Modeling Medical System Threats with Conditional Probabilities using Multiple-Valued Logic Decision Diagrams

Theodore W. Manikas
Department of Computer Science and Engineering
Southern Methodist University
Dallas, Texas, USA
manikas@lyle.smu.edu

David Y. Feinstein
Innoventions, Inc.
10425 Bissonnet Street
Houston, Texas, USA
david@innoventions.com

Mitchell A. Thornton
Department of Computer Science and Engineering
Southern Methodist University
Dallas, Texas, USA
mitch@lyle.smu.edu

***Abstract*—Design for medical system reliability has become an area of increasing importance. Medical system threats, which include system failures as well as malicious attacks, often have interdependent events that can adversely affect system operation. To address these problems, we build upon our previous threat cataloging methodology such that a large number of interdependent threats can be efficiently cataloged and analyzed for common features. Our approach utilizes Multiple-Valued Logic for describing the state of a large system and a multiple-valued decision diagram (MDD) for the threat catalog and analysis.**

Keywords—medical system analysis, threat cataloging, MDD, threat probability analysis.

I. INTRODUCTION

The Institute of Medicine shocked the medical community in 2000 when it reported that more than two million serious medical errors occur every year. This put the goal of patient safety Quality Improvement (QI) at the top priority of the health care industry [20]. As a result, Probabilistic Risk Assessment (PRA) techniques that use fault trees to model the combination of multiple failures that lead to a specific adverse outcome were adapted from aviation and other industrial fault tolerant disciplines [21]. Since adverse outcomes in patient safety are the result of a combination of machine and human errors, a PRA variant technique called Sociotechnical Probabilistic Risk Assessment (ST-PRA) has been promoted [1].

Recent events have demonstrated our vulnerability to system threats, both natural and man-made. Therefore, more emphasis has been placed on design for security, security assessment, disaster recovery, and disaster tolerance in addition to ongoing efforts in the established area of fault tolerance. While the term "threats" is commonly used to indicate areas of possible system security violations, in this paper we expand the definition of threats to include any item that has the potential to adversely affect system operation, such as faults. For medical systems, health care delivery relies upon a complex series of interactions between medical providers, equipment, and patients [1]. Specific medical system threat examples include component failures [2], misdiagnosis of the patient's symptoms, wrong treatment strategy selection, and errors in administration of the treatment [3]. Therefore, it is necessary to catalog and characterize anticipated system threats in order to formulate appropriate countermeasures during the design and implementation of a disaster tolerant system.

Disaster tolerant systems differ from fault tolerant systems since they are designed with the assumption that failures can occur due to threats that can result in either single or massive numbers of individual faults. Traditional fault tolerance system design usually relies on fault models that represent single points of failure for the entire system. In contrast, a disaster-tolerant system can still function with some degree of normality even in the presence of multiple or cascading faults [4, 5].

Various tree-like data structures have been developed to represent possible system threats, such as fault trees [6] or attack trees [7]. Specific medical applications of these tree structures include assessment of radiation treatment systems [3] and patient safety risks [1]. However, these structures are based on a binary model whereby a system either operates in a fully functional or a complete failure mode. The binary model limits the effectiveness of how such trees can be used to represent threats in a disaster tolerant system.

Modeling different operational modes other than the binary case of failure or normal operation are critical in analyzing large systems in the presence of threats. For example, radiation treatment systems have many complex interactions between their components, with multiple operational modes [3]. In order to effectively catalog these system threats, it is necessary to determine the probabilities of these threats based on various system stimuli, including input conditions and their probabilities.

As part of our preliminary research on large-scale system threat assessment, we developed threat tree models [8]. Threat trees are a superset of fault and attack trees since they are based on multiple-valued (MV) or radix-*p* valued algebras over a finite and discrete set of values [9]. The additional logic states allow for more complicated interactions to be modeled. In

0195-623X/12 $26.00 © 2012 IEEE
DOI 10.1109/ISMVL.2012.29

particular, these additional states can represent partial failures or degraded performance in a system, which are critical in analyzing large systems in the presence of threats.

