Robotica (1997) volume 15, pp 701–708. © 1997 Cambridge University Press

Safety and reliability assessment techniques in robotics

B.S. Dhillon and A.R.M. Fashandi

Department of Mechanical Engineering, University of Ottawa, Ottawa, Ontario K1N 6N5, Canada

(Received in Final Form: February 25, 1997)

SUMMARY

A robot has to be safe and reliable. An unreliable robot may become the cause of unsafe conditions, high maintenance costs, inconvenience, etc.

Over the years, in general safety and reliability areas various assessment methods have been developed, e.g. failure mode and effects analysis, fault tree analysis, and Markovian analysis. In view of these, this paper presents an overview of the most suitable robot safety and reliability assessment techniques.

KEYWORDS: Safety; Reliabiity; Assessment technique; Robots.

1. INTRODUCTION

A major concern in the design of any system is the determination of an acceptable level of risk of failure on the basis of economic and/or social consequences associated with such risks. This is normally accomplished by meticulous analysis of the reliability and safety of the system. Reliability may be defined[1] as the probability that an item will perform its function adequately for the desired period of time when operated according to specified conditions. On the other hand, safety may be defined[2] as freedom from those conditions that can cause damage to or loss of equipment or injury or death to human beings. These definitions clarify the fact that an industrial robot which fails to perform properly, due to either partial or total functional failure over extended periods of time, would not satisfy the required economics for implementation in an industrial application. Failures not only are uneconomical, but also can have an unsafe outcome. Engelberger[3] indicated that for most applications, up-time must exceed 97% to satisfy most users of industrial robots. In 1989 Klafter[4] wrote: "*a robot having the most innovative controller or programming language which if not mechanically reliable becomes nothing more than an expensive laboratory toy.*"

In recent years, the application of robots in the industrial sector has increased at an impressive rate. By the end of 1982, world robot population[5] was estimated to be at 30,000. According to the International Federation of robotics,[6] in 1987 there were 350,000 installed robots throughout the world and their number soared to over 520,000 in 1992. Although in the early years of robotics, applications were concentrated in automotive industry, recently however, the technology has been diversified and vastly utilized in other sectors of industry as well. A future potential market will undoubtedly be the general consumer where robots may well become another household item. By 2010, the predicted number of robots to be used in homes is over 5,000,000.[7] This makes the safety factor even more crucial since personal robots have to work among human beings. This means robots have to be much more reliable and safe, so as not to injure humans should a malfunction occur. In any case, this exponential increase in robot utilization underlines the fact that robots are here to stay. Not surprisingly Polakoff[8] expressed his passion for robots and wrote: *Man's marriage to robotics*: *A* "*for better or worse*".

Although a great deal of progression has been made to make robots safe and reliable, there is still much room for improvement. In fact there have been numerous reports of accidents and as far as reliability is concerned, according to published literature, recorded robot mean time to failure is only 500 to 2500 hours. There are many methods and techniques which may be used to make a robot more reliable and safer. This paper discusses the most suitable safety and reliability assessment methods separately.

2. ROBOTICS SAFETY PROCEDURES AND ANALYSIS TECHNIQUES

The major motive for investing in industrial robots is to enhance productivity and to relieve human operators from adverse environment and difficult or hazardous tasks. Robots, however, cannot function without human interference and if left unattended, it will gradually unable to continue its assigned tasks because breakdowns will occur which have not been allowed for by the human designers. Industrial robots like traditional machines can bring hazards for people who work with them. Human errors and component failures make such compulsory interaction (man-robot) dangerous and costly at times. Errors and/or failures which affect man-robot interface may be classified in various ways: What caused the error? What are the consequences? How can they be prevented? etc. Also, in order to understand how failures or errors may lead to accidents, to estimate their probabilities, and more importantly to reduce the likelihood of their happening, a number of analytical methods have been developed. Thus, this section presents most suitable robot related safeguarding techniques and safety methodologies taken from published literatures as well as a detailed introductory aspects of robot safety (i.e. the W5 of robot safety).

https://doi.org/10.1017/S0263574797000829 Published online by Cambridge University Press

2.1 The W5 (what, why, who, when, where) of robot safety

Safety requirements differ for applications with or without a human interface. In controlling hazards in a system without human interface, the entire application environment affecting the machine must be understood. In contrast, evaluating hazard potential with a human interface not only requires knowledge of the overall operation of the system, but also an understanding of how a human operator relates to the robot. This may be achieved by determining the universal questions (What?, Why?, Who?, When?, and Where?). The W5 of safety is illustrated in Figure 1.

