defined in some of the well-known reference materials. The ISO Guide 73 : 2009 [4] defines the terms used in risk management. Its objective is "to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk." The first edition of the ISO/IEC Guide 73 was published by the ISO Technical Management Board (TMB) Working Group 2 on risk management terminology. The second edition was compiled by the ISO TMB Working Group on

risk management in association with the development of ISO 31000 to reflect changes in risk management practices and feedback from users.

Studies of safety in the healthcare and other sociotechnological industries have demonstrated repeatedly that human error is the cause of many accidents in complex systems. In air traffic control, for example, it has been found that 80–90% of accidents are caused by human error rather than technical malfunctions [5]. The statistics for healthcare services are similar. For example, in [4], it was reported that 82% of anesthesia-related accidents were due to human error. The causes of human failure in the healthcare industry are the same as those in other industries, for example, distractions, mental fatigue, misdirected attention, and misinterpretation of information [6]. A 1999 report published by the American Hospitals Association estimated that at least 44,000, and perhaps as many as 98,000 Americans, die every year due to errors made in hospitals [7]. The figure is higher than the number of people who die annually in the United States as a result of motor vehicle accidents (43,458), breast cancer (42,297), or AIDS (16,516) [8]. If we evaluate the human tragedy in terms of financial costs, medical errors rank among the most urgent and widespread public problems. The Institute of Medicine (IOM) report [8] on the quality of healthcare in America (entitled *To Err is Human: Building a Safer Health System)* states that "... healthcare is a decade or more behind other high-risk industries in its attention to ensuring basic safety." Thus, we must pay more attention to healthcare industry that depends on perfect human performance and endeavor to eliminate adverse events and medical errors in the industry [9, 10].

To provide safe healthcare services, the industry must use every possible means to reduce risks. Generally, human errors are unavoidable because they are caused by environmental factors rather than incompetence on the part of the individuals involved. It is necessary to enhance patient care practices and establish standard operating procedures (SOPs). In [8], the authors posit that human errors occur because good people have to work in bad systems that need to be made safer [11]. Improving service quality and risk management may improve patient safety.

Failure mode and effect analysis (FMEA) is a technique that identifies the potential failure modes of a product or a process, determines the effects of failures, and assesses the criticality of the effects on the functionality of the product or service. It provides a mechanism for reliability prediction and process design. According to BS 5760 Part 5 [12], "FMEA is a method of reliability analysis intended to identify failures, which have consequences affecting the functioning of a system within the limits of a given application, thus enabling priorities for action to be set." It has been shown that FMEA is a useful tool for identifying potential failures in a tabular and structured manner. In an FMEA table, a list of critical items helps individuals identify potential failures and ensure the safety of the operating procedures.

However, the risk priority number (RPN) defined in FMEA cannot identify some failures. This shortcoming is due to the nonlinear structure of the RPN function in which the three parameters, that is, severity, occurrence, and detectability (SOD), are equally important. The RPN function has difficulty differentiating the type of risk (i.e., the failure mode). In an attempt to resolve the problem, we propose a generic RPN (GRPN) function that assigns a weight to each parameter so that the weights represent individual industry preferences for the parameters. The function is calculated with the logarithm of the weight and then transformed into a linear function to estimate the risk independently of the three parameters. The GRPN function-based FMEA model is capable of differentiating the type of risk, and it satisfies the requirement for diversified risk preferences. To validate the proposed adaptive risk identification model, we apply it to a case of testing Down syndrome and compare the results with those derived using the traditional RPN approach.

In addition, the global population is predicted to expand with both a shrinking number of economically active and a larger proportion of older people. The number of people with long-term conditions will increase the importance of perceived health. Due to the constant advances of mobile and wireless technologies, user-generated service is a development trend of mobile services [13]. Using the technologies to improve people's health and the delivery of healthcare have not only brought about caregiver/care provider connectivity but have brought the healthcare into a new era of ubiquitous/pervasive healthcare [14–16]; there are several examples: stroke patient monitoring and guidance for promoting rehabilitation, location tracking, vital signs and well-being data acquisition and analysis, fall detection, behavior tracking, and sleep analysis. No matter what the examples are, a lot of sensing devices are involved in distributed environment that requires a collaborative decision analysis system or workflow-driven healthcare platform for collaborative applications [17]. To facilitate the ubiquitous service, an ontology-based evaluation model is proposed to ensure the service quality [18]; while an emerging area called intelligent environments provide an integrated approach for collaborative data management of ubiquitous services [19]. Those studies show that e-healthcare is an emerging research issue and thus we propose the application of adaptive risk identification model on e-healthcare.

The remainder of this paper is organized as follows. In Section 2, we review the literature on risk management and the FMEA model. In Section 3, we propose a modified FMEA model called GRPN that includes model formulation, validation, and simulation. In Section 4, we conduct sensitivity analysis to compare the model's performance with that of RPN. In Section 5, we present a case study of healthcare risk analysis and show the adaptability of the proposed approach; in Section 6, we also apply the proposed model to e-healthcare environment; in Section 7, we conclude this paper with contributions and discussions.

2. Related Work

2.1. Failure Model and Effect Analysis (FMEA). FMEA has been used in the aerospace and automobile industries for several decades. The aerospace industry used FMEA as a formal design methodology in the 1960s because of the need for a

Table 1: Description of the three risk factor scales.

Scale	Factors		
	Severity	Occurrence	Detectability
1~2	Insignificant effect	Rare	Will detect a failure
3~4	Minor effect	Unlikely	Likely to detect a failure
5~6	Moderate effect	Possible	Might detect a failure
7~8	Major effect	Likely	Unlikely to detect a failure
9~10	Hazardous effect	Almost certain	Detection of a failure is highly unlikely

high level of reliability and safety. It is now used extensively to ensure the safety and reliability of products/processes in a wide range of industries, particularly the aerospace, automotive, and nuclear industries. In FMEA, the RPN is used to assess the level of risk based on three factors. The Potential Failure Mode and Effects Analysis Manual [20], section QS-9000, classifies the risk factors as follows: (1) severity (S): a rating of the seriousness of the effects of a potential failure; (2) occurrence (O): a rating of the likelihood that the failure will occur; (3) detectability (D): a rating of the likelihood that the current detection methods or controls will detect a potential failure mode. The three factors are rated on a scale of 1 to 10 on the basis of degree, as shown in Table 1. The RPN, which is denoted as a traditional RPN (TRPN), is the product of severity, occurrence, and detectability, as expressed in

$$\text{TRPN} = S \times O \times D. \tag{1}$$

The TRPN provides the foundation for improvement; that is, the larger the TRPN, the greater the potential for improvement. Corrective action is taken by the relevant departments, beginning with the department that makes the largest contribution to the risk. After corrections are made, the TRPN should be recalculated to determine if the risks have been reduced and to check the effectiveness of the corrective actions taken by each contributor.

To begin with FMEA, a high-level process flowchart should be compiled and appropriate knowledge resource experts should be selected to form an FMEA project team. An FMEA knowledge expert should be nominated to train team members in the selected process. On completion of their training, the team should start to build an FMEA model for the process. From the high-level flowchart, the team should identify the process functions and determine the scope of the project.

There are five steps in the FMEA method:

(1) select a procedure/subprocedure for study;

(2) assemble a team;

(3) make a diagram of the procedure/subprocedure;

(4) identify the failure modes (risks):

  (a) brainstorm potential failure modes, ascertain why they might happen, and determine their effects in terms of the occurrence, severity, and detectability criteria;

  (b) compile a worksheet for risk analysis, and rank the risk for each failure point;

(5) take corrective action:

  (a) redesign the process if the effects of errors are unacceptable;

  (b) analyze, test, implement, and monitor the new process.

2.2. Application of FMEA in Different Industries. The FMEA tool was developed by the US military in the late 1940s to evaluate system and equipment failures. Since then, it has been widely used in various industries. For example, the aerospace industry began utilizing FMEA in the mid-1960s, and it was adopted by the healthcare industry in the late 1990s. FMEA helps healthcare organizations reduce potential risks and allows them to develop control strategies for high-risk processes. In hospitals, for example, improving service quality and risk management to ensure patient safety are becoming increasingly critical. The Joint Commission (TJC) standard LD.4.40 regards proactive risk assessment as an element of the performance of all accredited facilities. Since 2003, TJC has mandated all accredited organizations to analyze at least one high-risk process annually and identify ways that a breakdown or process failure could occur. Organizations are also required to prioritize potential process breakdowns, redesign the processes, and assess the effects of any changes that are made [21].

FMEA is exactly the type of technique or model that TJC recommends to fulfill all of the above requirements. Like any new strategy, refining an FMEA model takes some practice; however, once the model is established, it becomes an indispensable technique in any hospital's risk assessment plan. In response to public concern about medical errors, the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) promised to enhance patient safety. Since 1996, JCAHO has introduced several standards to improve patient safety; and it set October 2001 as the date that all healthcare facilities had to have some kind of risk assessment framework in place. The commission did not specify the process that had to be used; however, the FMEA model satisfies the requirement. Under the JCAHO directive, facilities must perform a proactive risk assessment of at least one high-risk process annually. The choice of process can be driven by internal patient safety needs or the JCAHO sentinel event alerts. Much of what needs to be done to improve safety in the healthcare sector has been accomplished already in other industries. In 2001, the JCAHO chose the FMEA as an appropriate safety improvement technique for healthcare services.

2.3. Critique of the TRPN Model. Since more than 40 years, FMEA has been used successfully in various industries to predict how a work process may fail or how a device may be used incorrectly [22]. FMEA involves close examination

of high-risk procedures or error-prone processes to identify improvements that would reduce the occurrence of unintended adverse events. The method provides a straightforward, proactive process of risk identification and quality improvement that is simple to learn and is applicable in all settings. FMEA has proven to be one of the most important proactive measures that can be adopted to prevent failures and errors from occurring in a system, design, process, or service so that they do not reach the customer. However, for various reasons, the TRPNs have attracted a considerable amount of criticism [23–28].