We have also applied multiple-valued logic decision diagrams to threat trees to determine large-scale system threat probabilities [10]. Our initial approach assumed that system components operated independently. However, this assumption does not hold for all systems. In particular, medical systems often have many interdependent components, which means that the conditional probabilities of system threats must also be considered [1]. Therefore, we have expanded our initial threat assessment approach to address this concern.

The structure of this paper is the following: First, background information on decision diagram models is provided. Next, an approach is presented using decision diagram models to determine conditional system threat probabilities. Finally, a medical delivery system example is used to illustrate these concepts.

II. Decision Diagrams

A common structure for fault representation is the decision diagram, which is a rooted directed acyclic graph (DAG) that can be used to represent large switching functions in an efficient manner. Decision diagrams are well-suited for compact representation of a large number of threats and due to their canonical structure, efficient algorithms are formulated that analyze threats and identify those that pose the greatest threat to the system. For binary-valued logic, the binary decision diagram (BDD) is a well-known structure [11] that has been applied to many areas including the representation of fault trees [12-17]. Furthermore, efficient software is readily available to manipulate BDDs and a variety of heuristics and strategies have been adapted for use with fault trees [12, 13, 15]. Fig. 1 shows a BDD for the function *f(A,B) = A and B*.

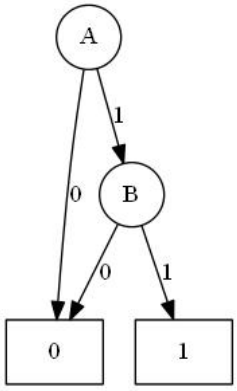

Figure 1. BDD for AND function.

In the case of *Multiple-Valued Logic* (MVL), an extension to the BDD construct has been developed and implemented called the *Multiple-Valued Decision Diagram* (MDD). Consider a totally-specified *p*-valued function with *n* inputs, $f(x_0, x_1, \ldots, x_n)$ where each dependent variable $x_i \in \{0,1,\cdots p-1\}$. $f(x)$ can be efficiently represented by an MDD. Similar to BDD, the MDD is also a DAG and it contains a maximum of *p* terminal nodes, where each terminal node is labeled by a distinct logic value in the range [0, *p*-1]. Every non-terminal node is labeled by an input variable, and has *p* outgoing edges, where each edge corresponds to each logic value. MDD can be minimized using various techniques that were developed for BDD, thus allowing the representation of exceptionally large number of such functions [18]. Fig. 2 shows an example of an MDD for the radix-3 function *f = min(A,B)*, while Table I shows the corresponding truth table.

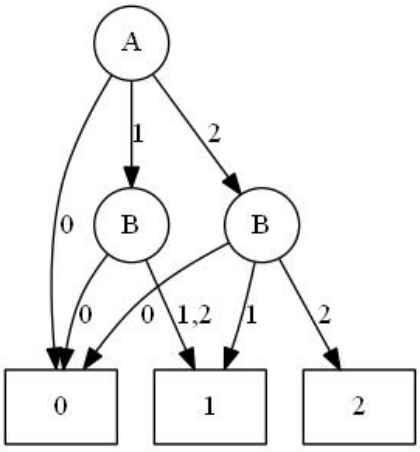

Figure 2. MDD for radix-3 MIN function.

TABLE I. Truth table for MDD.

A	B	f
0	X	0
1	0	0
1	1	1
1	2	1
2	0	0
2	1	1
2	2	2

III. Application of Conditional Probability

After developing a decision diagram to model system behavior, the next step is to add information to this diagram to help determine the probabilities of system output events, based on the given probabilities of system input events.