a. Why Consider Robot Safety? Like any other power-driven machine, to date, there have been many reports of minor cuts, bumps, pinches, and shocks to people working with robots. There have also been however, a few fatalities. In Japan for instance, a robot pushed a maintenance worker into a grinding machine and he died.[9] Later investigation revealed that the man did not take proper safety precautions before entering the robot work envelope. Reports from other fatal accidents concluded that in most cases, human negligence were the cause of these sad accidents. Nevertheless, if robots could have been a bit more forgiving, these people would not have had to pay such a high price for their mistake. But why are robots unforgiving at times? Attempting to answer this question is best done by identifying the dark side of a robot. Generally speaking, a robot is blind, deaf, mute, dumb, and unconscious. The sum of these elements render robots dangerous and unforgiving. Once the necessity of considering robot safety is realized, the next step is to identify the sources of hazards.

b. What are the sources of hazards? The sources of robot accidents can be grouped into three categories:

(i) Those due to human error,
(ii) Those caused by robots, and
(iii) The environment in which man-robot interact.

The hazards due to man may arise as a result of the psychological behavior of the worker or the software errors of the programmer. Hazards due to the robot may occur from loss of structural integrity of the robot such as joint failure, material fatigue, erosion, etc. It can also originate from mechanical or electrical faults due to failures which occur randomly during the useful life of a component. There are also hazards from the environment such as accumulation of dust in the joints and motors which may cause malfunction of the robot.

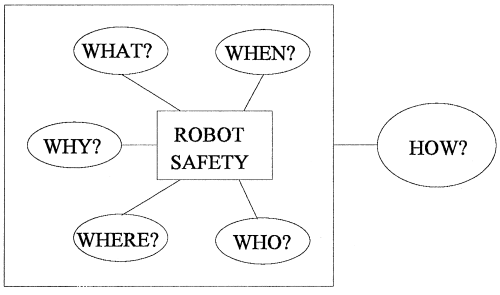

Fig. 1. The W5 of robot safety.

c. Who is Responsible?, Who is at Risk? and Who should be protected? The highest percentage of robot-related accidents occur during programming, teaching, and maintenance. A Swedish survey revealed that human error accounted for over 90% of accidents, whereas in another survey in Japan 2/3 were robot caused accidents.[10] With such discrepant data, it is not clear how much blame can be put on man and how much on the robot. Nevertheless, the primary objective of safeguarding is to protect humans from robots and the prevention of damage to the robots by the humans, particularly:

- Programmer/Teacher
- Maintenance personnel
- Operators
- Observers
- Equipment
- Work piece

d. When to Consider Safety? and When is the Critical Time? Historically new technologies were always implemented first and the safety factors incorporated afterwards because of lessons learned from unfortunate accidents resulting in injuries and property losses. The legal, social, and humanitarian considerations of our present world, however, require that safety issues be addressed during the early stages of technology implementation. Sugimoto[11] stated that the principal of safety starts with the notion: ''Safety is not the correction of accident that has already occurred and if a machine with no accident record has a potential hazard, safety measures should be instituted beforehand''. This implies that:

- Safety measures should be incorporated before accidents occur, and
- Safety is a planned and continuous process that is paramount to any successful robot application. The cost of safety is always acceptable compared to the cost of accident.

Robots typically have reliability, 98% or better. The 2% downtime (critical time) include factors like planned maintenance and programming or is due to failure of some sort. During this period the robot is the most dangerous, because people directly interface with it. According to many studies, only 5 to 15 percent of the accidents occurred in automatic mode.[11,12] This means 85 to 95 percent occur when the robot system is under manual operation control, such as during programming or maintenance of the robot.

e. Where to Consider Safety? Types of injuries caused by robots are more diverse than those caused by other machines. Robots can strike, crush, or thrust to any location inside the point of operation. The likelihood of accidents taking place outside the work envelope must also be considered. One such situation could arise if a part being handled by the end effector slips and is thrown at varied trajectories well outside the point of operation.

https://doi.org/10.1017/S0263574797000829 Published online by Cambridge University Press

This could become more dangerous in the case of mobile robots which are to assume prominence in industry.

