

Robot Safety Analysis Methods

B.S. Dhillon

Department of Mechanical Eng.
University of Ottawa
Ottawa
Canada

Abstract

This paper presents robot safety related facts and figures along with the most useful seven safety analysis methods. The methods are failure modes and effect analysis, fault free analysis, Markov analysis, probability tree analysis, technic of operation review, hazards and operability analysis, and nuclear safety cross-check analysis. The application of the two most widely used methods (i.e., fault tree analysis and Markov analysis) is demonstrated by solving two robot safety-related problems.

INTRODUCTION

Robots are increasingly being used in the industry to perform various types of tasks: material handling, arc welding, spot welding, etc.

The history of robots/automation may be traced back to the ancient times when the Egyptians built water-powered clocks and the Chinese and Greeks built water- and stream-powered toys. Nonetheless, the idea of the functional robot originated in Greece in the writings of Aristotle (4th century B.C.), the teacher of Alexander The Great, in which he wrote: "If every instrument could accomplish its own work, obeying or anticipating the will of others..." [1].

In 1920, Karl Capek (1890-1938), a Czechoslovak science-fiction writer first coined the word "robot" and used it in his play entitled "Rossums Universal Robots" which opened in London in 1921. In the Czechoslovakian language, robot means "worker".

In 1954, George Devol [2] developed a programmable device that could be considered the first industrial robot. Nonetheless, in 1959, the first commercial robot was manufactured by the Planet Corporation and Japan, today the world leader in the use of robots, imported its first robot in 1967 [2]. In 1970, the first conference on industrial robots was held in Chicago, Illinois, and five years later (i.e., in 1975), the Robot Institute of America (RIA) was founded.

In 1985, the Japanese Industrial Safety and Health Association (JISHA) developed a document entitled “An Interpretation of the Technical Guidance on Safety Standards, etc. of Industrial Robots” [3].

Six years later, in 1991 a book entitled “Robot Reliability and Safety” was published and it presented a comprehensive list of publications on robot safety in addition to the important aspects of robot safety [4].

Over the years a large number of publications on various aspects of robot safety have appeared. Ref. [5] provides a list of these publications up to 2002. Robot safety may be interpreted in many different ways including preventing the robot from damaging its environments, particularly the human element of that environment or simply preventing damage to the robot itself [6].

ROBOT SAFETY RELATED FACTS, FIGURES, AND EXAMPLES

Some of the facts, figures, and examples concerning robot safety directly or indirectly, are as follows [7]:

- There are around one million robots in use world wide [8].
- In the mid-1990s, the total annual world robot market was estimated to be around \$6 billion with an average price of a robot being approximately \$82,000 [9].
- In 2000, there were a total of a 97300 unintentional injury deaths in the United States and their total cost was estimated to be around \$512.4 billion [10].
- The first robot-induced fatal accident occurred in Japan in 1978 [11].
- For the period 1978-1984, there were at least five fatal accidents involving robots: four in Japan and one in the United States [12].
- The first fatal robot-related accident occurred in 1984 in the United States [13].
- For the period 1978-1987, there were a total of ten robot-related fatal accidents in Japan [14].
- In 1987, a study of 32 robot-related accidents in Japan, the United States, West Germany, and Sweden revealed that line workers were at the greatest risk of the injury followed by maintenance personnel [15].
- A study reported that around 12-17% of the accidents in industries using advanced manufacturing technology were related to automated production equipment [12, 16].
- A material handling robot was operating in its automatic mode and a worker violated safety devices to enter robot work cell. The worker got trapped between the robot and a post anchored to the floor. Consequently, the worker was injured and died a few days later [4,17-18].

- A maintenance person climbed over a safety fence without turning off robot power and performed tasks in robot work zone while it was temporarily stopped. When the robot recommenced operation, it pushed the person into a grinding machine and the person died, subsequently [4, 17-18].