From general probability theory [19], the conditional probability of event B given the occurrence of event A is given in (1). For a binary system, P(A) = probability that A = 1, while P(A') = probability that A = 0. Assuming that conditional probability applies to inputs A and B of the BDD in Fig. 1, we can add conditional probabilities to the edges as shown in Fig. 3.

$$P(B|A) = \frac{P(B \cap A)}{P(A)} \quad (1)$$

Output $f = 1$ requires both $A = 1$ and B = 1. The probability of $f = 1$ is $P(A \cap B) = P(A)P(B|A)$ from (1).

Output $f = 0$ if either of the following conditions is true:

1. A = 0, with probability P(A')
2. A = 1 and B = 0, with probability $P(A \cap B') = P(A)P(B'|A)$

Applying the Total Probability Rule [19], we get the probability of $f = 0$ in (2). Therefore, the output probability for $f = 0$ is the sum of the probabilities for each possible condition that produces $f = 0$.

$$P(f = 0) = P(A') + P(A \cap B') = P(A') + P(A)P(B'|A) \quad (2)$$

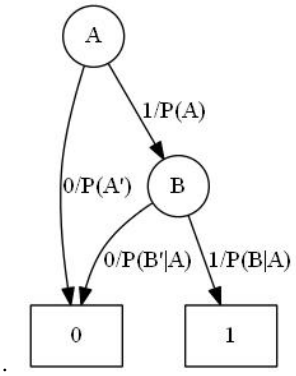

Figure 3. BDD for AND function with conditional probabilities.

A. Expansion to MDD's

Traditional probability theory assumes radix-2 systems: either an event X is true (X=1) or false (X=0). For general radix-p systems, we develop the notation X_j, which indicates that event X has state j ($j \in [0, \cdots, p-1]$). Therefore, we can modify the conditional probability equation of (1) to handle radix-p events as shown in (3).

$$P(B_j|A_k) = \frac{P(B_j \cap A_k)}{P(A_k)} \quad (3)$$
$$where\ j,k \in [0, \cdots, p-1]$$

Given function f(A,B), what are the output probabilities of function f? For our radix-3 example of Fig. 2, we have $P(f_j)$ = probability that output $f = j$, where $j \in [0,1,2]$. Output $f = 2$ only if both inputs A and B are 2. More specifically, we have the output probability shown in (4).

$$P(f_2) = P(A_2 \cap B_2) = P(A_2)P(B_2|A_2) \quad (4)$$

Output $f = 1$ if any of the following conditions are true:

1. A = 1 and B = 1, with probability $P(A_1 \cap B_1) = P(A_1)P(B_1|A_1)$
2. A = 1 and B = 2, with probability $P(A_1 \cap B_2) = P(A_1)P(B_2|A_1)$
3. A = 2 and B = 1, with probability $P(A_2 \cap B_1) = P(A_2)P(B_1|A_2)$

Applying the Total Probability Rule as described earlier, we obtain (5). Therefore, the output probability for $f = 1$ is the sum of the probabilities for each possible condition that produces $f = 1$.

$$P(f_1) = P(A_1 \cap B_1) + P(A_1 \cap B_2) + P(A_2 \cap B_1) = P(A_1)P(B_1|A_1) + P(A_1)P(B_2|A_1) + P(A_2)P(B_1|A_2) \quad (5)$$

Output $f = 0$ if any of the following conditions are true:

1. A = 0, with probability P(A0)
2. A = 1 and B = 0, with probability $P(A_1 \cap B_0) = P(A_1)P(B_0|A_1)$
3. A = 2 and B = 0, with probability $P(A_2 \cap B_0) = P(A_2)P(B_0|A_2)$

Using the Total Probability Rule, we obtain the output probability for $f = 0$ using (6).

$$P(f_0) = P(A_0) + P(A_1 \cap B_0) + P(A_2 \cap B_0) = P(A_0) + P(A_1)P(B_0|A_1) + P(A_2)P(B_0|A_2) \quad (6)$$

Fig. 4 shows the probabilities applied to the associated edges of the example of Fig. 2. Note that $P(B_{1,2}) = P(B_1) + P(B_2)$. The output probabilities are calculated by traversing the MDD using a depth-first search, and adding the total output probability components.