2.2 Safety analysis methodologies

As a branch of system analysis, system safety analysis has come of age in many areas of design and manufacture. The system safety concept requires timely identification and evaluation of system hazards before losses occur. In other words, the ultimate aim is to produce a better understanding of the potential safety problems for a given system (such as in robotics) and to suggest actions which may improve system safety. To achieve this aim, the process of safety analysis often calls for the use of different methodologies which may include qualitative and quantitative analysis or both. These techniques are used to identify and evaluate system hazards and assure that safety is properly designed into each subsystem component of a major system. Clemens[13] outlined 25 methods for hazard identification and evaluation while Rahimi[14] gave an overview of the system safety techniques applied to robotics. Among the qualitative techniques are preliminary hazard analysis, subsystem analysis, failure mode and effects analysis (FMEA), energy barrier analysis (EBA), critical incident technique, task analysis approach, system simulation, deviation analysis, and near accident analysis. An example of a more quantitatively inclined technique is fault tree analysis (FTA) which usually involves application of probability theory to quantify the hazard probability of each event or component of a system. Some of these techniques have a broad application base (e.g., Preliminary hazard analysis, Task analysis, system simulation) and need to be further detailed out for an application such as robotics safety. Deviation analysis is a new method which is used principally in other methods such as FMEA. Among the techniques listed above, FTA and FMEA appear to be more appropriate techniques for robot safety analysis. Almost all of the potential dangers in the robot-man work environment are the result of combinations of unsafe conditions and unsafe actions. A deductive analysis of the conditions for combination of these factors and their cause-and-effect logical construction can be made by fault-tree analysis. FTA concentrates on accidents arising from characteristic function or structural features of robots. These two techniques are described below.

a. Fault-Tree-Analysis (FTA). The fault tree method is a systematic, descriptive form of analysis that has been widely used for quantitative analysis of the safety and reliability of nuclear power generation systems. Sugimoto and Kawaguchi,[10] Nagamachi,[15] Nagamachi *et al.,*[16] Sugimoto,[17] and Devianayagam[18] proposed the use of fault tree analysis in robot safety. As used in system safety analysis, the tree leads to an undesired event (i.e. top event) and determines the sets of fault events that cause the outcome in question. For example, sudden transfer of kinetic energy of the robot to the human body due to unexpected robot motion is responsible for the majority of accidents. The top event in Figure 2 is a classical example of such a case. The fault-tree method is described in detail in reference 19.

b. Failure Mode and Effects Analysis (FMEA). Failure mode and effect analysis (FMEA) is one of the most widely used methods that uses a tabular form to identify the modes of failure for the components of a system along with their occurrence probability, severity, and effects of failure. In general terms, FMEA is used to do the following:[20]

- Ensure that all conceivable failure modes and their effects are understood.
- Assist in the identification of system weaknesses.
- Provide a basis for selecting alternatives during each stage of operation.
- Provide a basis for recommending test programs and improvements.
- Provide a basis for corrective action priorities.

The analysis traces the problem back into its root by answering the following questions;

- How can the component fail (cause)?
- What are the consequences (effects) of the failure?

Once these questions are properly answered, a list of symptoms or methods of detection of each failure mode is formulated for safe operation. Thus, the next step would be to answer the following:

- How is failure detected? and,
- What are the safeguards against the failure?

One example of studies concerning FMEA in robotics safety was performed by Jiang and Gainer.[12] The study was motivated as a result of 32 robot accidents which occurred between 1984 to 1986 in the U.S., West Germany, Sweden and Japan. The analysis included the accident source, the accident cause, the accident effect in terms of human injury, recommended guidelines to be implemented, and applicable safety standards in each case. The accidents' causes were grouped into four categories (human error, workplace design, robot design and others). The accidents' effects were grouped according to who was injured (line worker, maintenance worker or programmers), the type of injury (pinch-point, impact or other), and the degree of injury (fatal or non-fatal). By using this approach (i.e. FMEA), the authors were able to conclude that one of the most important tasks in eliminating or reducing the probability of robot accidents is to identify the cause by which they may take place, and attention must be paid to safety throughout all phases of robot implementation including workplace design, robot installation, robot testing and robot operation. The FMEA method is described in detail in reference 19.