The shortcomings of the TRPN model are analyzed in depth [29]. Here, we review them briefly. Recall that the TRPN is the mathematical product of three factors (S: the severity of the effect, O: the probability of occurrence, and D: the probability of detectability) related to a failure mode rated on a scale of 1 to 10 based on a number of linguistic terms. The first shortcoming is that the TRPN elements are not weighted equally in terms of risk. As a result, SOD scenarios in which their TRPNs are lower than other combinations could still be dangerous. For example, in a scenario with very high severity, a low rate of occurrence, and very high detectability, the TRPN $9 \times 3 \times 2 = 54$ is lower than in the scenario with a moderate severity level, moderate rate of occurrence, and low detectability where the TRPN $4 \times 5 \times 6 = 120$, even though it should have a higher priority for corrective action. The second shortcoming is that the TRPN scale has some nonintuitive statistical properties. The initial and correct assumption that the scale starts at 1 and ends at 1000 often leads to incorrect assumptions about the midpoint of the scale. The 1000 TRPN numbers are generated from all possible combinations. However, most TRPN values are not unique, and some are recycled up to 24 times.

3. Method

3.1. Model Formulation

3.1.1. Formulation of a Generic RPN (GRPN). The traditional FMEA model assumes that the contributions of the risk factors (SOD) to the value of the TRPN are homogeneous. However, the importance of each indicator probably depends on the type of industry. Therefore, a modified RPN function is needed to provide a more generalized application and to rectify any bias in the TRPN indicators. For example, in aerospace, automotive, and medical applications, the impact of severity (S) on the failure effect should be greater than that of frequency (O). When failures occur, regardless of the frequency, high priority should be given to taking corrective action. Because the above-mentioned industries involve the safety of people, the importance of S is significantly greater than that of O. By contrast, in commodity manufacturing, the priority is to reduce the frequency (O) of failures, so O is more important than S. To differentiate between the priorities of the three TRPN indicators (SOD), we denote their weights as w_S, w_O, and w_D, respectively; the weight is an exponent of the indicator, such that $w_S + w_O + w_D = 1$. Then, the expression of the logarithm operation represents the RPN as a linear function of the parameters. We define the function as a generic RPN (GRPN) with two types of parameters, namely, risk factors and risk weights, as expressed in

$$\begin{aligned} \mathrm{GRPN}(w_S, w_O, w_D) &= \log\left(S^{w_S} \cdot O^{w_O} \cdot D^{w_D}\right) \\ &= w_S \log S + w_O \log O + w_D \log D. \end{aligned} \tag{2}$$

Table 2: Priority of the risk weights with respect to concern priority of the risk factors.

Concern priority of the risk factors	Priority of the risk weights
$S > O > D$	w_S (H) > w_O (M) > w_D (L)
$S > D > O$	w_S (H) > w_D (M) > w_O (L)
$O > S > D$	w_O (H) > w_S (M) > w_D (L)
$O > D > S$	w_O (H) > w_D (M) > w_S (L)
$D > S > O$	w_D (H) > w_S (M) > w_O (L)
$D > O > S$	w_D (H) > w_O (M) > w_S (L)

3.1.2. Using a GRPN-Based FMEA Model. The GRPN, which is a modified FMEA model, is a function of the risk factors (SOD) and the weights (w_S, w_O, w_D). Although the failure model is related to S, O, and D, the three factors are independent; therefore, each of them can be described by a stochastic model. To apply the modified FMEA model based on the GRPN function, we consider the possible effects of the factors and the values of the weights.

(i) Risk factors (SOD): to evaluate the feasibility of the modified FMEA, SOD can be simulated as a stochastic model, for example, with a uniform (U) distribution or a normal (N) distribution. The SOD factors form eight combinations: UUU, UUN, UNU, UNN, NUU, NUN, NNU, and NNN.

(ii) Risk weights (w_S, w_O, w_D): the weight of each factor is given a value, that is, low (L), medium (M), or high (H). The weights form six combinations: LMH, LHM, MLH, MHL, HLM, and HML. In fact, the weight combinations could vary in different organizations. The weights can be arbitrarily assigned only if the sum of the weights is equal to 1 (L + M + H = 1). For example, if the factor S is more important than the factor O, it will give a larger value of the weight w_S than the value of the weight O, and vice versa. On the basis of concern priority of the risk factors, we illustrate possible weight priority respective to the risk factors, as in Table 2. In this paper, for example, we give L = 0.1, M = 0.3, and H = 0.6. In addition, we consider a special weight (E, E, E), where E = 0.333 (1/3), to be equivalent to TRPN-based FMEA model.

Both the factor distributions and the weights consist of 56 combinations. To determine the applicability of the proposed model, we assess the effect of the GRPN values in all combinations of the parameters. For all the 56 combinations, let D_i denote the ith distribution of the GRPN values, and let T_i denote the acceptable level of the risk value

Table 3: Possible combination of the risk factors and weights.

GRPN (D_i, T_i)	Combination of (w_S, w_O, w_D), GRPN							TRPN
	(L, M, H)	(L, H, M)	(M, L, H)	(M, H, L)	(H, L, M)	(H, M, L)	(E, E, E)	
(S, O, D)								
(UUU)	(D_1, T_1)	(D_2, T_2)	(D_3, T_3)	(D_4, T_4)	(D_5, T_5)	(D_6, T_6)	(D_7, T_7)	TRPN1
(UUN)	(D_8, T_8)	(D_9, T_9)	(D_{10}, T_{10})	(D_{11}, T_{11})	(D_{12}, T_{12})	(D_{13}, T_{13})	(D_{14}, T_{14})	TRPN2
(UNU)	(D_{15}, T_{15})	(D_{16}, T_{16})	(D_{17}, T_{17})	(D_{18}, T_{18})	(D_{19}, T_{19})	(D_{20}, T_{20})	(D_{21}, T_{21})	TRPN3
(UNN)	(D_{22}, T_{22})	(D_{23}, T_{23})	(D_{24}, T_{24})	(D_{25}, T_{25})	(D_{26}, T_{26})	(D_{27}, T_{27})	(D_{28}, T_{28})	TRPN4
(NUU)	(D_{29}, T_{29})	(D_{30}, T_{30})	(D_{31}, T_{31})	(D_{32}, T_{32})	(D_{33}, T_{33})	(D_{34}, T_{34})	(D_{35}, T_{35})	TRPN5
(NUN)	(D_{36}, T_{36})	(D_{37}, T_{37})	(D_{38}, T_{38})	(D_{39}, T_{39})	(D_{40}, T_{40})	(D_{41}, T_{41})	(D_{42}, T_{42})	TRPN6
(NNU)	(D_{43}, T_{43})	(D_{44}, T_{44})	(D_{45}, T_{45})	(D_{46}, T_{46})	(D_{47}, T_{47})	(D_{48}, T_{48})	(D_{49}, T_{49})	TRPN7
(NNN)	(D_{50}, T_{50})	(D_{51}, T_{51})	(D_{52}, T_{52})	(D_{53}, T_{53})	(D_{54}, T_{54})	(D_{55}, T_{55})	(D_{56}, T_{56})	TRPN8

Table 4: An example of corrective action on the failure mode (FM) with respect to T.

Risk weight*			GRPN	Action or not with respect to given threshold T^{**}				
w_S	w_O	w_D		$T = 0.60$	$T = 0.65$	$T = 0.70$	$T = 0.75$	$T = 0.80$
0.1	0.3	0.6	0.78	Yes	Yes	Yes	Yes	No
0.1	0.6	0.3	0.72	Yes	Yes	Yes	No	No
0.3	0.1	0.6	0.70	Yes	Yes	Yes	No	No
0.3	0.6	0.1	0.60	Yes	No	No	No	No
0.6	0.1	0.3	0.52	No	No	No	No	No
0.6	0.3	0.1	0.48	No	No	No	No	No

*$(S, O, D) = (2, 5, 8)$ and GRPN $= \log(S^{w_S} \cdot O^{w_O} \cdot D^{w_D})$.
**T denoted as GRPN threshold T_i.

(GRPN threshold) for the ith combination. In addition, for comparison, TRPNs (TRPN1~TRPN8) are also simulated with the risk factors (SOD) in both uniform and normal distributions. The overall combination is shown in Table 3.

Risk analysis is based on an acceptable risk probability α, which is assigned by organization, department, or process. Given α, a threshold can be precalculated, where Prob (GRPN $\leq$ T_i) = α and the probability that the GRPN value is less than or equal to T_i is equal to α, as shown in Figure 1. Whenever the GRPN value $>$ T_i, priority should be given to take corrective action on the failure mode (FM). The threshold T_i can be analyzed and suggested by a simulation approach with respective scenarios, as discussed in Section 3.3.

In this section, we give an example to show how the proposed model works. Having an FM, for example, we assign a risk factor (S, O, D) to (2,5,8), and the risk weight (L, M, H) is given (0.1, 0.3, 0.6). Corrective action should be taken on the FM whenever its GRPN value is greater than or equal to a given threshold T_i. The weight combination (w_S, w_O, w_D) is illustrated in Table 4 to show whether we should act on the FM. To use the proposed model, we summarize the procedure in the following steps in which GRPN$'$ and GRPN$''$ denoted the GRPN values that are calculated in simulated and real environments, respectively. The most important thing is to decide the threshold T_i by a simulation process with a given α.

(1) Use historical data of risk factors (S, O, D) to build a probability model of the factors.