If events A and B are independent, then $P(B_j \cap A_k) = P(B_j)P(A_k)$. The conditional probability equation reduces to $P(B_j|A_k) = P(B_j)$. This becomes the case described in our previous paper [10].

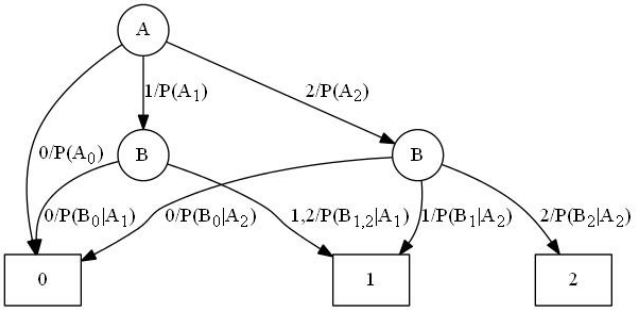

Figure 4. Probabilities applied to MDD of Fig. 2.

IV. Application Example

We demonstrate the techniques of this paper using a patient safety example that assesses the risk of medication delivery to a patient within the hospital environment. It is interesting to note that ST-PRA analysis of medication delivery has been extensively published in the medical literature, using a binary outcome of the process indicating success or failure [1, 22]. We extend the outcome of the medication delivery process to radix-3 with the following system states: 2 – successful medication delivery; 1 – benign (or partial) failure; and 0 – harmful failure. We assume, of course, that once the medical team identifies a benign failure outcome, they will repeat the process to insure proper patient care [21].

We model the medication delivery process as being composed of two sub-processes A and P, as shown in Fig. 5. Sub-process A models the medication administration process, and it takes into accounts faults in the medication pump equipment, the pump monitoring/alarm system and the nursing team in charge of the process. Sub-process A is adapted from a binary ST-PRA example discussed in [1]. Sub-process P models the medication prescription process which takes into accounts faults in the associated medical equipment used for patient data and medical diagnostic equipment, the nursing team that access the medical data and perform medical test, and the doctor who diagnoses the patient illness and prescribe the medication. Sub-process P follows an example in [22] with the addition of the medical diagnostic equipment and electronic medical records.

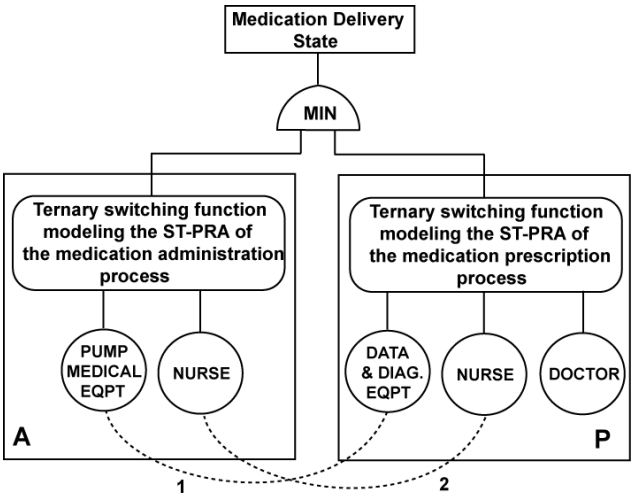

Figure 5. Ternary Threat Tree Analysis of Medication Delivery.

Fig. 5 illustrates the need for conditional probabilities analysis due to the apparent dependencies between sub-processes A and P. Line 1 relates to the dependencies of faults occurring in the medication pump equipment and the electronic medical data computers and the medical diagnostic equipment. With today's online sophistication, the pump equipment may be subject to the same cyber threat as the computers performing the medical tests and retaining the medical data. In addition, the same technician may be in charge of repairing and maintaining all the medical equipment in the patient vicinity. Line 2 relates to the dependencies through the nursing teams. The same potentially over extended and tired nurse might be involved in the medical tests that helps determine the proper prescription as well as in the actual medication administration sub-process. Alternatively, inadequate nursing procedures in a given hospital may correlate failures even if there are different nursing teams involved in the two sub-processes.