3. RELIABILITY ANALYSIS TECHNIQUES FOR ROBOTS

Robot reliability is a very complex issue. There are many interlocking variables in predicting and achieving various levels of reliability. Components with varying degrees of

https://doi.org/10.1017/S0263574797000829 Published online by Cambridge University Press

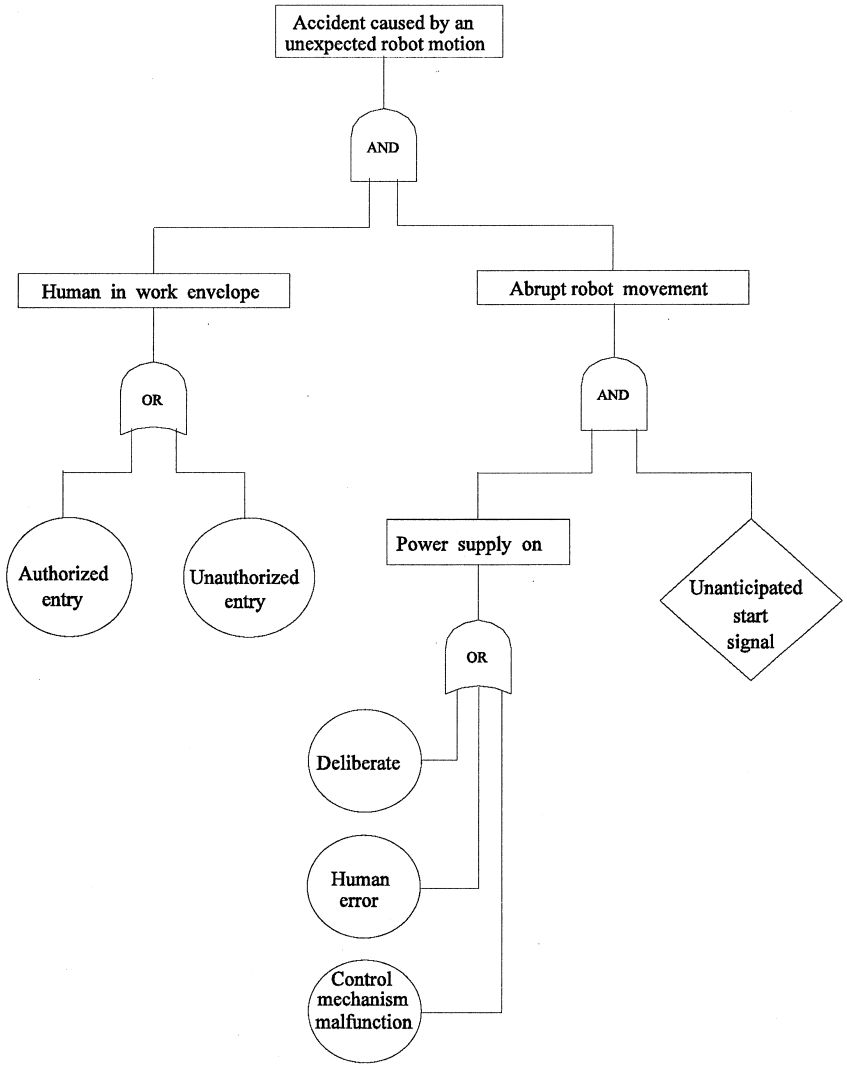

Fig. 2. Fault-tree analysis for the top event: accident caused by an unexpected robot movement.

sophistication are used in many different combinations to make today's industrial robots. As mechanical, hydraulic, pneumatic, and electronic parts are used in their design, this brings with it many sources of failures. In general, failures of a robot system may be classified into the following categories:[21,22]

- Failures due to structural malfunctions,
- Failures due to technological malfunctions, and
- Failures due to behavioral malfunctions.

In robot systems, structural failures could be related to the materials that are susceptible to external and internal changes in temperature, pressure, etc. Technological failures could be due to random component failures, systematic hardware faults, and software error. Behavioral failures could be the result of decisional (human) errors during operation or maintenance repair. Sources of failure must be considered right from the design and development phase to implementation and continuous operational phases. It is therefore necessary to assess the reliability of the robot in depth so that modifications of the design as well as component selection can be allowed for achieving a higher degree of reliability. Robot reliability assessment is performed to identify potential design weaknesses through systematic documented consideration of the following topics:

- All possible ways in which robot can fail.
- Causes for each mode of failure.
- Effects of each failure mode on robot system reliability.
- Probability of occurrence of each failure mode.

In performing the reliability analysis of a robot system, first of all an important task is to identify the most suitable available analytical methods. After considering the factors such as cost, simplicity, and effectiveness, the most appropriate of the analytical methods are as follows:

- Failure Mode and Effects Analysis (FMEA),
- Fault Tree Analysis (FTA),
- Block diagram,
- Combinational models (i.e., combined Fault Trees and block diagram),
- Markov and Non-Markovian Models, and
- Simulation Technique (Monte-Carlo).