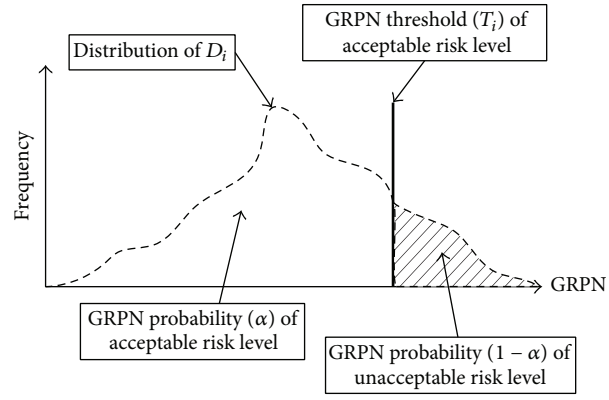


Figure 1: Analysis of the acceptable risk.

(2) Give α and risk weights (w_S, w_O, w_D) according to organization policy.

(3) Suggest threshold T_i by analyzing GRPN$'$ with probability model from step (1), such that Prob (GRPN $\leq$ T_i) = α.

(4) Create an FMEA worksheet (a comprehensive worksheet example will be given in Section 5.1), and compute GRPN$''$ on all FMs.

(5) Act on FMs whose GRPN$''$ are greater than T_i.

(6) Repeat steps (2) to (5) until GRPN$'' \leq T_i$.

Table 5: The statistics of simulation input functions.

Name	S (U)	O (U)	D (U)	S (N)	O (N)	D (N)
Min.	1.00057	1.000374	1.000033	1.484494	1.780332	1.560566
Mean	5.500004	5.5	5.499998	5.499975	5.500002	5.500066
Max.	9.999767	9.999713	9.999903	9.266962	9.414956	10.13493
5% of percentile	1.449774	1.449551	1.449979	3.854347	3.854757	3.854582
95% of percentile	9.549781	9.54951	9.549447	7.144094	7.144127	7.144537

3.2. Model Validation—Simulation Approach

3.2.1. Simulation Models and Inputs. The normal distribution is that random variable X is with the probability density function as defined in (3), where μ and σ are mean and standard deviation, respectively. The former determines central tendency, while the latter measures the degree of dispersion. The distribution can be expressed as $X \sim N(\mu, \sigma)$, where $\pi = 3.14159\ldots$ and $e = 2.71828\ldots$. Consider

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{(-1/2)((x-\mu)/\sigma)^2}, \quad -\infty < x < \infty. \tag{3}$$

In addition, uniform distribution is that random variable Y is with the equal probability in the range of (a, b) as defined in (4), where the probability function value is independent of the variable y. The distribution can be expressed as $Y \sim U(a, b)$:

$$f(y) = \frac{1}{b-a}, \quad a < y < b. \tag{4}$$

The validation uses @RISK decision tool, Palisade Corporation [30]. On the basis of simulation settings, the simulation models by way of @RISK functions, RISKUNIFORM (1, 10) and RISKNORM (5.5, 1), are defined as follows, where C3, C4, K3, K4 are names of cells in a datasheet of Microsoft Excel, and RiskStatic () is a function of @RISK tool.

(i) Uniform functions:

S(U), O(U), D(U): RiskUniform (C4, C3, RiskStatic (9.76))

(ii) Normal functions:

S(N): RiskNormal (K3, K4, RiskStatic (5.17))
O(N): RiskNormal (K3, K4, RiskStatic (5.20))
D(N): RiskNormal (K3, K4, RiskStatic (5.20))

We define a rounding function in @RISK model to guarantee integer value for all inputs of risk factor SOD. For example, a generated set of risk factors $(S, O, D) = (1.65, 3.89, 9.26)$ is rounded to (2, 4, 9). To ensure that the generated values are in the range of [1, 10], we also define a filter in @RISK model. The values smaller than 0.5 or greater than 10.5 are discarded. After 10,000 iterations in the simulation, Table 5 summarizes the statistics of input function and their details.

To validate the proposed model, two stochastic distributions, uniform (U) and normal (N), are simulated up to 10,000 iterations for three risk factors: severity, occurrence, and detectability. There are two parameters, lower bound (LB) and upper bound (UB), defined in the uniform distribution U $\sim$ (LB, UB), while mean (μ) and standard deviation (ρ) are given in the normal function N $\sim$ (μ, ρ). In this study, simulation settings are defined as U $\sim$ (1, 10) and N $\sim$ (5.5, 1.5) for uniform and normal distributions, respectively. The risk weights are assigned to L = 0.1, M = 0.3, and H = 0.6 throughout the paper. The simulation settings are listed in Table 6.

Table 6: The simulation settings.

Workbook name	Simulation models
Number of simulations	1
Number of iterations	10000
Number of inputs	6
Number of outputs	64
Sampling type	Latin hypercube
Simulation start time	5/7/11 19:39:34
Simulation duration	00:00:07
Random number generator	Mersenne twister
Random seed	404885595

3.3. Simulation Results

3.3.1. Details of Data Statistics. To easily review the simulation results, we summarize the descriptive statistics of RPN values (TRPN and GRPN) with (1) mean and standard deviation (SD) (mean ± SD), (2) skewness, and (3) kurtosis in Table 7, and the distribution sketch is shown in Figure 2.

We describe the central location of the distribution via mean value and the spread via SD. For the GRPN function, the mean values are in a range of 0.67 to 0.73, while the SDs are in a range from 0.05 to 0.18; they are shown as a stable result. For TRPN function, the mean values are around 166, and SDs varied from 56.38 to 153.37.

Skewness is used to measure the asymmetry of the distribution. The GRPN values are all negative in range from −0.37 to −0.88, while the TRPN values are all positive in range from 0.60 to 1.56. The negative values verify the critique that most TRPN values are not unique, and some are recycled up to 24 times [29]. Kurtosis is used to measure the extent of the distribution peak. For the GRPN function, the kurtosis is in a range from 3.02 to 3.75 and a range from 2.95 to 5.55 in the GRPN function. Applying the RPN-based FMEA model to manage risks, an acceptable risk probability

Table 7: Descriptive statistics of mean ± SD, skewness, and kurtosis.

Mean ± SD, skewness, and kurtosis	Combination of (w_S, w_O, w_D), GRPN							TRPN
	(L, M, H)	(L, H, M)	(M, L, H)	(M, H, L)	(H, L, M)	(H, M, L)	(E, E, E)	
(S, O, D)								
	0.67 ± 0.18	0.67 ± 0.18	0.67 ± 0.18	0.67 ± 0.18	0.67 ± 0.18	0.67 ± 0.18	0.67 ± 0.15	165.80 ± 153.37
(UUU)	−0.72	−0.71	−0.71	−0.70	−0.72	−0.71	−0.51	1.56
	3.09	3.07	3.08	3.03	3.09	3.08	3.05	5.55
	0.67 ± 0.18	0.69 ± 0.16	0.71 ± 0.10	0.68 ± 0.18	0.69 ± 0.16	0.68 ± 0.18	0.69 ± 0.13	166.30 ± 124.94
(UUN)	−0.72	−0.85	−0.61	−0.72	−0.85	−0.73	−0.60	1.08
	3.09	3.08	3.18	3.03	3.10	3.07	3.03	3.84
	0.69 ± 0.16	0.71 ± 0.10	0.68 ± 0.18	0.71 ± 0.10	0.68 ± 0.18	0.69 ± 0.16	0.69 ± 0.13	166.01 ± 124.85
(UNU)	−0.85	−0.58	−0.73	−0.56	−0.73	−0.85	−0.59	1.11
	3.10	3.09	3.08	3.04	3.08	3.09	3.03	3.96
	0.73 ± 0.06	0.73 ± 0.06	0.71 ± 0.10	0.71 ± 0.10	0.70 ± 0.16	0.70 ± 0.16	0.71 ± 0.10	166.58 ± 94.61
(UNN)	−0.44	−0.45	−0.61	−0.61	−0.87	−0.87	−0.69	0.67
	3.41	3.43	3.07	3.06	3.08	3.09	3.02	3.11
	0.68 ± 0.18	0.68 ± 0.18	0.69 ± 0.16	0.69 ± 0.16	0.71 ± 0.10	0.71 ± 0.10	0.69 ± 0.13	166.40 ± 125.19
(NUU)	−0.74	−0.73	−0.85	−0.85	−0.59	−0.59	−0.59	1.08
	3.09	3.07	3.11	3.08	3.14	3.10	3.04	3.79
	0.71 ± 0.10	0.70 ± 0.16	0.73 ± 0.06	0.70 ± 0.16	0.73 ± 0.06	0.71 ± 0.10	0.71 ± 0.10	166.56 ± 93.80
(NUN)	−0.66	−0.88	−0.48	−0.88	−0.50	−0.66	−0.73	0.60
	3.25	3.10	3.50	3.09	3.59	3.16	3.10	2.95
	0.70 ± 0.16	0.71 ± 0.10	0.70 ± 0.16	0.73 ± 0.06	0.71 ± 0.10	0.73 ± 0.06	0.71 ± 0.10	166.40 ± 94.14
(NNU)	−0.88	−0.63	−0.88	−0.47	−0.64	−0.47	−0.72	0.65
	3.11	3.17	3.12	3.49	3.21	3.58	3.13	3.03
	0.73 ± 0.06	0.73 ± 0.06	0.73 ± 0.06	0.73 ± 0.06	0.73 ± 0.06	0.73 ± 0.06	0.73 ± 0.05	166.68 ± 56.38
(NNN)	−0.51	−0.54	−0.49	−0.53	−0.52	−0.53	−0.39	0.64
	3.57	3.71	3.48	3.67	3.75	3.75	3.30	3.59

Table 8: Threshold value (T_i) for each of the combinations with $\alpha = 0.9$.