The total medication delivery condition C is found by C = min(P,A). All sub-processes are radix-3, with states and probabilities as shown in Table II. We chose probabilities for this example that are useful in demonstrating our proposed technique rather than attempting to use strictly realistic medical values. The columns in Table II represent probability values for the condition of the prescription sub process P, while the rows represent probability values for the medication administration sub-process A. For row j and column k, the number in the table cell is the probability of the intersection of input A = j and P = k. For instance, $P(A_0 \cap P_2) = 0.005$. This value is the probability that the medication administration sub-process is failing, while the medication prescription sub-process P is successful. The "total" row indicates the independent probability values of P_k, while the "total" column indicates the independent probability values of A_j. For instance, $P(A_0) = 0.045$ and $P(P_2) = 0.9$.

Since the total medication delivery condition C = min(P,A), we can use the MDD of Fig. 4, substituting variable P (prescription) for A and variable A (administration) for B. If P = 0 (wrong and harmful prescription), then C = 0, regardless of the value of A. From Table II, $P(P_0) = 0.04$. Similarly, $P(P_1) = 0.16$ and $P(P_2) = 0.9$.

TABLE II. PROBABILITES AND STATES FOR MEDICATION DELIVERY SYSTEM.

		P			
		0	1	2	total
A	0	0.025	0.015	0.005	0.045
	1	0.01	0.03	0.045	0.085
	2	0.005	0.015	0.85	0.87
	total	0.04	0.06	0.9	1

Using our notation, $P(A_0|P_1)$ is the conditional probability that sub-process A is at state 0 (harmful failure), given that system P is at state 1 (benign failure). From Table II, we have the following probabilities as shown in (7) – (9).

$$P(A_0 \cap P_1) = 0.015 \tag{7}$$

$$P(P_1) = 0.06 \tag{8}$$

$$P(A_0|P_1) = \frac{P(A_0 \cap P_1)}{P(P_1)} = \frac{0.015}{0.06} = 0.25 \tag{9}$$

Developing the other conditional probabilities, we obtain the MDD shown in Fig. 6.

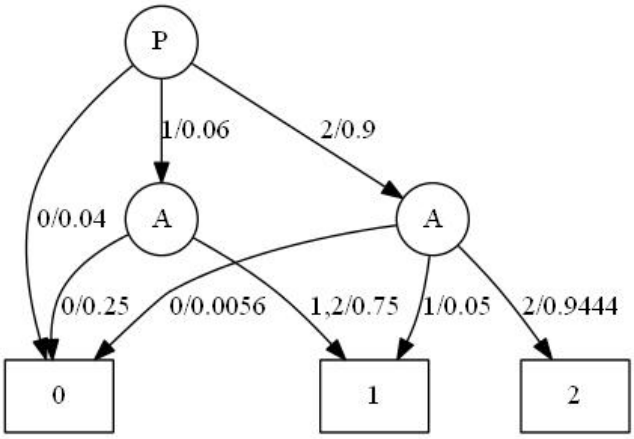

Figure 6. MDD for the Medication Delivery Example.

Using the approach described in Section III, the output probabilities are calculated as shown in (10) – (12):

$$P(C_0) = 0.04 + (0.06)(0.25) + (0.9)(0.0056) = 0.06 \quad (10)$$

$$P(C_1) = (0.06)(0.75) + (0.9)(0.05) = 0.09 \quad (11)$$

$$P(C_2) = (0.9)(0.9444) = 0.85 \quad (12)$$

Now, if we assume that sub-process A is *independent* of sub-process P, then $P(A_j|P_k) = P(A_j)$. From Table II, $P(A_0) = 0.045$, $P(A_1) = 0.085$, and $P(A_2) = 0.87$. This results in the modified MDD shown in Fig. 7.