Each of the above methods is described below briefly.

https://doi.org/10.1017/S0263574797000829 Published online by Cambridge University Press

3.1. Failure Mode and Effect Analysis (FMEA)

As in safety analysis, FMEA can also be used in reliability evaluation of a robot system. It is used to systematically analyze the failure modes of components of a robot and determine the effects of these failures on robot performance. One main advantage of FMEA is hypothesizing the source of failure, thereby reducing the probability of failure or reducing the severity of failure by redesign to produce a fail-safe, or system redundancy, etc. For instance, the robot joint in Figure 3 can fail due to various faults. Each component and its associated failure modes are considered individually and their effect on other components as well as on the whole system, (i.e. the point) is identified. One major draw back of FMEA is its singularity-failure analysis.[23] This means that FMEA is not well suited for assessing the combined effects of two or more failures.

3.2. Fault Tree Analysis (FTA)

This method is equally applicable to robot safety/reliability analyses. FTA is a valuable tool that can be applied by which the subsystem or component failure events leading to system failure are related using simple logical relationships. These relationships are a structural-model of cause and effect that represent the system failure modes. FTA can provide information on how a system may fail, what the probability of the occurrence of the top event (i.e. undesired event) is, and what remedies may be used to overcome the causes of failure. Figure 4 shows the hierarchy of the combination of events that contribute to the top event of joint failure. The joint can fail either because of actuator failure, structural failure, or failure of one of the hinges. Hinge failure is a basic fault which can be assigned an independent probability. Actuator failure however, can either be caused by pipe failure or to valve malfunction. Pipe failure may be treated as a basic fault whereas valve malfunction can be traced back further. FTA is described in detail in reference 19.

3.3 Reliability block diagram

In general, the main objective of a reliability study is to predict the performance of a complete system. Block diagram[1] (also called reliability network) is one of the

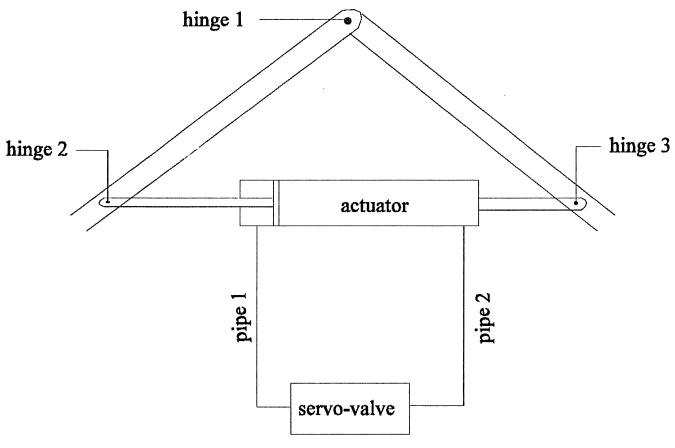

Fig. 3. Possible sources of failure of a robot joint.[24]

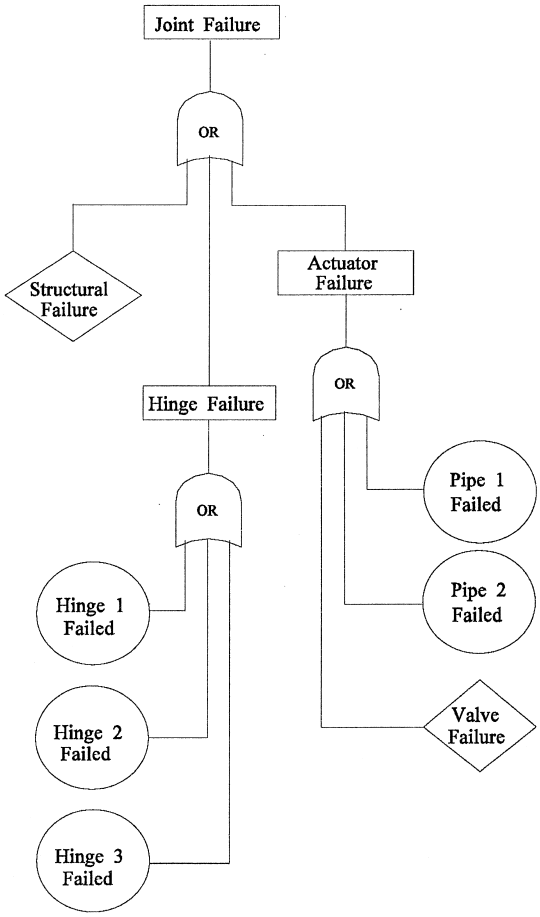

Fig. 4. Fault-tree for a robot joint failure.

simple and effective methods which enables the system failure probability to be evaluated in terms of the component performance characteristics. The first step in the reliability prediction is to identify failure modes of the system and collect reliability information on all of its components. A block with assigned probability of success or failure rate represents each component. Blocks are then connnected together so as to form a reliability network which represents the reliability dependencies between components of the system. Figure 5(a) represents a system reliability whose components are placed in series (also known as non-redundant system). In this fashion component failure cannot be tolerated and any component failure will break the single path, thus cause system failure.

