Overview of system reliability analyses for PSA

MATSUOKA Takeshi

Mechanical Systems Engineering, Department of Engineering, Utsunomiya University,
7-1-2 Yoto, Utsunomiya City, 321-8585 Japan, (mats@cc.utsunomiya-u.ac.jp)

Abstract: Overall explanations are given for many matters relating to system reliability analysis. Systems engineering, Operations research, Industrial engineering, Quality control are briefly explained. Many system reliability analysis methods including advanced methods are introduced. Discussions are given for FMEA, reliability block diagram, Markov model, Petri net, Bayesian network, goal tree success tree, dynamic flow graph methodology, cell-to-cell mapping technique, the GO-FLOW and others.
Keyword: systems engineering; system reliability analysis; FMEA; DFM; GO-FLOW

1 Introduction

In this paper, overall explanations are given for system reliability analyses [1] and related matters.

We will first define what a system is, and thereafter give explanations regarding systems engineering and related technological fields. Frankly speaking, there are a plethora of related fields and a detailed discussion is required for each field. In this paper, however (vide infra), relatively brief explanations are given in order to understand the systems engineering in relation to other technologies.

Many system reliability analysis methods have been proposed and used for PSAs, particularly in the assessment of nuclear power plant safety. Event tree and fault tree analyses are widely used in nuclear field, but there are many other advanced methods that can possibly be utilized in more realistic and sophisticated analysis. Discussions are given for various kinds of system reliability analysis methods including FMEA, reliability block diagram, Markov model, Petri net, Bayesian network, dynamic flow graph methodology, the GO-FLOW and so forth. If you find out a promising method for your analysis, please check the references for more comprehensive details.

2 What is a system?

System can be defined in layman's terms as something consisting of fundamental elements. The elements interact with each other and produce some function as a whole, which is in principle not obtainable by the elements alone.

As such, then, a system has some structure and behavior. Usually, a system receives inputs from surroundings, processes internally, produces a new thing and sends out as outputs.

Systems are not restricted as engineering systems. If fundamental elements are humans, systems are social organizations such as university, company, administrative body and so on.

If we consider more abstract elements, we can justifiably assert that economical systems such as International Olympic Committee and United Nations can also be considered as systems.

In addition, if we treat both engineering equipment and humans at the same time, we can confidently say that the object is "Human-Machine system". In recent days, engineers have to consider human-machine system for the safety operation of engineering systems.

3 Systems engineering and related fields

In this chapter, explanations are given for systems engineering and related technological fields. There are many kinds of pertinent fields with each field having its own distinctive features. To grasp the fundamental features in each respective field, there is indeed a need to discuss the various features for each field. However, in this (article) we will give relatively

Received date: February 25, 2012
(Revised date: March 14, 2012)

brief explanations sufficient to understand the systems engineering in relation to other technologies.

3.1 Systems engineering

Systems engineering is utilized for designing and constructing large facilities, or for executing big projects or for managing large organizations.

The term "Systems engineering" has its roots from Bell Telephone Laboratory in 1940s. But, activities of systems engineering are found even in the ancient ages. Construction of Pyramid in Egypt, or contraction of Great Wall in China could be achieved by the aid of "Systems engineering".

In recent days, "Air defense system" in the United States, "Apollo project", "modern Olympic game", and "International space station", are exemplars of systems running under systems engineering.

Systems engineering is pivotal to resolving problems in our society, for instance, heavy traffic and environmental pollution. For the solution of these problems, we should consider not only the technical aspects of each element, but also the correlation between elements, total system structure, information flow, control system, *etc*.

Systems engineering is the art and skill of developing a system capable of meeting requirements under certain restrictions. In other words, systems engineering is a logical way of thinking.

Running systems engineering for robust projects warrants cooperation among structural engineers, electrical engineers, mechanism designers, power engineers, human factors engineers, and many more engineers in various disciplines.

3.2 Operations research (OR)

Operations research is an interdisciplinary mathematical science that focuses on the effective use of technology. A wide range of problem-solving techniques and methods are applied in the pursuit of improved decision-making and efficiency. It provides useful solution for military research, planning of production, transportation, and so on. It largely overlaps with systems engineering.