SAFETY ANALYSIS METHODS

Over the year various analysis methods have been developed in many areas of engineering including safety, reliability, and quality. Seven of these methods considered most useful to perform robot safety analysis are presented below [4, 19-20]

1. Failure Mode and Effect Analysis (FMEA)

FMEA is an important tool to evaluate system design from the reliability and safety angle. Originally, the method was developed in the early 1950s to evaluate the design of flight control systems [21]. The FMEA approach demands listing potential failure modes of each and every component on paper and their effects on the listed subsystems, system, and the surroundings. The following steps are associated with FMEA:

- Establish analysis scope.
- Collect data.
- List all possible failure modes, the identification, and description of each component.
- Assign failure rate/probability to each identified failure mode.
- List each failure mode effect or effects on subsystem, system, and so on.
- Enter appropriate remarks for each failure mode.
- Review each critical failure mode and take appropriate corrective measures.

The method is described in detail in Ref. [20].

2. Hazard and Operability Analysis (HAZOP)

HAZOP was originally developed for use in the chemical industry. HAZOP helps to identify problems prior to availability of full data concerning a product/system. The approach calls for the formation of a team made up of knowledgeable members with varying backgrounds, and in turn, the team brainstorms about potential hazards. An experienced individual chairs the team and serves as a facilitator during brainstorming sessions. The following basic steps are associated with the HAZOP technique [22]:

- Choose the system/product to be analyzed.
- Establish a team made up of appropriate members.
- Describe the HAZOP process to all individuals forming the team.
- Set goals and time schedules.

- Conduct brainstorming sessions as appropriate.
- Document end results.

One major drawback of the HAZOP approach is that it does not take into consideration human error in the final equation.

3. Technic of Operations Review (TOR)

Just like in the case of HAZOP, TOR seeks to identify systemic causes rather than assigning blames. TOR allows management and workers to work jointly to perform analysis of workplace accidents, incidents, and failures [23].

This safety analysis technique is not new; it was developed by D.A. Weaver of the American Society of Safety Engineers (ASSE) in the early 1970s.

TOR, basically, is a hands-on analytical methodology developed to determine the root system/product causes of an operation malfunction. The technique makes use of a worksheet containing simple terms requiring yes/no decisions. The basis for activating TOR is an incident occurring at a certain time and place involving certain individuals. The strength of the technique comes from involving line personnel in the analysis, and its weakness stems from the fact that it is designed as an after-the-fact process. The following steps are associated with the method:

- Form the TOR team containing appropriate members.
- Conduct a roundtable session for the purpose of departing common knowledge to all team members.
- Highlight one crucial factor that played an important role in the occurrence of accident/incident. This factor must be the result of team consensus and serves as an initial point to further investigations.
- Use the team consensus to respond to a sequence of yes/no options.
- Carefully evaluate the identified factors and ensure the existence of consensus among the team members.
- Prioritize the contributing factors.
- Establish corrective/preventive strategies with respect to each contributing factor.
- Implement strategies.

4. Nuclear Safety Cross-Check Analysis (NSCCA)

This is comprehensive software safety analysis method originally developed to meet the requirements of the United States Air force entitled “Nuclear Surety Design Certification for Nuclear Weapon System Software and Firmware” [23]. The method consists of an adversarial approach with the objective of showing a high degree of confidence that the software will not cause an undesirable event. The NSCCA is composed of two main components: technical and procedural. The purpose of the technical component is to ensure that system safety-related requirements are fully

satisfied. Similarly, the purpose of the procedural component is to provide effective protection and security for critical software elements.

The technical component analyzes and tests the software under consideration. First, the degree to which each software function affects safety goals is assessed and then the software is broken-down to the lowest-level functions. All these lowest-level functions are reviewed and the ones that do not affect critical events are not reviewed again. A critical matrix is established by plotting software functions against safety objectives. Each matrix cell assigns influence rating categorized into three levels: high, medium, or low. Furthermore, each software function is assigned recommendations for applicable evaluation methods.

The procedural component is concerned with security and control measures, in which factors such as background investigations for personnel clearances, facility security, configuration control and document security, and product controls are instituted.

All in all, this is a useful method for assuring that the system software has no incorrect design, programming, fabrication, or application that may result in unsafe conditions.

5. Probability Tree Analysis

This is one of the main techniques for human reliability analysis. Success or failure of each critical human action or associated event is assigned a conditional probability. The outcome of each event is represented by the branching limbs of the probability tree. The total probability of success for a particular operation is obtained by summing up the associated probabilities with the end point of the success path through the probability tree diagram. This technique, with some refinement, can include factors such as time stress, emotional stress, interaction stress, interaction effects, and equipment failures.