For a general series network containing n components, the system failure and success expressions are

$$Q_{SS} = 1 - \prod_{i-1}^{n} (1 - Q_i) \tag{1}$$

and

$$R_{SS} = \prod_{i-1}^{n} R_i \tag{2}$$

where Q_i = Probability of failure of the ith component.
Q_{ss} = Probability of failure of the series system.
R_i = Probability of success of the ith component.
R_{ss} = Probability of success of the series system.

https://doi.org/10.1017/S0263574797000829 Published online by Cambridge University Press

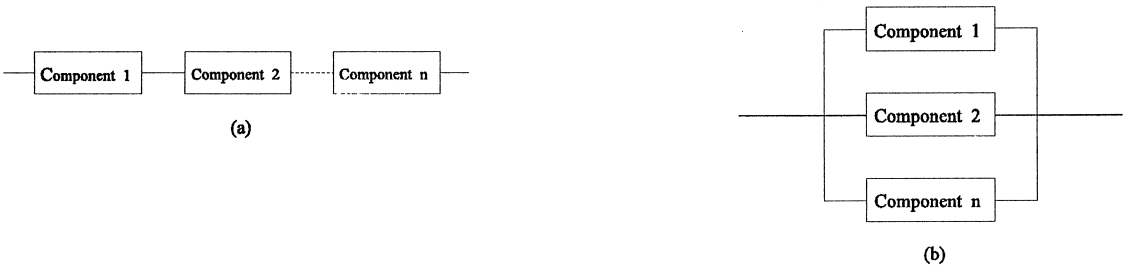

Fig. 5. Reliability block diagrams: (a) Series configuration, (b) Parallel configuration.

Systems with a higher degree of reliability usually require redundancy in part or all of the system. The simplest form of a redundant system is the parallel configuration shown in Figure 5(b). Here, all paths must fail to cause system failure. The system reliability for a parallel configuration is given by

$$Q_{PS} = \prod_{i-1}^{n} Q_i \tag{3}$$

and

$$R_{PS} = 1 - \prod_{i-1}^{n} (1 - R_i) \tag{4}$$

where Q_{PS} = Probability of failure of the parallel system.
R_{PS} = Probability of success of the parallel system.
n = Number of components.

The primary advantage of this method is that it is easy to understand and apply. However, generally it is not suitable for degraded failure modes of components and subsystems.

a. Combinational Models. Combinational models have been widely used and have become a standard method for reliability prediction because they are conceptually simple and easy to understand. These models are basically represented by combination of fault trees and block diagrams. There are however, some limitations to this approach:[25]

- It is difficult, if not impossible to allow for various types of dependencies such as repair, near coincident faults, transient and intermittent faults and standby systems with spares.
- The nature of the combinational approach requires that all combinations of events for the entire time period must be included. For complex systems, this results in complicated models.
- A fault tree is constructed to predict the probability of a single failure condition (i.e. top event). If a robot has many failure conditions, separate fault trees must be constructed for each one of them.

3.4. Markov analysis

Markov method has been used extensively in determining the reliability of complex systems. It is a powerful method which can handle a wide range of system behaviors. The method is particularly useful in representing situations where component failures are not independent. In this technique, the random behavior of systems varies discretely or continuously with time and space but the technique can be applied only when certain restrictions are fulfilled. The assumptions[26] such as the following are made in developing reliability analysis of a system:

(i) The state of the system changes as time progresses.
(ii) The transition rates are constant.
(iii) All failure occurrences are independent.
(iv) The probability of two or more failure occurrences in a finite time interval is negligible.

The following example demonstrates the applicability of the Markov method to a repairable robot system. The transition diagram of the repairable robot system[27] is illustrated in Figure 6.