Operations research originated in the efforts of military planners during World War II by US and UK. Britain introduced the convoy system to reduce shipping losses, with the principle of using warships to accompany merchant ships. It was unclear whether it was better for convoys to be small or large. Small convoys could travel faster. It was also argued that small convoys would be harder for German U-boats to detect. On the other hand, large convoys could deploy more warships against an attacker.

A team at Coastal Command's Operational Research Section (CC-ORS), showed that the losses suffered by convoys depended largely on the number of escort vessels present, rather than on the overall size of the convoy. Their conclusion, therefore, was that a few large convoys are more defensible than many small ones. This was the first example of the application of operations research.

After the war, the techniques began to be applied more widely to problems in business, industry and society.
Later, computer was used in OR. Tools used in OR are statistics, optimization, probability theory, queuing theory, game theory, graph theory, decision analysis, mathematical modeling, simulation, *etc*.

3.2.1 Cake shop example

Let us learn a logical way of thinking by a model situation given as follows.

There is a prosperous cake shop which has a sellout policy. At every morning, 100 cakes are produced, and all are sold by the end of the day. Cost of material is 70cents per 1 cake. Staff costs and running costs of shop are 50 dollars per day. They are constant costs independent of the number of sold cakes. They are equivalent to 50 cents per 1 cake. The shop sells this cake at a price of 2 dollars, that is, the profit is 80 cents per 1 cake.

(Question 1) If shop attendant drops one cake by mistake, how much is the loss of the shop? (Answer is given in chapter 7.)

In the second situation, the shop produces lots of cakes every day and keeps stock at any time. At the end of day, the shop discards unsold cakes.

(Question 2) If shop attendant drops one cake by mistake, how much is the loss of the shop?

In the third situation, consider an Italian restaurant. It serves spaghetti plate with 2 dollars, and material cost, constant cost and profits are the same to the cake situation. The restaurant makes plate by the order of guest. Unused material can be used on the next day.

(Question 3) If a visitor goes out without making order, how much is the loss of the shop?

3.2.2 Linear programming

Linear programming is a technique for the optimization of a linear objective function, subject to linear equality and linear inequality constraints. It aims at "optimization", that is, "maximum achievement with minimum efforts".

A linear programming algorithm finds a point in the polyhedron where this function has the smallest (or largest) value if such point exists.

Typical problems solved by linear programming are warehouse management, water intake plan, optimal allocation of traffic or facility.

3.2.3 Decision theory

Decision theory is closely related to the field of game theory as to interactions of agents with at least partially conflicting interests whose decisions affect each other. One example is shown in Table 1, which is a payoff matrix of an investment.

Table 1 Payoff matrix

	Strong economy	Slowdown economy
Aggressive policy	10	-3
Negative policy	5	2

A president of a company has to decide the policy of next year's investment based on this payoff matrix.

(Question 4) What is the optimum decision of the president ?

3.2.4 Game theory

This is the study of mathematical models of conflict and cooperation between intelligent and rational decision-makers. A person's success is based upon the choices of others. Game theory is mainly used in economics, political science, and psychology, and other, more prescribed sciences.

Von Neumann's work in game theory culminated in his book[2].

A matrix of symmetric 2×2 game is shown in Table 2. In this table, values of matrix elements are the ones for A and the values inside the parenthesis are for B.

Table 2 Symmetric 2×2 game

		B's strategy	
		B1	B2
A's strategy	A1	$\alpha(\alpha)$	$\beta(\gamma)$
	A2	$\gamma(\beta)$	$\delta(\delta)$

According to the values of matrix elements, situations are categorized as follows[3].