Some of the advantages of this technique are as follows:

- It serves as a visibility tool.
- The mathematical computations are simplified, which in turn decrease the probability of occurrence of errors due to computation.
- The human reliability analyst can estimate conditional probability readily, which may otherwise be obtained from the complicated probability equations.

The method is described in detail in Ref. [20].

6. Fault Tree Analysis (FTA)

FTA is a useful tool that can be employed to predict and prevent accidents. The method was originally developed at the Bell Telephone Laboratories to analyze the Minuteman Launch Control System with respect to reliability and safety in the early 1960s.

FTA may be described as an analytical methodology that uses graphic symbols to visually display the analysis process. Fault tree analysis begins by identifying an undesirable event, known as the top event, associated with a system. The events that could cause the occurrence of the top event are generated and connected by logic operators such as AND and OR. Thus, the fault tree itself is the logic structure relating the top event to the basic or the primary events. The basic principle underlying the construction of a fault tree is successively asking the question, “How could this event occur?”

Four basic symbols used in the construction of a fault tree are described below:

- AND gate (The symbol with a dot in middle in Fig. 1): This denotes that an output fault event occurs if all the input fault events occur.
- OR gate (The symbol without a dot in middle in Fig. 1): This denotes that an output fault event occurs if any one or more of the input fault events occur.
- circle: This denotes a basic fault event or the failure of an elementary component.
- rectangle: This denotes a fault event that results from the combination of fault events through the input of a logic gate.

A safety-related fault tree may be developed through following four steps:

- Decide on the top event accident/incident to be investigated.
- Identify the non-top event accidents/incidents/faults that may cause the top event to occur and assign appropriate symbols.
- Move downward through successive steps until basic fault/accident/incident events are identified.
- Review the end fault tree and make appropriate recommendations.

A detailed description of FTA is provided in Reference [20].

Example 1

Develop a fault tree, using the above four symbols, for the occurrence of a robot accident involving a human, which it caused by sudden robot movement. Fig. 1 shows the fault tree for Example 1.