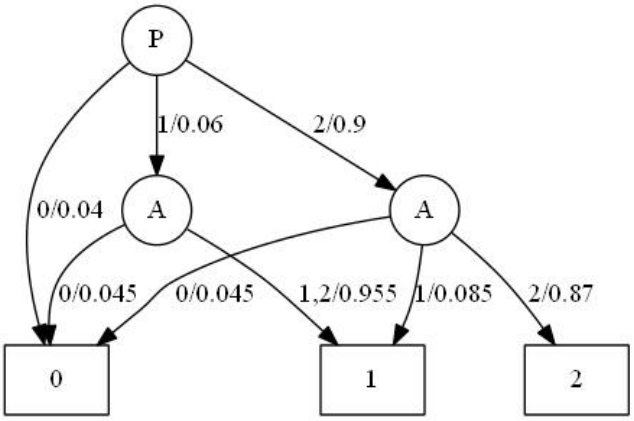

Figure 7. MDD for the Medication Delivery System, assuming independent probabilities.

Next, the output probabilities are calculated as shown in (13) – (15):

$$P(C_0) = 0.04 + (0.06)(0.045) + (0.9)(0.045) = 0.08 \quad (13)$$

$$P(C_1) = (0.06)(0.955) + (0.9)(0.085) = 0.13 \quad (14)$$

$$P(C_2) = (0.9)(0.87) = 0.78 \quad (15)$$

Note the differences in output probabilities, depending on whether the input probabilities are independent or conditional. Therefore, it is important to consider the interdependence of input conditions to obtain a more accurate model of system operation when performing threat analysis.

V. CONCLUSION

The challenge of system threat determination in medical systems is crucial for patient care quality improvement. In this work we have shown how to model system threat probabilities using edge weights on MDD's, with emphasis on conditional probabilities. Our approach allows efficient determination of overall system state probabilities and can accommodate complex systems with the efficient scalability of modern MDD packages.

We have demonstrated the importance of accounting for conditional probabilities and lay out the mechanism to take them into account in conjunction with the MDD analysis of other systems. While we have focused on medical system threat analysis, the framework discussed in this paper can be further applied to general large system risk analysis which is useful in the determination of the initial system element probability values.

We also plan to investigate the use of mixed-radix MDDs to model medical threats that cannot be explored with a fixed radix.

VI. ACKNOWLEDGMENT

This research was partially supported by the U.S. Office of Naval Research (ONR) project N000140910784.

REFERENCES

[1] D.A. Marx and A. D. Slonim, "Assessing patient safety risk before the injury occurs: an introduction to socitechnical probabilistic risk modeling in health care", *Qua.l Safety Health Care 2003*; 12(Suppl II): ii33-ii38.

[2] M. Jiang, K. Herzog, T. Pepin, and M. D. Baca, "A quantitative approach for medical device Health Hazard Analysis," in *2011 Proc. Annu. Reliability and Maintainability Symp. (RAMS)*, 2011, pp. 1-5.

[3] E. Ekaette, D. L. Cooke, R. C. Lee, P. Craighead, and S. Iftody, "Probabilistic fault tree analysis of a radiation treatment system," *Risk analysis*, vol. 27, no. 6, pp. 1395-1410, Dec. 2007.

[4] M. A. Harper, C. M. Lawler, and M. A. Thornton, "IT Application Downtime, Executive Visibility and Disaster Tolerant Computing," in *Proc. Int. Conf. on Cybernetics and Information Technologies, Systems and Applications (CITSA 2005)*, and *Int. Conf. on Information Systems Analysis and Synthesis (ISAS)*, 2005, pp. 165-170.