1)Situation 1: $\gamma>\delta>\alpha>\beta$ --> "Deadlock game"

2)Situation 2: $\gamma>\alpha>\delta>\beta$ --> "Prisoner's dilemma"

3)Situation 3: $\gamma>\alpha>\beta>\delta$ --> "Chicken game"

4)Situation 4: $\alpha>\gamma>\beta>\delta$ --> "Deer hunting game"

Chicken game is an influential model of conflict for two players in game theory. While each player prefers not to yield to the other, the worst possible outcome occurs when both players do not yield. The name "chicken" has its origins in a game in which two drivers drive towards each other on a collision course. One must swerve, or both may die in the crash, but if one driver swerves and the other does not. The one who swerved will be called a "chicken," meaning a coward.

3.2.5 Queuing theory

Queuing theory is the mathematical study of waiting lines, or queues. The theory enables mathematical analysis of several related processes, including arriving at the back of the queue, waiting in the queue, and being served at the front of the queue. The theory

permits the derivation of average waiting time, the expected number of waiting or receiving service, and so forth.

As a simple example, consider the following case. A customer arrives every 5 minutes, and a cash register takes 3 minutes to deal with the customer, on average. If both activities take regularly, there is no waiting. However, in the actual situation, customers arrive irregularly, sometimes 8 minutes interval. Cash register also sometimes takes longer time, for example, 6 minutes.

Assume distributions for the arrival interval and service time duration, for example, to be Poisson distribution and exponential distribution, respectively. Then analysis result reveals us that "number of waiting person" is 0.9 persons and "waiting time" is 4.5 minutes, on average.

If average service time of cash register changes to 4.5 minutes from 3 minutes, "number of waiting person" becomes 8.1 persons and "waiting time" becomes 40.5 minutes, surprisingly.

3.3 Industrial engineering (IE)

Industrial engineering deals with the optimization of complex processes or systems, and is concerned with the development, improvement, implementation and evaluation of integrated systems. It is also largely overlapped with systems engineering and operations research.

In the 18th and 19th century, many people tried to apply science to the design of processes and production systems. The efforts evolved into disciplines such as industrial engineering, production engineering, or systems engineering.

Originally, industrial engineering was mainly applied to manufacturing, that is, planning the layouts of factories and designing assembly lines and other manufacturing paradigms. Currently, it covers more diverse fields such as process, system, or organization.

The various topics are closely related to industrial engineering, some of them are included in industrial engineering itself. These are management science, financial engineering, engineering management, supply chain management, process engineering, operations research, systems engineering, ergonomics engineering, safety engineering, cost and value engineering, quality engineering, facilities planning, and the engineering design process.

3.4 Quality control (QC)

Quality control is a process to review the quality of all factors involved in production. It emphasizes testing of products to uncover defects and reporting to management who makes the decision to allow or deny product release.

The followings are examples of QC's practical steps. Every product is examined visually and often using a stereo microscope for fine detail before the product is sold into the external market. Inspectors will be provided with lists and descriptions of unacceptable product defects such as stain, small dent or color fading for example.

In QC activities, PDCA (plan–do–check–act) is used for the continuous improvement of processes and products. The PDCA cycle is a four–step model for carrying out change, and the cycle should be repeated consecutively for continuous improvement.

Total quality control (TQC) has been evolved, which is an approach that extends beyond ordinary quality control. It covers from research and development steps to maintenance of sold products.

4 Probabilistic safety assessment

In this chapter, brief explanations are given for the safety assessment and for the relation between the probabilistic safety assessment (PSA) and system reliability analysis methods.

Safety assessment is an interdisciplinary approach that focuses on the scientific understanding of hazards as well as harm, and ultimately the risks associated with them. There are two different kinds of approach for safety assessment, one is a deterministic and the other is a probabilistic approach.

The deterministic analytical procedure attempts to ensure that various situations and particular accidents have been taken into account, and that engineered safety and safeguard systems will be capable to prevent fatal accidents. It is assumed that operating incidents occur by potential equipment failures and human errors. As such then, verification that provisions are made to detect such incidents and designing safety systems will restore the plant to a normal state and maintain it under safe conditions.

Probabilistic safety assessment (PSA) has been developed in order to find out scenarios for hypothetical accidents that might result in, for example, severe core damage in nuclear power plant, and to estimate the frequency of such accidents.