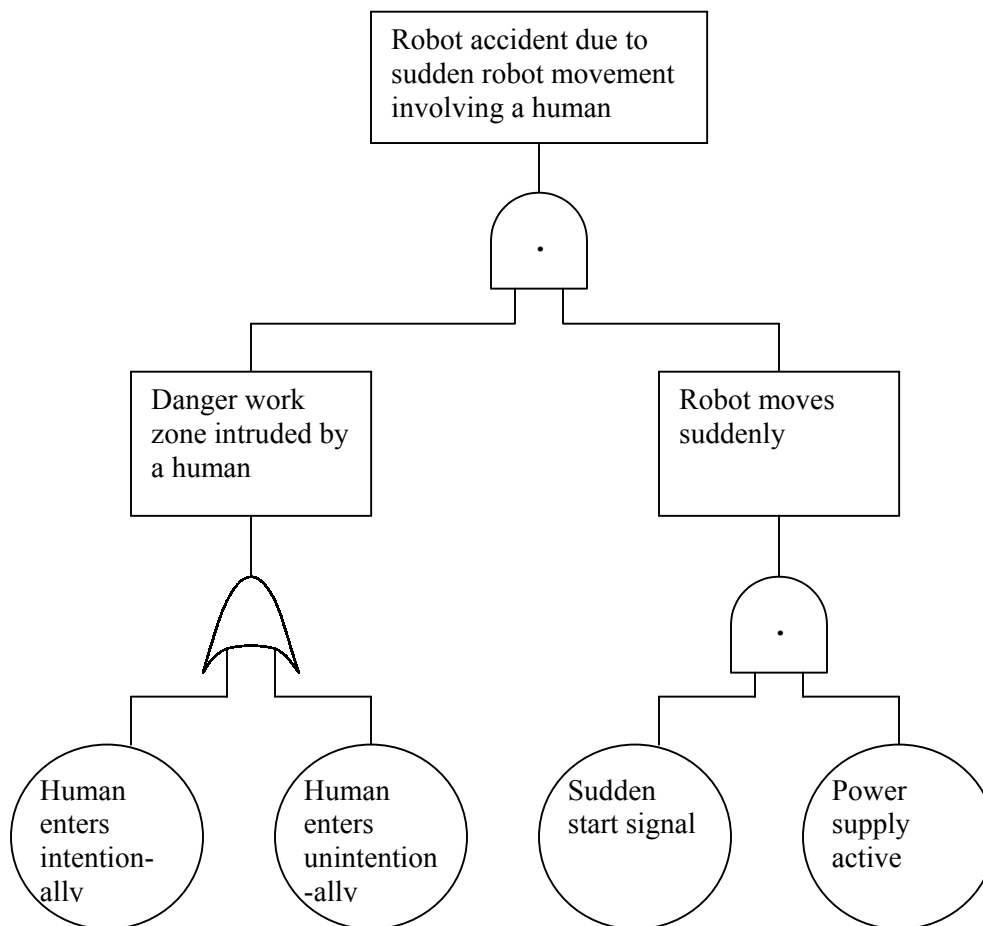


Fig. 1 Fault tree for the top event: robot accident due to sudden robot movement involving a human.

7. Markov Analysis

Markov analysis is a powerful reliability and availability analyses method named after a Russian mathematician. The method can also be used to perform various types of robot safety analysis [4]. Its application to perform robot safety analysis is demonstrated through a model whose state space diagram is shown in Fig. 2. The numerals in the boxes of Fig. 2 denote robot states.

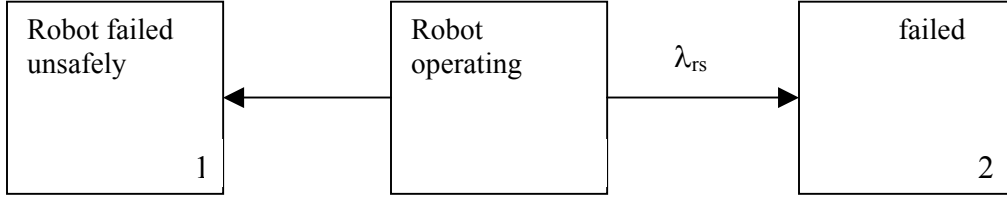


Fig. 2 State space diagram of a model representing a robot

The following two assumptions are associated with this model:

- All robot failures occur independently.
- Both robot failure rates are constant.

The following symbols were used to develop equations for the Fig. 2 model:

$P_i(t)$ is the probability that the robot is in state i at time t , for $i=0$ (working normally), $i=1$ (failed unsafely), $i=2$ (failed safely).

λ_{rs} is the constant failure rate of the robot failing safely.

λ_{ru} is the constant failure rate of the robot failing unsafely.

With the aid of Markov method we write down the following equations for Fig. 2 diagram [7]:

$$\frac{dP_0(t)}{dt} + P_0(t)\lambda_{rs} + P_0(t)\lambda_{ru} = 0 \quad (1)$$

$$\frac{dP_1(t)}{dt} - P_0(t)\lambda_{ru} = 0 \quad (2)$$

$$\frac{dP_2(t)}{dt} - P_0(t)\lambda_{rs} = 0 \quad (3)$$

At times $t=0$, $P_0(0)=1$, $P_1(0)=0$, and $P_2(0)=0$.

By solving Equations (1)-(3), we get

$$P_0(t) = e^{-(\lambda_{rs} + \lambda_{ru})t} \quad (4)$$

$$P_1(t) = \frac{\lambda_{ru}}{\lambda_{ru} + \lambda_{rs}} [1 - P_0(t)] \quad (5)$$

$$P_2(t) = \frac{\lambda_{rs}}{\lambda_{ru} + \lambda_{rs}} [1 - P_0(t)] \quad (6)$$

CONCLUSION

This paper presented seven methods considered useful to perform various types of robot safety analysis. A careful consideration must be given in selecting a method for a particular application, otherwise the effectiveness of the method could be compromised. It is contended that this study will be useful to design engineers, safety professionals, researchers, and others involved with robots.