[5] S. A. Szygenda and M. A. Thornton, "Disaster Tolerant Computing and Communications," in *Proc. Int. Conf. on Cybernetics and Information Technologies, Systems and Applications (CITSA 2005)*, and *Int. Conf. on Information Systems Analysis and Synthesis (ISAS)*, 2005, pp. 171-173.

[6] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasi, "Fault tree handbook," U.S. Nuclear Regulatory Commission, NUREG-0492, Jan. 1981.

[7] B. Schneier, "Attack trees," *Dr. Dobb's Journal*, vol. 24, no. 12, pp. 21 - 21, 1999.

[8] P. Ongsakorn, K. Turney, M. Thornton, S. Nair, S. Szygenda, and T. Manikas, "Cyber threat trees for large system threat cataloging and analysis," in *2010 4th Annu. IEEE Systems Conf.*, 2010, pp. 610 -615.

[9] D. M. Miller and M. A. Thornton, *Multiple Valued Logic: Concepts and Representations*. Morgan & Claypool Publishers, 2007.

[10] T. W. Manikas, M. A. Thornton, and D. Y. Feinstein, "Using Multiple-Valued Logic Decision Diagrams to Model System Threat Probabilities," in *41st IEEE Int. Symp. on Multiple-Valued Logic (ISMVL)*, 2011, pp. 263 -267.

[11] R. E. Bryant, "Graph-Based Algorithms for Boolean Function Manipulation," *IEEE Trans. Comput.*, vol. 35, no. 8, pp. 677 -691, Aug. 1986.

[12] L. M. Bartlett and J. D. Andrews, "Choosing a heuristic for the 'fault tree to binary decision diagram' conversion, using neural networks," *IEEE Trans. Reliab*., vol. 51, no. 3, pp. 344 - 349, Sep. 2002.

[13] K. A. Reay and J. D. Andrews, "A fault tree analysis strategy using binary decision diagrams," *Rel. Eng. and System Safety*, vol. 78, no. 1, pp. 45-56, 2002.

[14] R. Remenyte and J. D. Andrews, "A simple component connection approach for fault tree conversion to binary decision diagram," in *Proc. - First Int. Conf. on Availability, Reliability and Security, ARES 2006*, Vienna, Austria, 2006, vol. 2006, pp. 449 - 456.

[15] A. B. Rauzy, J. Gauthier, and X. Leduc, "Assessment of large automatically generated fault trees by means of binary decision diagrams," *Proc. of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 221, no. 2, pp. 95 -105, Jun. 2007.

[16] L. Xing and Y. Dai, "A New Decision-Diagram- Based Method for Efficient Analysis on Multistate Systems," IEEE *Trans. Dependable and Secure Computing*, vol. 6, no. 3, pp. 161 -174, Sep. 2009.

[17] O. Yevkin, "Truncation approach with the decomposition method for system reliability analysis," in *2009 - Annu. Reliability and Maintainability Symp., RAMS 2009,* Fort Worth, TX, United states, 2009, pp. 430-435.

[18] D. M. Miller and R. Drechsler, "Implementing a multiple-valued decision diagram package," in *Proc. 28th IEEE Int. Symp. on Multiple-Valued Logic*, 1998, pp. 52 -57.

[19] D. C. Montgomery and G. C, Runger, *Applied Statistics and Probability for Engineers*, 3rd ed. John Wiley & Sons, 2003.

[20] B. J. Weiner, J. A. Alexander, S. M. Shortell, L. C. Baker, M. Becker and J. J. Geppert, "Quality improvement implementation and hospital performance on quality indicators", *Health Services Res*.41(2) 307–333, 2006.

[21] J.R. Grout, "Preventing medical errors by designing benign failure", *Jt Comm J Qual Saf*, 2003 July, Vol 29(7) pp. 354-362.

[22] M. Lyons, S. Adams, M. Woloshynowych and C. Vincent, "Human Reliability analysis in healthcare: A review of techniques", *Intl J. of Risk & Safety in Medicine*, Vol 16, pp. 223-237, 2004.