The probabilistic approach is based on the idea that there is no perfect artificial system, and even multiple safety systems happen to reach simultaneous failures. Component failures, human errors, environmental conditions are considered as stochastic phenomena, and undesired system states are evaluated by their occurrence probability.

The first assessment carried out in the United States was the Reactor Safety Study (RSS: Rasmussen report) published in 1975[4]. In the RSS, the event tree (ET) method has been used for identifying possible scenarios to cause accidents (sequences). Failure probabilities of safety or safeguard systems have been evaluated by the fault tree (FT) analysis. The RSS quantitatively estimated the occurrence frequencies of accident sequences by the combination of ET and FT. The total core damage frequency and risks to surrounding people were evaluated by summing up accident scenarios.

After the Three Mile Island accident in 1979, recommendations were made that PSA should be used to supplement deterministic safety assessment procedures for nuclear power plants. Since that time, more than a hundred of generic and plant-specific PSA studies have been carried out in the OECD countries. These studies are of interest not only in determining the absolute value of the risk of damage to the reactor core, but also for the information they can provide about the various components of this risk and their relative weighting.

5 System reliability analysis methods

After the RSS, many analysis methods in addition to ET and FT have been proposed for more realistic and sophisticated analyses to be performed easily. They are used mainly for the assessment of nuclear power plant safety. Brief explanations are given for various kinds of system reliability analysis methods. If you find out a promising method for your analysis purpose, please examine more details by references.

5.1 Failure mode and effects analysis (FMEA)

Failure modes and effect analysis (FMEA) was developed in the 1950s and was one of the first systematic methods used to analyze failures in engineering systems.

An example of FMEA application is by the Ford Motor Company. The Ford sold a compact car named "Pint" from 1971. This car had design defects and produced deadly fires from spilled fuel in a rear-end collision. The California court gave decision of the compensatory damages of $2.5 million and punitive damages of $3.5 million against Ford in a car fire accident, partially because Ford had been aware of the design defects before production. This is when Ford introduced FMEA to the automotive industry for safety and regulatory consideration in the late 1970s.

The U.S. National Aeronautics and Space Administration (NASA) has used variations of FMEA in many NASA programs including Apollo, Viking, Voyager, Magellan, Galileo, and Skylab.

FMEA is a simple qualitative method to reveal possible failures and to predict the failure effects on the system. It is an inductive method. Start with a component to identify possible failure modes, and then investigate what will happen if this component fails. After the completion of the analysis, one can reveal the significant failure modes and important effects to system performance.

There is "failure modes and effects and criticality analysis (FMECA)" which is an extension of FMEA, and is somewhat a quantitative analysis method. In

the analysis, "criticality numbers" are evaluated, which are products of failure rates, failure mode ratio, conditional occurrence probability of severity and mission time duration. The procedures for conducting FMECA were well described in MIL standard [5].

Figure 1 is an example of FMEA worksheet, which has been developed for a safety analysis of elevator system. Considerations are made for single component base, that is, the other components are assumed to function perfectly. Therefore, FMEA is not suitable to finding out critical combinations of component failures.

Failure modes and effects analysis (FMEA)			
System	Elevator, Protection System for Running with Door open state	System/Block Diagram	Over all diagram, Electrical wiring diagram, Structural configuration
Date	20th June 2011	Discussion/Revision/Final approval	1st May 2011 / 25th May 2011, 5th June 2011 / not yet
Analyst	MATSUOKA Takeshi		