T_i	Combination of (w_S, w_O, w_D), GRPN							TRPN
	(L, M, H)	(L, H, M)	(M, L, H)	(M, H, L)	(H, L, M)	(H, M, L)	(E, E, E)	
(S, O, D)								
(UUU)	0.88	0.88	0.88	0.88	0.88	0.88	0.86	378
(UUN)	0.88	0.87	0.83	0.89	0.87	0.89	0.85	350
(UNU)	0.87	0.83	0.89	0.83	0.89	0.87	0.85	350
(UNN)	0.80	0.80	0.83	0.83	0.87	0.87	0.82	294
(NUU)	0.89	0.89	0.87	0.87	0.83	0.83	0.85	350
(NUN)	0.83	0.87	0.80	0.87	0.80	0.83	0.82	294
(NNU)	0.87	0.83	0.87	0.80	0.83	0.80	0.82	294
(NNN)	0.80	0.80	0.80	0.80	0.80	0.80	0.80	245

α must be defined, which depends on the risk preference of organization, department, or process. Given α, a threshold can be precalculated where Prob (GRPN $\leqq T_i$) = α, as shown in Figure 1. Whenever the GRPN value > T_i, priority should be given to taking corrective action against the failure modes. In this paper, we assign $\alpha = 0.9$ as an example; then threshold values (T_i) with respective risk factors and the risk weights for each of combinations are suggested in Table 8. The threshold values for GRPN function are in the range from 0.80 to 0.89, while the threshold values for TRPN function vary from 245 to 378. Potential failure modes whose value are greater than the threshold in respective scenarios must be taken corrective actions. If several failure modes are more critical, we can assign α for them with a smaller value.

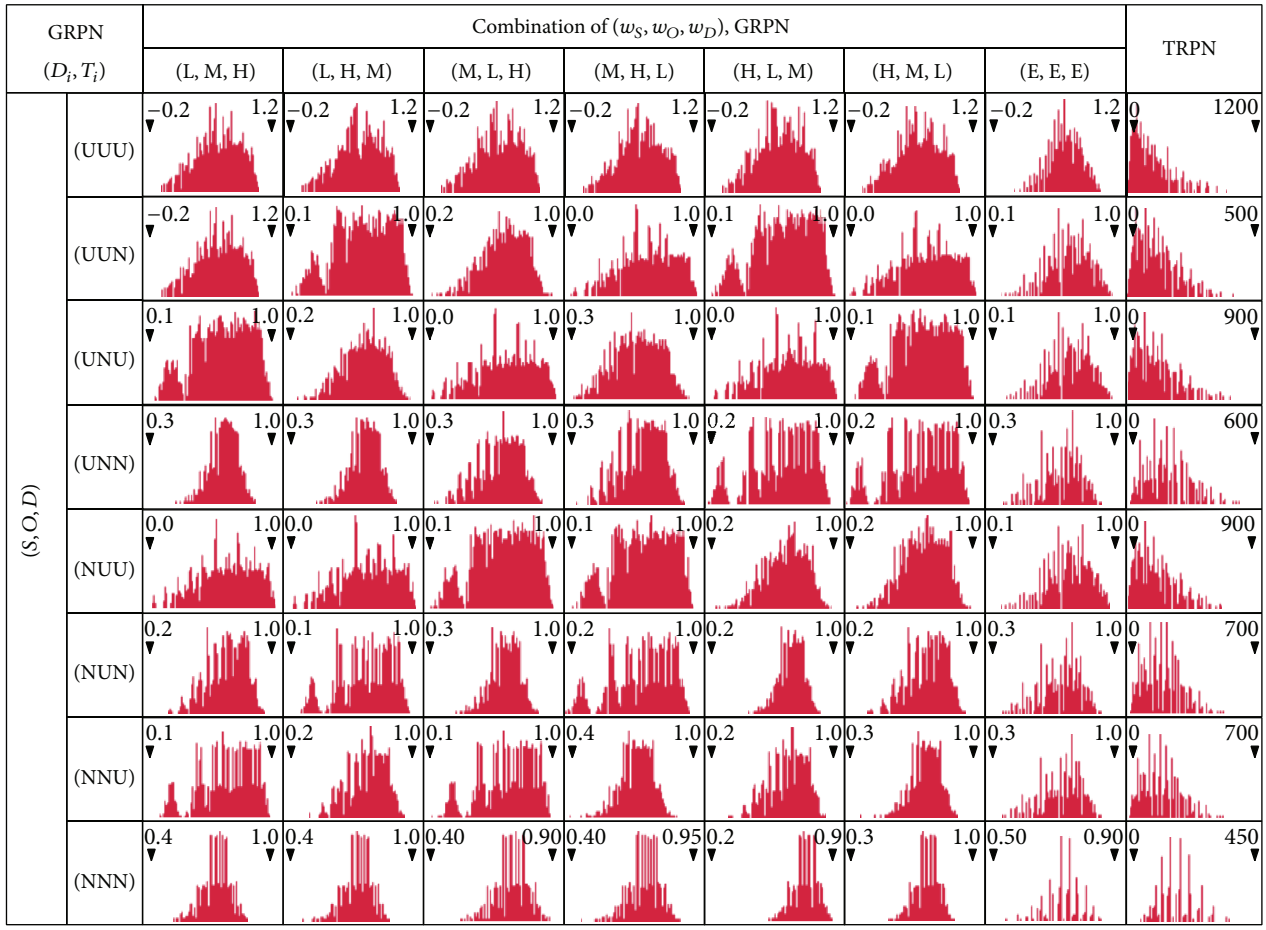


Figure 2: Comparison of correlation coefficients for the risk factors.

The smaller the acceptable risk probability (α), the larger the possibility that the GRPN values that are contributed by the failure modes will be greater than the T_i.

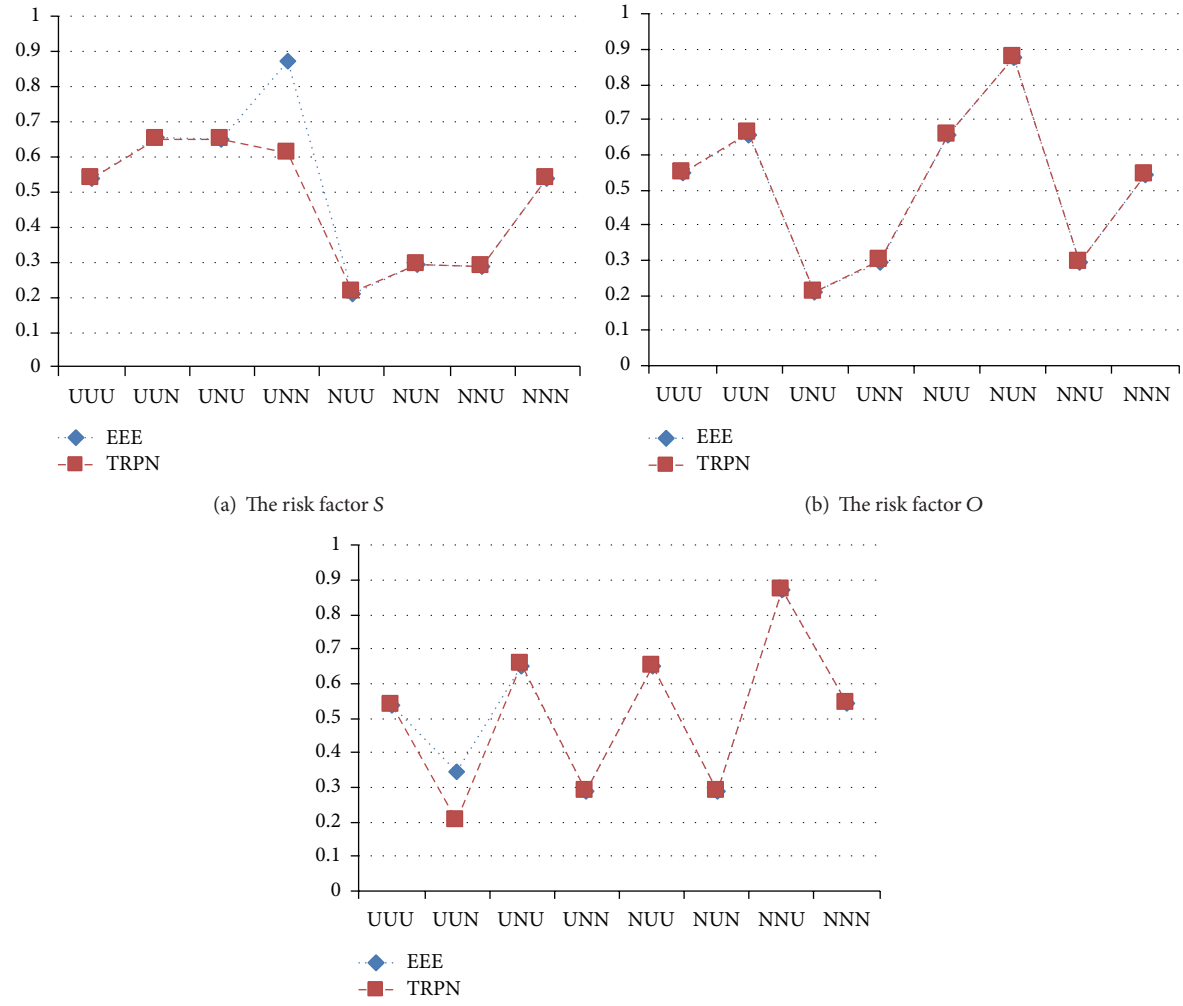
4. Sensitivity Analysis

To evaluate the function's stability, we perform sensitivity analysis on both correlation and regression. They are generated from the @RISK built-in function.

4.1. Correlation Coefficient. To validate that the proposed GRPN-based model dominates the TRPN-based model, the GRPN function is equivalent to TRPN when the risk weight is assigned with (EEE). Moreover, we compare the correlation coefficients of the risk factors (SOD) with different distributions (uniform and normal) respective to function values, that is, GRPN with weight (EEE) and TRPN. For the risk factor S in Figure 3, the values of both functions are almost the same, except the (UNN) distribution. They are 0.871 and 0.612 for EEE and TRPN, respectively. Regarding the risk factor O, both the functions are similar because the lines between each function overlap. Again, both functions are almost the same for the risk factor D except for the distribution (UUN). They are 0.348 and 0.203 for EEE and TRPN, respectively. According to the correlation coefficient, both the functions are highly correlated. This implies that the GRPN function is equivalent to TRPN function when the weight (EEE) is assigned.