REFERENCES

1. Heer, E., Robots in Modern Industry, in Recent Advances in Robotics, Beni, G. and Hackwood, S., Eds., pp. 11-36, John Wiley and Sons, New York, 1985.
2. Zeldwan, M. I., What Every Engineer should know About Robots, Marcel Dekker, New York, 1984.
3. An Interpretation of the Technical Guidance on Safety Standards in the Use of Industrial Robots, Japanese Industrial Safety and Health Association, Tokyo, 1985.
4. Dhillon, B. S., Robot Reliability and Safety, Springer-Verlag, New York, 1991.
5. Dhillon, B. S., Fashandi, A. R. M., Liu, K. L., Robot System Reliability and Safety: A Review, Journal of Quality in Maintenance Engineering, 8, 170-212, 2002.
6. Graham, J. H., Overview of Robot Safety, Reliability, and Human Factors in Robot Systems, Graham, J. H., Ed., pp. 1-10, Van Nostrand Reinhold, New York, 1991.
7. Dhillon, B. S., Engineering Safety: Fundamentals, Techniques, and Applications, World Scientific Publishing, New York, 2003.
8. United Nations Economic Commission for Europe (UN/ECE), World Robotics 2002-Statistics: Market Analysis, Forecasts, Case Studies and Profitability of Robot Investment, United Nations, New York, 2002.
9. Holland, S. W., Nof, S. Y., Emerging Trends and Industry Need, in Handbook of Industrial Robotics, Nof, S. Y., Ed., pp. 31-40, John Wiley and Sons, New York, 1999.
10. Report on Injuries in America in 2000, National Safety Council, Chicago, Illinois, 2000.
11. Tver, D. F., Bolz, R. W., Robotics Source Book and Dictionary, Industrial Press, New York, 1983.

12. Backstrom, M., Doos, M., A Comparative Study of Occupational Accidents in Industries with Advanced Manufacturing Technology, *International Journal of Human Factors in Manufacturing*, 5, 267-282, 1995.
13. Sanderson, L. M., Collins, J. W., McGlothlin, J. D., Robot-Related Fatality Involving a US Manufacturing Plant Employee: Case Report and Recommendations, *Journal of Occupational Accidents*, 8, 13-23, 1986.
14. Nagamachi, M., Ten Fatal Accidents Due to Robots in Japan, in *Ergonomics of Hybrid Automated System I*, Karwowski, H. R., Parsaei, H. R., Eds., pp. 391-396, Elsevier, Amsterdam, 1988.
15. Jiang, B. C., Gainer, C. A., A Cause and Effect Analysis of Robot Accidents, *Journal of Occupational Accidents*, 9, 27-45, 1987.
16. Clark, D. R., Lehto, M. R., Reliability, Maintenance and Safety of Robots, in *Handbook of Industrial Robotics*, Nof, S. Y., Ed., pp. 717-753, John Wiley and Sons, New York, 1999.
17. Nicolaisen, P., Safety Problems Related to Robots, *Robotics*, 3, 205-211, 1987.
18. Study on Accidents Involving Industrial Robots, Report No. PB 83239822, Prepared by the Japanese Ministry of Labor, Tokyo, 1982. Available from the National Technical Information Service (NTIS), Springfield, Virginia.
19. Addison, J. H., Robotic Safety Systems and Methods: Savannah River Site, Report No. DPST-84-907 (DE 35-008261), December 1984, issued by E.I. du Pont de Nemonts and Co., Savannah River Laboratory, Aiken, South Carolina.
20. Dhillon, B. S., *Design Reliability: Fundamentals and Applications*, CRC Press, Boca Raton, Florida, 1999.
21. Countinho, J. S., Failure Effect Analysis, *Transactions of the New York Academy of Sciences*, 26, 564-584, 1964.
22. Risk Analysis Requirements and Guidelines, Report No. CAN/CSA-Q634-91, Prepared by the Canadian Standards Association (CSA), 1991. Available from CSA, 178 Rexdale Blvd., Rexdale, Ontario, Canada.
23. AFR-122-9, Nuclear Surely Design Certification for Nuclear Weapon System Software and Firmware, Department of the Air Force, Washington, D. C., August 1987.

Short Biography

Dr. Dhillon has served as Chairman/Director/Acting Director of the Mechanical Engineering Department/Engineering Management Program for

over 10 years at the University of Ottawa. He has published over 300 articles and 26 books: Wiley (1981), Van Nostrand (1983), Marcel Dekker (1984), Pergamon (1986), etc. Many of his books are translated into languages such as German, Russian and Chinese and he is /has been on the editorial boards of 7 international scientific journals. Professor Dhillon has lectured in over 50 countries including keynote addresses at various scientific conferences held in North America, Europe, Asia, and Africa..