The following equations translate the robot system diagrammatically described in Figure 6:

$$P_0(t + \Delta t) = P_0(t)(1 - \lambda_r \Delta t) + P_1(t)\mu_r \Delta t \tag{5}$$

and

$$P_1(t + \Delta t) = P_1(t)(1 - \mu_r \Delta t) + P_0(t)\lambda_r \Delta t \tag{6}$$

where

j = State of the system; $j = 0$ means the robot is operating normally, $j = 1$ means robot system has failed.
$P_j(t)$ = The probability that the robot is in state j at time t for $j = 0,1$.
λ_r = Constant failure rate of the robot system.
$\lambda_r \Delta t$ = Transitional probability of failure of the robot in finite time interval Δt.
$P_j(t + \Delta t)$ = The probability that the robot system is in state j at time $t + \Delta t$ for $j = 0,1$.
$(1 - \lambda_r \Delta t)$ = Probability of no failure in time interval Δt when the robot system is in state 0.

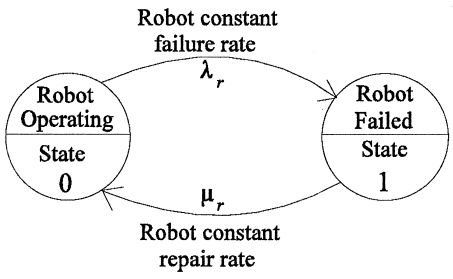

Fig. 6. Transition diagram for the states of a robot.

https://doi.org/10.1017/S0263574797000829 Published online by Cambridge University Press

μ_r = Constant repair rate of the robot system.
$\mu_r \Delta t$ = Transitional probability of restoration of the robot in finite time interval Δt.
$(1 - \mu_r \Delta t)$ = Probability of not restoring the robot system in time interval Δt.

Using equations (5) and (6) we get

$$AV_r(t) = P_0(t) = \frac{\mu_r}{\mu_r + \lambda_r} + \frac{\lambda_r}{\lambda_r + \mu_r} e^{-(\lambda_r + \mu_r)t} \tag{7}$$

and

$$UA_r(t) = P_1(t) = \frac{\lambda_r}{\lambda_r + \mu_r} - \frac{\lambda_r}{\lambda_r + \mu_r} e^{-(\lambda_r + \mu_r)t} \tag{8}$$

where

$AV_r(t)$ = Availability of the robot system at time t.
$UA_r(t)$ = Unavailability of the robot system at time t.

In practice, the industry sector is usually concerned with the proportion of potential running time that the robot is available (up-time). Equations (7) and (8) also represent the availability and unavailability of the robot, respectively. When time becomes infinitely large, the robot steady-state availability (SSAV) and unavailability (SSUA) are as follows:

$$SSAV = \frac{\mu}{\mu + \lambda} \tag{9}$$

and

$$SSUA = \frac{\lambda}{\mu + \lambda} \tag{10}$$

3.5. Non-Markovian models

Constant hazards rates are analysis friendly and are very good assumptions in many reliability studies. In fact, in most cases exponentially distributed failure times are assumed in reliability analysis of components during their useful life period. This is the middle portion of so called "bathtub" curve. Non-constant failure and repair rates are a reasonable assumption during the "debugging period" (also called infant mortality period) and "wear-in period". Also in many other cases where reliability/availability predictions are crucial to system operation at any given time, the constant failure and repair rates may not be a valid assumption. A typical example is the reliability and safety assessment of components used in nuclear industry. Two frequently proposed methods to deal with those cases are supplementary variables[28] and the device of stages.[29] Thus such methods may be applied to analyze robots with non-constant failure and repair rates.

3.6. Monte-Carlo simulation

Monte-Carlo simulation can be used to calculate system reliability by simulating the failure of the components at times distributed according to their failure rates. Random samples from item failure and repair distributions are taken which require the generation of very large quantities of random numbers. Since every event (failure, repair, movement, etc.) must be sampled for every unit of time, a simulation of a moderately large system over a reasonable period of time can require hours of computer time. This technique is recommended only when other methods cannot handle the robot problem or when the simplifying assumptions to be made to make the problem solvable by other methods are not acceptable. For example, failure of components may not be independent and prevent the use of a general fault tree analysis. In addition, component failure or repair distributions may not be exponentially distributed. This means that the transition from one state to another is not governed by the negative exponential distribution which therefore prevents the use of the Markov method. As indicated earlier, the major drawback with this method is its extensive use of computer time. Also, if a minor change occurs the simulation must be rerun at considerable cost.