4.2. Regression Coefficient. Regression analysis is used to investigate the relationship between the risk factors (independent variables) and RPN function value (dependent variable, that is, GRPN/TRPN function value). The coefficient of determination R^2 is used in the context of statistical models. The primary objective is to predict future outcomes on the basis of other related information. It is the proportion of variability in a dataset that is accounted for the statistical model. It also provides a measure of how well the future outcomes are likely to be predicted by the model.

In Figure 4, we illustrate the R^2 values for all combinations. Regardless of the risk weight (LMH, LHM, MLH, MHL, HLM, HML, or EEE) assigned, the GRPN function has stable R^2 values about 0.9; they are in a range from 0.894 to 0.906. The results show that the proposed GRPN function outperforms TRPN function because the R^2 of the GRPN function is stable and greater than that of the TRPN function. An interesting finding is that the R^2 values of TRPN



(a) The risk factor S

(b) The risk factor O

(c) The risk factor D

FIGURE 3: Distribution sketch with respect to risk factors and risk weights.

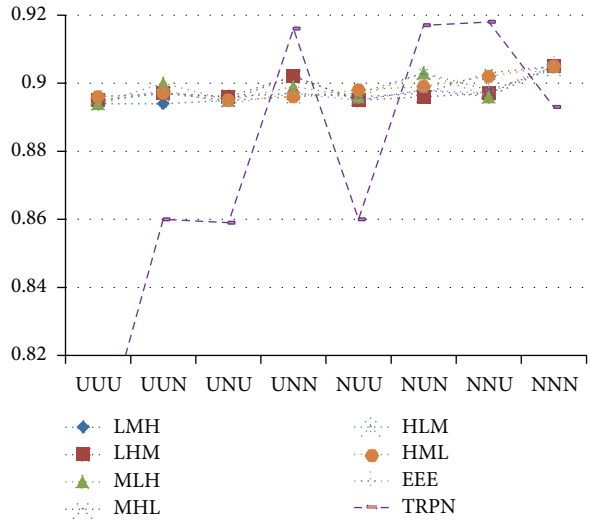


FIGURE 4: R^2 comparison of eight distributions with respect to several risk weights.

function are larger than that of GRPN function in three special cases of SOD distribution, that is, UNN, NUN, and NNU. The TRPN function is suitable for cases in which the majority of the three risk factors are in normal distribution, whereas the GRPN function is suitable for the others. In general, the proposed GRPN function offers a more adaptive approach, which can be applied in industries with various risk preferences.

5. Case Study

5.1. An Example of Down Syndrome Test. We use an example of Down syndrome test—a healthcare application—to explain the operation of the proposed GRPN model. It is to identify significant achievement and its adaptability compared with that of the TRPN model. In addition, we consider three scenarios to demonstrate the adaptability of the proposed model. The steps are as follows:

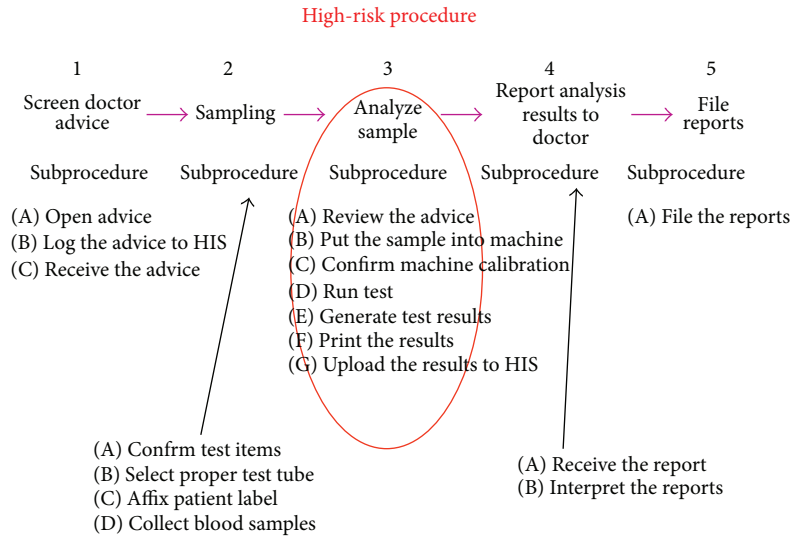


Figure 5: The test procedure for Down syndrome.

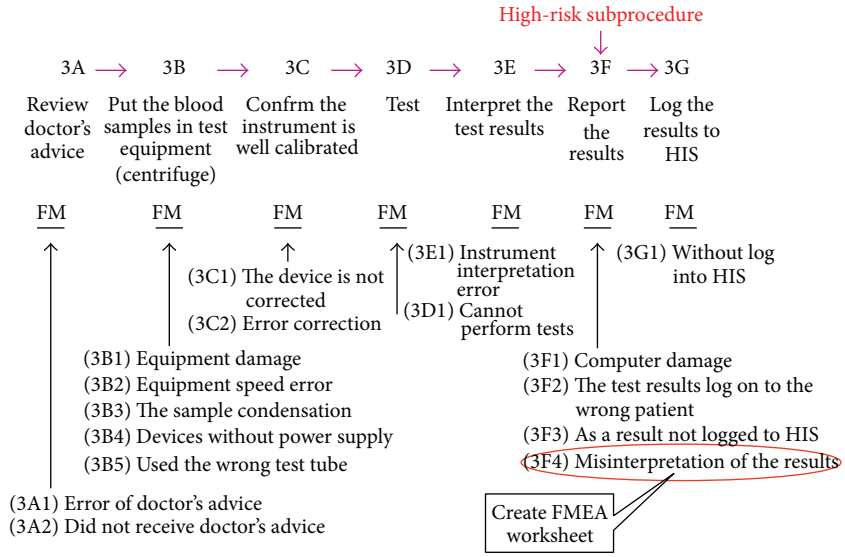


Figure 6: The high-risk subprocedures and the failure modes in Step 3.

Step 1. Select a procedure for study, as shown in Figure 5.

Step 2. Assemble a team to monitor the failure mode.

Step 3. Compile an operational risk analysis flowchart. If the third stage (analysis of the sample) involves a high-risk procedure, it is also necessary to implement the following (sub)procedures: (3A) review the doctor's advice; (3B) put the blood sample into the machine for testing; (3C) confirm that the machine is calibrated; (3D) run the test; (3E) generate the test results; (3F) print the results; and (3G) upload the results to the health information system (HIS). The results of the high-risk subprocedures (step 3F) and their failure modes are shown in Figure 6. The potential failure modes are damage to the computer, the test results are logged to the wrong patient's file, the results are not uploaded to the HIS, and misinterpretation of the results.

Step 4. Identify the potential failure modes via a group discussion. In Figure 6, the misinterpretation of the results (step 3F4) is probably a failure mode (FM).

Step (4-1). Identify the reasons for the failure, and determine its severity, occurrence, and detectability. For each failure mode, the root cause(s) of the failure should be determined. The failure "misinterpretation of the results" has four possible causes, namely, "too tired," "too busy,"

Table 9: Step 3F4 worksheet: misinterpretation of the results.

			Step 4: failure risk analysis						Step 5: correction/action/result				
			Rating*				Decision tree						
	Reasons for failure		S	O	D	GRPN	With Control mechanism	Problems Detectable	Continued	Correction	Action	Result	Role in charge
Step 3F4	3F4a	Too tired	9	8	2	0.874	No	Yes	Yes	Control	Confirmed by second examination	Confirmed by two examiners	Laboratory director
	3F4b	Too busy	3	9	8	0.663	No	No	Yes	Control	Personnel access control and provision of a single telephone	Replacement of laboratory and telephone system	General department
	3F4c	Insufficient light	2	8	8	0.542	No	No	Stop	Provide a second light source	Installation of new lights	Brighter lights	General department
	3F4d	Misunderstanding of the machine report	8	6	4	0.836	No	Yes	Yes	Need to deal with	Purchase new equipment	Equipment installed on a given date (YY/MM/DD)	Procurement department

*$w_S = 0.6$, $w_O = 0.3$, and $w_D = 0.1$.

Table 10: Comparison of the TRPN and GRPN test procedures—scenario 1.

FM	Risk factor			TRPN			GRPN		
	S	O	D	Value	Mean value of the acceptable threshold T	Identify risk	Value	Mean value of the acceptable threshold T	Identify risk
3F4a	9	8	2	*144*	*166*	*N*	*0.876*	*0.74*	*Y*
3F4b	3	9	8	*216*	*166*	*Y*	*0.663*	*0.74*	*N*
3F4c	2	8	8	128	166	N	0.542	0.74	N
3F4d	8	6	4	192	166	Y	0.836	0.74	Y

Table 11: Comparison of the TRPN and GRPN test procedures—scenario 2.

FM	Risk factor			TRPN			GRPN		
	S	O	D	Value	Mean value of the acceptable threshold T	Identify risk	Value	Mean value of the acceptable threshold T	Identify risk
3F4a	9	8	2	144	166	N	0.557	0.74	N
3F4b	3	9	8	216	166	Y	0.780	0.74	Y
3F4c	2	8	8	128	166	N	0.722	0.74	N
3F4d	8	6	4	*192*	*166*	*Y*	*0.710*	*0.74*	*N*

"insufficient light," and "misunderstanding of the machine report."

Step (4-2). Compile an FMEA worksheet (as shown in Table 9).

Step (4-3). Sort the failure modes by their GRPN values.

Step 5. Take corrective action if the GRPN value of a failure mode is higher than a given threshold.

5.2. Comparison of the GRPN and RPN Test Procedures. To differentiate between GRPN-based FMEA model and the TRPN-based FMEA approach, we consider different values for the weights (w_S, w_O, w_D). Let *** denote weight "H" (value 0.6), ** denote weight "M" (value 0.3), and * denote weight "L" (value 0.1). In addition, we set the threshold value for traditional RPN functions at 166 (it is the average RPN value = SOD) [20] and calculate an equivalent threshold value (with SOD = 166) for the GRPN at 0.74. We also give an average value of the weights (equal weight), $w_S = w_O = w_D = 0.333333$; then the GRPN value is $\log(S^{w_S} \cdot O^{w_O} \cdot D^{w_D}) = w_S \log S + w_O \log O + w_D \log D = w_S * (\log S + \log O + \log D) = w_S * \log(\text{SOD}) = 0.333333 * \log(166) = 0.74$. With an equivalent value, the following scenarios demonstrate adaptability of the proposed GRPN approach. Irrespective of the approach applied, corrective action should be taken on the FMs whose values are greater than the given thresholds. We compare three scenarios of (w_S, w_O, w_D): (H, M, L), (M, L, H), and (L, H, M).

5.2.1. Scenario 1 (w_S^{***}, w_O^{**}, w_D^{*}). This scenario focuses on the factor *S*. It is assumed that the preferences for the SOD weights are $w_S = 0.6$, $w_O = 0.3$, and $w_D = 0.1$, as shown in Table 10. The italic indicates the differentiation of risk identification from the GRPN function to the TRPN function. The values are $144(9 \times 8 \times 2)$, $216(3 \times 9 \times 8)$, $128(2 \times 8 \times 8)$, and $192(8 \times 6 \times 4)$, and the GRPN values are $0.876 = \log(9^{0.6} \times 8^{0.3} \times 2^{0.1})$, $0.663 = \log(3^{0.6} \times 9^{0.3} \times 8^{0.1})$, $0.542 = \log(2^{0.6} \times 8^{0.3} \times 8^{0.1})$, and $0.836 = \log(8^{0.6} \times 6^{0.3} \times 4^{0.1})$, for 3F4a, 3F4b, 3F4c, and 3F4d, respectively. By using the proposed GRPN model, we can identify the risk of failure mode (FM) 3F4a, but the FM is ignored (no corrective actions will be taken on the FM) by the traditional RPN approach. For FM 3F4b, the GRPN approach ignores the failure (without corrective actions); however, the traditional RPN approach identifies the FM.

5.2.2. Scenario 2 (w_S^{**},0020 w_O^{*}, w_D^{***}). This scenario focuses on the factor *D*. It is assumed that the preferences for the SOD weights are $w_S = 0.3$, $w_O = 0.1$, and $w_D = 0.6$, as shown in Table 11. The TRPN values are $144(9 \times 8 \times 2)$, $216(3 \times 9 \times 8)$, $128(2 \times 8 \times 8)$, and $192(8 \times 6 \times 4)$, and the GRPN values are $0.557 = \log(9^{0.3} \times 8^{0.1} \times 2^{0.6})$, $0.780 = \log(3^{0.3} \times 9^{0.1} \times 8^{0.6})$, $0.722 = \log(2^{0.3} \times 8^{0.1} \times 8^{0.6})$, and $0.710 = \log(8^{0.3} \times 6^{0.1} \times 4^{0.6})$, for 3F4a, 3F4b, 3F4c, and 3F4d, respectively. For FM 3F4d, the GRPN approach ignores the FM, but the traditional RPN approach identifies it.

5.2.3. Scenario 3 (w_S^{*}, w_O^{***}, w_D^{**}). This scenario focuses on the factor *O*. It is assumed that the preferences for the SOD weights are $w_S = 0.1$, $w_O = 0.6$, and $w_D = 0.3$, as shown in Table 12. The TRPN values are $144(9 \times 8 \times 2)$, $216(3 \times 9 \times 8)$, $128(2 \times 8 \times 8)$, and $192(8 \times 6 \times 4)$, and the GRPN values are $0.728 = \log(9^{0.1} \times 8^{0.6} \times 2^{0.3})$, $0.891 = \log(3^{0.1} \times 9^{0.6} \times 8^{0.3})$, $0.843 = \log(2^{0.1} \times 8^{0.6} \times 8^{0.3})$, and $0.738 = \log(8^{0.1} \times 6^{0.6} \times 4^{0.3})$, for 3F4a, 3F4b, 3F4c, and 3F4d, respectively. By using the proposed GRPN model, we can identify a risk in the FM 3F4c, but the traditional RPN approach ignores the risk. GRPN ignores the FM 3F4d; however, the traditional RPN approach can identify the FM.

Table 12: Comparison of the TRPN and GRPN test procedures—scenario 3.

FM	Risk factor			TRPN			GRPN		
	S	O	D	Value	Mean value of the acceptable threshold T	Identify risk	Value	Mean value of the acceptable threshold T	Identify risk
3F4a	9	8	2	144	166	N	0.728	0.74	N
3F4b	3	9	8	216	166	Y	0.891	0.74	Y
3F4c	2	8	8	*128*	*166*	*N*	*0.843*	*0.74*	*Y*
3F4d	8	6	4	*192*	*166*	*Y*	*0.738*	*0.74*	*N*

6. Application on E-Healthcare

With the development of information technology, in recent years, it will be an increased focus on healthcare that is user-centered in design in an attempt to meet demand. It also is one of the fastest growing areas of healthcare provision [31]. An integrated framework of e-healthcare service is proposed and it consists of both architecture design and network transmission design [32]. The e-healthcare equipment is used as a tool in the management of long-term conditions in the community to proactively monitor patients and respond promptly to indicators of acute exacerbations. For example, care receivers are trained to operate a device which measures physiological indices such as blood pressure, oxygen saturations and pulse, spirometry, temperature, ECG, and blood glucose readings each day in their home. All devices can be individually programmed to suit the lifestyle and day to day living habits of the person. Generally speaking, the caregivers/care providers take most of the decision-making responsibility and play an important role in healthcare environment which is human intensive task and intention-aware systems that outperform situation-aware systems can eliminate unnecessary humans involved [33]. With the constantly growing information in ubiquitous environment, for example, Internet of Things (IoT), quality and reliability of healthcare sensors has become the new strategic challenge for care providers that aim to capture the whole healthcare information. A data mining-based knowledge mapping approach is proposed to improve the process of acquiring knowledge for healthcare [34]. Even e-healthcare is a convenient approach for improving care access for the care receivers; one of three criteria to evaluate the effectiveness is quality of e-healthcare service [35]. An example of e-healthcare architecture is shown in Figure 7, in which three levels of services can be organized:

(i) infrastructure level [14, 17, 32, 36–39]: endpoint device (vital sign sensor, POC detector), data transmission (Bluetooth, Zegbee, Wi-Fi, 3G+, Internet), middleware (Gateway, data exchange, HL7, LOINC, etc.), care system (call center, e-healthcare IS, HIS, etc.);

(ii) system level [17, 32, 36]: user interface, data processing, data exchange, data repository.

(iii) Data source level [32, 37, 40]: sensor data, HIS, disease IS, clinical interview.

Due to the complexity of e-healthcare service environment, we present a generic modeling of failure risk analysis for the environment, as shown in Figure 8. Define L as the number of levels in e-healthcare service hierarchy, S_l ($l \in L$) as the number of service sets in l-level and S_{ls} as s-set in l-level, and E_{ls} ($l \in L, s \in S_l$) as the number of service elements in the s-set of l-level. Then, we define R_{lse} as the e-element ($e \in E_{ls}$) of e-healthcare service, where R_{lse} ($e \in E_{ls}$) belongs to the service set S_{ls}.

Definition 1. Risk(S) is the risk of the entire e-healthcare service S, where Risk(S) = Risk(S_{11}) and is a function of $R_{lse}(l = 1, s = 1, e \in E_{ls})$, because S_{11} is the first/highest level of the S and the only one service set in the first level.

Definition 2. Risk(S_{ls}), where $l > 1$, is the risk of the service set s in the level l. Moreover, the risk R_{lse} is derived from the service set in lower level $l + 1$. For example, the set $S_{ls} = \{R_{ls1}, R_{ls2}, \ldots, R_{lsE_{ls}}\}$, each of service elements, R_{lse}, is recursively expanded to the respective service sets in next level and there are $S_{l+1,k}, S_{l+1,k+1}, \ldots, S_{l+1,k+E_{ls}}$.

Definition 3. GRPN(R_{lse}) is the value of GRPN function defined in (2). For each R_{lse} in S_{ls}, the value can be expressed as (5), where $w_{S_{lse}}$, $w_{O_{lse}}$, and $w_{D_{lse}}$ are the weights given for the service element e in the service set s of the level l. Consider

$$\mathrm{GRPN}\left(R_{lse}\right) = w_{S_{lse}} \log S_{lse} + w_{O_{lse}} \log O_{lse} + w_{D_{lse}} \log D_{lse}. \tag{5}$$

Property 1 (risk analysis/identification for the entire service S). Risk(S) = $\{R_{lse} \mid \mathrm{GRPN}(R_{lse}) \geq T_{ls}, l = 1, s = 1, e \in E_{ls}\}$, where T_{ls} is the acceptable level of the risk value (GRPN threshold) for the e-healthcare service, as defined in Section 3.1.2.

Property 2 (risk analysis/identification for the service S_{ls}). Risk(S_{ls}) = $\{R_{lse} \mid \mathrm{GRPN}(R_{lse}) \geq T_{ls}, l > 1, e \in T_{ls}\}$, where T_{ls} ($l \in L, s \in S_l$) is the acceptable level of the risk value (GRPN threshold) for the e-healthcare service.