References

1. B.S. Dhillon, *Reliability Engineering in System Design and Operation* (Van Nostrand Reinhold Company, New York, 1–4, 1983).
2. *MIL-STD-882,* "System Safety Program for System and Associated Subsystem and Equipment-Requirements for" (1962).
3. J.F. Engleberger, "Three Million Hours of Robot Field Experience" *The Industrial Robot* 164–168 (1974).
4. R.D. Klafter *et al., Robotic Systems* (Prentice-Hall, Englewood Cliffs, New-Jersey, 1989).
5. "Worldwide Robotics Survey and Directory" *Robotic Institute of America* 25–27 (1983).
6. E. Solem, "Social and Economic Factors of Robotics Systems" *Proceedings of the 1987 Military Robotics Association Conference,* Victoria, B.C. Canada (1987) pp. 83–94.
7. I.C. Kato, "Towards the Age of Minor Robots" *Proceedings of the 20th Century Symposium on Industrial Robots,* Tokyo, Japan (1989) pp. 233–239.
8. P.L. Polakoff, *Man's Marriage to Robotics*: A "for Better or Worse" (Union, Occupational Health and Safety) **54,** No. 4, 24–25 1985).
9. V.M. Altamuro, "Working Safely With Iron Collar Worker" *National Safety News* 38–40 (1983).
10. N. Sugimoto and K. Kawaguchi, "Fault Tree Analysis of Hazards Created by Robot" *Proceedings of the 13th International Symposium on Industrial Robots and Robot 7* (1983) **Vol. 7,** pp. 9.13–9.28.
11. N. Sugimoto and T. Houshi, "Fundamental Safety in a New Machine with a Minimum Record of Accidents" *Proceedings of the 16th International Symposium on Industrial Robots* (1986) pp. 1123–1135.
12. B.C. Jiang and C.A. Gainer, "A Cause and Effect Analysis of Robot Accidents" *J. Occupational Accidents* **9,** 27–45 (1987).
13. P.E. Clemens, "Compendium of Hazard Identification and Evaluation Techniques for System Safety Application" *Hazard Prevention* **2,** No. 2, Chicago, Illinois, 11–18 (1982).
14. M. Rahimi, "System Safety for Robots: An Energy Barrier Analysis" *J. Occupational Accidents* **8,** 127–138 (1984).
15. M. Nagamachi, "Human Factors In Industrial Robots" Robot Safety Management in Japan, *Applied Ergonomics* **17,** No. 1, 9–18 (1986).
16. M. Nagamachi and Y. Anayama, "Human Factor Study of the Industrial Robot, Part II: Human Reliability on Robot Manipulation" *Japanese Journal of Ergonomics* **20,** 55–64 (1984).
17. N. Sugimoto, "Subjects and Problems of Robot Safety

https://doi.org/10.1017/S0263574797000829 Published online by Cambridge University Press

Technology'' *Occupational Health and Safety in Automation and Robotics* (edited by K. Noro) (Taylor & Francis, London, 1987) pp. 175–195.
18. S. Devianayagam, ''Safety of Robotics Work Systems'' *Trends in Ergonomics/Human Factors III* (edited by Karwowski) (Elsevier, Amsterdam, 1986) pp. 1035–1040.
19. A. Pouliezos and G.S. Stavrakakis, ''Fast Fault Diagnosis for Industrial Processes Applied to the Reliable Operation of Robotic Systems'' *Int. J. Systems Science* **20,** 1233–1257 (1989).
20. C. Sundararajan, *Guide to Reliability Engineering* (Van Nostrand Reinhold, New York, 1991) pp. 146–152.
21. J.P. Van Gigch, ''Modelling, Metamodeling and Taxonomy of System Failure'' *IEEE Transaction on Reliability* **32,** 131–136 (1986).
22. J.P. Van Gigch, ''Diagnosis and Metamodeling of System Failure'' *System Practice* **10,** 31–45 (1988).
23. E.E. Lewis, *Introduction to Reliability Engineering* (John Wiley & Sons, New York, 1987).
24. P.B. Scott, *The Robotics Revolution*: *Safety and Reliability* (Basil, Blackwell, Oxford, London, 1984) pp. 27–40.
25. I. Bazovsky, ''Reliability Analysis of Large System by Markov Techniques'' *Proceedings Annual Reliability and Maintainability Symposium* (1993) pp. 260–267.
26. S.S. Rao, *Reliability Based Design* (McGraw-Hill, New York, 1992) p. 415.
27. B.S. Dhillon, *Robot Reliability and Safety* (Springer-Verlag, New York, 1991).
28. D.P. Gaver, ''Time to Failure and Availability of Paralleled Systems With Repair'' *IEEE Transactions on Reliability* **12,** 30–38 (1963).
29. M.L. Shooman, *Probabilistic Reliability*: *An Engineering Approach* (McGraw-Hill, New York, 1968).