The acceptable level of risk value, T_{ls}, can be all the same or different according to the requirement of risk management policy. Based upon the properties 1 and 2, we can identify the potential risks of e-healthcare service. To illustrate the capability of the proposed adaptable risk identification model, we present a simple example to differentiate the risk of service elements with the hierarchical architecture of e-healthcare environment. Referring to Figure 7, if there are three elements in the infrastructure level: endpoint device (R_{111}), data transmission (R_{112}), and care system (R_{113});

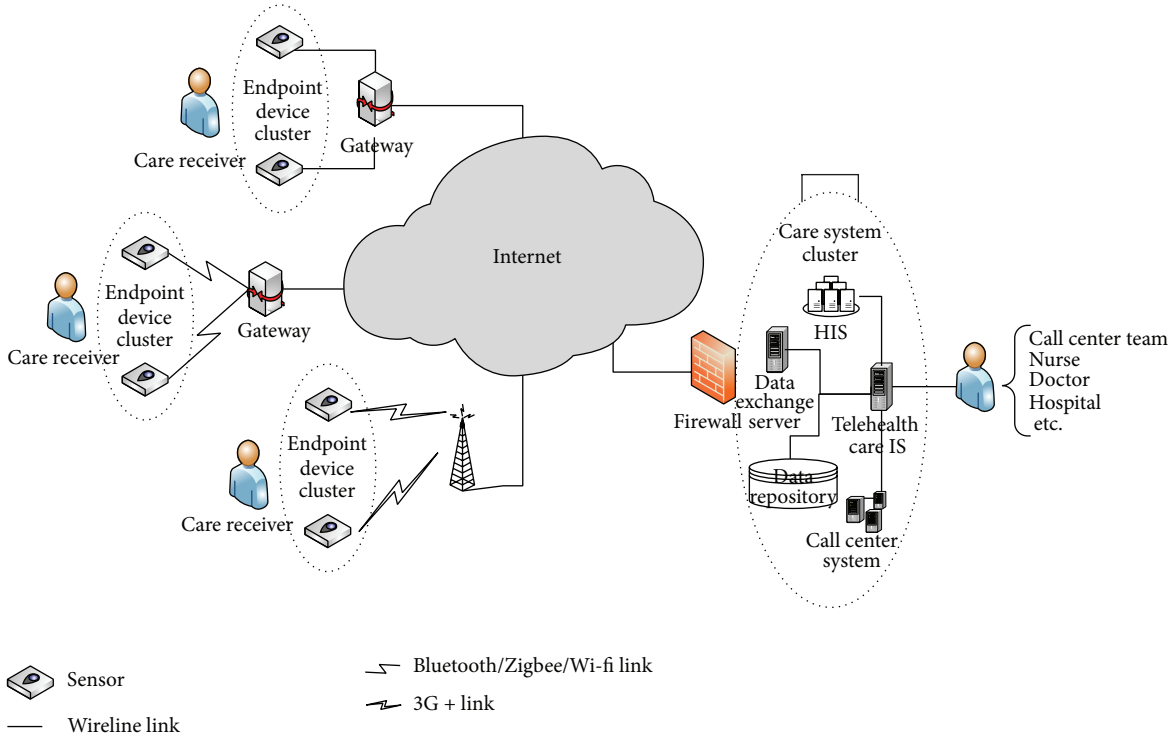


Figure 7: An example of e-healthcare architecture.

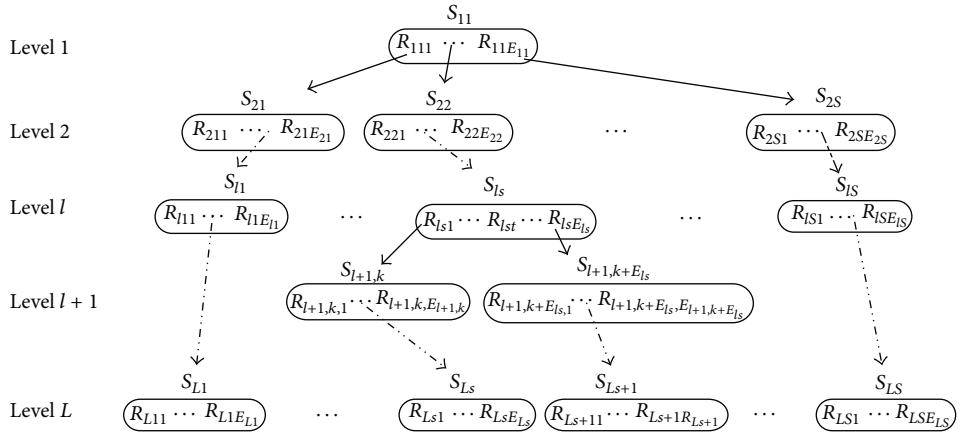


Figure 8: Hierarchy of e-healthcare service architecture.

Table 13: Adaptive risk identification with scenario of risk weight threshold: homo-homo.

Elements in level 1	Risk factor			Risk weight			Risk (S_{ls})		
	S	O	D	w_S	w_O	w_D	GRPN (R_{lse})	T_{ls}	Identify risk
R_{111}	5	8	1	0.6	0.3	0.1	0.69	0.74	No
R_{112}	5	8	4	0.6	0.3	0.1	0.75	0.74	Yes
R_{113}	2	5	8	0.6	0.3	0.1	0.48	0.74	No
R_{114}	2	9	3	0.6	0.3	0.1	0.51	0.74	No
R_{115}	9	4	2	0.6	0.3	0.1	0.78	0.74	Yes
R_{116}	5	9	5	0.6	0.3	0.1	0.78	0.74	Yes
R_{117}	5	2	4	0.6	0.3	0.1	0.57	0.74	No

Table 14: Adaptive risk identification with scenario of risk weight threshold: homo-hetero.

Elements in level 1	Risk factor			Risk weight			Risk (S_{ls})		
	S	O	D	w_S	w_O	w_D	GRPN (R_{lse})	T_{ls}	Identify risk
R_{111}	5	8	1	0.6	0.3	0.1	0.69	0.55	Yes
R_{112}	5	8	4	0.6	0.3	0.1	0.75	0.78	No
R_{113}	2	5	8	0.6	0.3	0.1	0.48	0.50	No
R_{114}	2	9	3	0.6	0.3	0.1	0.51	0.62	No
R_{115}	9	4	2	0.6	0.3	0.1	0.78	0.75	Yes
R_{116}	5	9	5	0.6	0.3	0.1	0.78	0.61	Yes
R_{117}	5	2	4	0.6	0.3	0.1	0.57	0.55	Yes

Table 15: Adaptive risk identification with scenario of risk weight threshold: hetero-homo.

Elements in level 1	Risk factor			Risk weight			Risk (S_{ls})		
	S	O	D	w_S	w_O	w_D	GRPN (R_{lse})	T_{ls}	Identify risk
R_{111}	5	8	1	0.6	0.3	0.1	0.69	0.74	No
R_{112}	5	8	4	0.3	0.6	0.1	0.81	0.74	Yes
R_{113}	2	5	8	0.3	0.1	0.6	0.70	0.74	No
R_{114}	2	9	3	0.6	0.1	0.3	0.42	0.74	No
R_{115}	9	4	2	0.6	0.1	0.3	0.72	0.74	No
R_{116}	5	9	5	0.3	0.6	0.1	0.85	0.74	Yes
R_{117}	5	2	4	0.6	0.3	0.1	0.57	0.74	No

three elements in the system level: user interface (R_{114}), data processing (R_{115}), and data exchange (R_{116}); one element in the data source level: sensor data (R_{117}), each of elements can be further recursively divided into respective services (S_{ls}, $l > 1$) in higher levels, in which potential risks are to be identified.

In this example, we only focus on seven elements of service S_{11} in level 1; they are $R_{111}, R_{112}, R_{113}, R_{114}, R_{115}, R_{116}$, and R_{117}. Moreover, model adaptability is shown with parameter combination of both risk weight ($w_{S_{lse}}$, $w_{O_{lse}}$, $w_{D_{lse}}$) and acceptable risk threshold (T_{ls}). Each of them is further separated into homogeneous (homo) and heterogeneous (hetero) cases between seven elements ($R_{111} \sim R_{117}$). The case homo means values assigned to the parameter are all the same, while the case hetero means values assigned to the parameter are different. Accordingly, there are four scenarios of risk weight-threshold combination: homo-homo, home-hetero, hetero-home, and hetero-hetero; they are illustrated in Tables 13, 14, 15, and 16, respectively. From the results of four scenarios analysis, only two elements (R_{114} and R_{116}) get identical suggestion, without risk identification for R_{114} and with risk identification for R_{116}. The proposed adaptive approach is capable of differentiating the other five elements with regard to different risk preferences.

7. Conclusion

FMEA has long been used to evaluate the safety and reliability of products and services in a number of industries. The traditional FMEA model uses the RPN number to prioritize failure modes. Since the three indices used to calculate the RPN are ordinal scale variables, the product of the three ordinal numbers cannot reflect the actual costs incurred by failures. As a result, the traditional model cannot provide precise information about failure risks, such as the probabilities of the severity, occurrence, and detectability factors. In addition, it is difficult to apply the traditional FMEA to various risk preferences. To overcome these limitations, we propose a generic RPN model called GRPN-based FMEA, which allows us to evaluate the risk factors and their relative weights in a linear manner rather than in a nonlinear relationship. The model uses the logarithm function to assess the severity, occurrence, and detectability factors. It also represents the risk value (GRPN) as a risk factor and a risk weight in a linear relationship, instead of the nonlinear approach used in the traditional RPN formulation. The result shows that the proposed model outperforms the TRPN model. The proposed model provides a practical, effective, and adaptive method for risk evaluation in FMEA. In particular, the defined GRPN offers a new way to prioritize failure modes in FMEA. The different risk preferences considered in the healthcare example show that the modified FMEA model can take account of the various risk factors and prioritize failure modes more accurately. Moreover, with the constantly increasing requirement of e-healthcare service, we also propose a generic modeling of failure risk analysis for the service. The model is capable of adaptively identifying the failure risks in a hierarchical service architecture.

This paper proposes a generic RPN (GRPN) function-based FMEA model for risk analysis that assigns a weight (risk weight) to each risk factor so that the weights represent individual organization/department/process preferences for the factors. To validate the proposed model, the risk factors are randomly generated with both uniform and normal distributions via a simulation process. We also conduct sensitivity

Table 16: Adaptive risk identification with scenario of risk weight threshold: hetero-hetero.

Elements in level 1	Risk factor			Risk weight			Risk (S_{ls})		
	S	O	D	w_S	w_O	w_D	GRPN (R_{lse})	T_{ls}	Identify risk
R_{111}	5	8	1	0.6	0.3	0.1	0.69	0.55	Yes
R_{112}	5	8	4	0.3	0.6	0.1	0.81	0.78	Yes
R_{113}	2	5	8	0.3	0.1	0.6	0.70	0.50	Yes
R_{114}	2	9	3	0.6	0.1	0.3	0.42	0.62	No
R_{115}	9	4	2	0.6	0.1	0.3	0.72	0.75	No
R_{116}	5	9	5	0.3	0.6	0.1	0.85	0.61	Yes
R_{117}	5	2	4	0.6	0.3	0.1	0.57	0.55	Yes

analysis on correlation and regression to compare it to the traditional (TRPN-based) approach. To understand how the proposed model works, we use a healthcare example as a potential application of the proposed GRPN-based FMEA model. An illustrated example of Down syndrome test is given, and the computation of GRPNs is explained in detail.

We introduce two application modes based on experience and preference. The experience-based mode allows the user to choose a risk factor combination arbitrarily. This mode can be used in different organizations, departments, or processes, by estimating historical data of failure modes for each of the risk factors (SOD). Under the preference-based mode, we assume that the organization always defines a risk management policy to identify failure modes. Therefore, the weight combination is determined by the policy, for example, (H, L, M). After selecting the weight combination, we set the GRPN threshold to determine if the failure modes exist. However, this paper only discusses two of various stochastic models for the risk factor distribution, that is, uniform and normal. In fact, there are numerous distributions in real world. More realistically, future work can pay more attention to testing and validation for various distributions.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This paper is sponsored by the National Science Council of Taiwan (NSC 98-2410-H-227-004).

References

[1] R. Y. Shtykh and Q. Jin, "A human-centric integrated approach to web information search and sharing," *Human-Centric Computing and Information Sciences*, vol. 1, p. 2, 2011.

[2] N. Y. Yen and S. Y. F. Kuo, "An intergrated approach for internet resources mining and searching," *Journal of Convergence*, vol. 3, no. 2, pp. 37–44, 2012.

[3] D. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*, John Wiley & Sons, New York, NY, USA, 2009.

[4] ISO, *ISO/IEC Guide 73:2009 Risk Management-Vocabulary*, 2009.

[5] H. VanCott, "Human errors: their causes and reduction," in *Human Error in MEdicine*, M. S. Bogner, Ed., pp. 82–98, Lawrence Erlbaum Associates, Hillsdale, NJ, USA, 1994.

[6] S. Ternov, "The human side of medical mistakes," in *Error Reduction in Health Care: A Systems Approach to Improving Patient Safty*, P. L. Spath, Ed., pp. 97–138, AHA Press, Chicago, Ill, USA, 2002.

[7] American Hospital Association, *Hospital Statistics*, American Hospital Association, Chicago, Ill, USA, 1999.

[8] Centers for Disease Control and Prevention-National Center for Health Statistics, "Births and deaths: preliminary data for 1998," *National Vital Statistics Reports*, vol. 47, no. 25, p. 6, 1999.

[9] T. S. Lesar, B. M. Lomaestro, and H. Pohl, "Medication-prescribing errors in a teaching hospital: A 9-year experience," *Archives of Internal Medicine*, vol. 157, no. 14, pp. 1569–1576, 1997.

[10] E. J. Thomas, D. M. Studdert, H. R. Burstin et al., "Incidence and types of adverse events and negligent care in Utah and Colorado," *Medical Care*, vol. 38, no. 3, pp. 261–271, 2000.

[11] L. T. Kohn, J. M. Corrigan, and M. S. Donaldson, Eds., *To Err Is Human: Building a Safer Health System*, Institute of Medicine, National Academy Press, Washington, DC, USA, 2000.

[12] BS5760:Part5, *Reliability of Systems, Equipment and Components. Guide to Failure Modes, Effects and Criticality Analysis*, 1991.

[13] D. Werth, A. Emrich, and A. Chapko, "Prosumerization of mobile service provision: a conceptual approach," *International Journal of Web Portals*, vol. 3, no. 4, pp. 44–55, 2011.

[14] J. K.-Y. Ng, "Ubiquitous healthcare: healthcare systems and applications enabled by mobile and wireless technologies," *Journal of Convergence*, vol. 3, no. 2, pp. 15–20, 2012.

[15] A. K. Dey and D. Estrin, "Perspectives on pervasive health from some of the field's leading researchers," *IEEE Pervasive Computing*, vol. 10, no. 2, pp. 4–7, 2011.

[16] W. Kaiser and M. Sarrafzadeh, "Introduction to special issue on wireless health," *Transactions on Embedded Computing Systems*, vol. 10, no. 1, article 10, 2010.

[17] S. Deng, C. Youn, Q. Liu, H. Y. Kim, T. Yu, and Y. H. Kim, "Policy adjuster-driven grid workflow management for collaborative heart disease identification system," *Journal of Information Processing Systems*, vol. 4, no. 3, pp. 103–112, 2008.

[18] M. Lee, J.-W. Lee, K.-A. Kim, and S. S. Park, "Evaluating service description to guarantee quality of U-service ontology," *Journal of Information Processing Systems*, vol. 7, no. 2, pp. 287–298, 2011.

[19] J. C. Augusto, V. Callaghan, D. Cook, A. Kameas, and I. Satoh, "Intelligent environments: a manifesto," *Human-Centric Computing and Information Sciences*, vol. 3, p. 12, 2013.

[20] AIAG, A.I.A.G., *Potential Failure Mode and Effects Analysis (FMEA) Reference Manual*, AIAG, Southfield, Mich, USA, 2nd edition, 1995.

[21] JCAHO, J.C.o.A.o.H.O., Hospital accreditation standards, in Oak Brook Terrace (IL): Joint Commission Resources 2006. pp. 255-256, 261–277.

[22] P. L. Spath, "Using failure mode and effects analysis to improve patient safety," *AORN Journal*, vol. 78, no. 1, pp. 16–41, 2003.

[23] M. Ben-Daya and A. Raouf, "A revised failure mode and effects analysis model," *International Journal of Quality & Reliability Management*, vol. 13, no. 1, pp. 43–47, 1996.

[24] J. B. Bowles, "An assessment of RPN prioritization in a failure modes effects and criticality analysis," *Journal of the IEST*, vol. 47, pp. 51–56, 2004.

[25] M. Braglia, M. Frosolini, and R. Montanari, "Fuzzy TOPSIS approach for failure mode, effects and criticality analysis," *Quality & Reliability Engineering International*, vol. 19, no. 5, pp. 425–443, 2003.

[26] C.-L. Chang, P.-H. Liu, and C.-C. Wei, "Failure mode and effects analysis using grey theory," *Integrated Manufacturing Systems*, vol. 12, no. 3, pp. 211–216, 2001.

[27] W. Gilchrist, "Modelling failure modes and effects analysis," *International Journal of Quality & Reliability Management*, vol. 10, no. 5, pp. 16–23, 1993.

[28] A. Pillay and J. Wang, "Modified failure mode and effects analysis using approximate reasoning," *Reliability Engineering and System Safety*, vol. 79, no. 1, pp. 69–85, 2003.

[29] N. R. Sankar and B. S. Prabhu, "Modified approach for prioritization of failures in a system failure mode and effects analysis," *International Journal of Quality & Reliability Management*, vol. 18, no. 3, pp. 324–335, 2001.

[30] http://www.palisade.com/.

[31] C. Ruggiero, R. Sacile, and M. Giacomini, "Home telecare," *Journal of Telemedicine and Telecare*, vol. 5, no. 1, pp. 11–17, 1999.

[32] L.-C. Chen, C. W. Chen, Y. C. Weng et al., "An information technology framework for strengthening telehealthcare service delivery," *Telemedicine Journal and e-Health*, vol. 18, no. 8, pp. 596–603, 2012.

[33] N. Howard and E. Cambria, "Intention awareness: improving upon situation awareness in humancentric environments," *Human-Centric Computing and Information Sciences*, vol. 3, no. 9, 2013.

[34] M. Brahami, B. Atmani, and N. Matta, "Dynamic knowledge mapping guided by data mining: application on healthcare," *Journal of Information Processing Systems*, vol. 9, no. 1, pp. 1–30, 2013.

[35] L. Prinz, M. Cramer, and A. Englund, "Telehealth: a policy analysis for quality, impact on patient outcomes, and political feasibility," *Nursing Outlook*, vol. 56, no. 4, pp. 152–158, 2008.

[36] M. S. H. Talpur, "The appliance pervasive of internet of things in healthcare systems," *International Journal of Computer Science Issues*, vol. 10, no. 1, pp. 419–424, 2013.

[37] J. Basilakis, N. H. Lovell, S. J. Redmond, and B. G. Celler, "Design of a decision-support architecture for management of remotely monitored patients," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 5, pp. 1216–1226, 2010.

[38] A. Kailas and M. A. Ingram, "Wireless communications technology in telehealth systems," in *Proceedings of the 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless (VITAE '09)*, pp. 926–930, May 2009.

[39] R. D. Berndt, M. C. Takenga, S. Kuehn, P. Preik, G. Sommer, and S. Berndt, "SaaS-platform for mobile health applications," in *Proceedings of the 9th International Multi-Conference on Systems, Signals and Devices (SSD '12)*, pp. 1–4, 2012.

[40] A. Kuusik, E. Reilent, I. Lõõbas, and M. Parve, "Software architecture for modern telehome care systems," in *Proceedings of the 6th International Conference on Networked Computing (INC '10)*, pp. 326–331, May 2010.