Number, Name of equipment	Component	Function	Failure modes	Potential cause	Potential effects of cause		Detection methods	Action taken	Severity of the failure effects	References
					Restricted effects	Overall effects				
2 Control system for Elevator movement	Control program for Movement	Door switch signal, Brake detection signal, Signal from distance detection system, Analyze the signals from judgment program and control normal condition	Fault Judgment Fault signal	Insulation failure, Short Degradation of elements, Aging,	Improper control signal is generated	Various kind of accidents	Abnormal operation	Component exchange	Very high, or Hazardous	Possible accidents of running with door open state and fall accident
	Watch dog timer		No output	Short, Degradation of elements, Aging,	Unable to detect program failure	Various kind of accidents	Abnormal operation	Component exchange	Very high, or Hazardous	Possible accidents of running with door open state, caged accident, and fall accident
3 Power source	Power source for motor	Supply power for the movement of case	No output	Short, Degradation of elements, Aging,	Cage does not move	Movement impossible, Caged accident	No operation	Component exchange, of repair	Very high	Sudden stop will produce accidents
	Power source to stadby type brake	Supply power to stadby type brake	No output	Short, Degradation of elements, Aging,	Impossible to release brake	Movement impossible,	No operation	Component exchange, of repair	Very high	
	Power source to safety system of Elevator	Supply electricity to safety system	No output	Short, Degradation of elements, Aging,	Impossible to operate safety system	Unable to correspond in emergency	Unusual operation	Component exchange, of repair	Small effects	No problem if usual operation is normal
	Breaker	Protection of excess current	Shut down	Leakage / Overheat	Unable to use power source	Movement impossible, Caged accident	Unusual operation	Component exchange, of repair	Very high	Sudden stop will produce accidents
4 Brake system	Normal operation type brake, Auxiliary brake	Safety hold cage at door open state	Braking power decrease	Oil adherence, wear-out	Unusual actuation of brake	Cage does not stop perfectly, Running with Door open state, fall accident	Unusual operation	Component exchange, of repair	Very high, or Hazardous	Redundant system by Normal operation type brake and auxiliary brake

Fig. 1 Example of FMEA worksheet.

5.2 Hazard and operability analysis (HAZOP)

HAZOP is based on a theory that assumes risk events are caused by deviations from design or operating intentions. Identification of such deviations is facilitated by using sets of “guide words” as a systematic list of deviation perspectives.

HAZOP was developed by ICI company UK in 1970s. Details pertaining to the HAZOP methodology are found within IEC International Standard[6]. The procedure makes tables similar to FMEA, and find out the cause of deviation, and the effects to system. It is a systematic and comprehensive methodology.

The starting point of a HAZOP is the search for possible deviations from design intention. Then the search becomes bidirectional: in one direction to find the possible causes of the deviation and in the other to deduce the likely hazardous consequences. On the other hand, a FMEA is unidirectional: on identifying a possible component failure, it proceeds to investigate the likely consequences on the system.

Neither HAZOP nor FMEA is likely to uncover all hazards. It is difficult to find out a possible deviation from design intent on an interaction between two components. In general, the complementary use of HAZOP and FMEA on the same system offers improved thoroughness and efficiency.

5.3 Reliability block diagram (RBD)

RBD performs the system reliability and availability analyses on large and complex systems using block diagrams to show network relationships. The structure of the reliability block diagram defines the logical interaction of failures within a system that are required to sustain system operation. Once the block diagrams are configured properly and data is provided, the failure rate, MTBF, reliability, and availability of the system can be calculated.

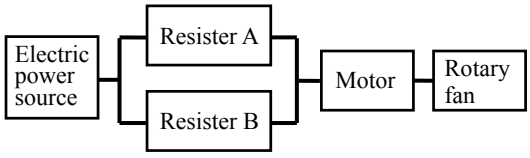


Fig. 2 Example of a reliability block diagram.

Reliability block diagrams often correspond to the physical arrangement of components in the system. Figure 2 illustrates a very simple example of a RBD. Parallel paths represents redundant, meaning that all of the parallel paths must fail for the parallel line to fail. In the Fig. 2 above, an “open” failure of resister A does not produce the system failure. The system fails, vide infra, if resister A has the "fail short" mode of failure. Physical layout of two resistors is in parallel, albeit the reliability block diagram would be composed of two series blocks for the "fail short" mode. In certain cases, reliability block diagrams do not correspond to the physical arrangement of components in the system.

5.4 Markov model

Markov process, named after the Russian mathematician Andrey Markov, is a time-varying random phenomenon for which the Markov property holds. The Markov property, or memorylessness, is one for which future state will depend on the present state, and not of the states in before time.

Markov model is used to describe and analyze the movement of a system among various states. The movement can be described as shown in Fig. 3. In this case, a system is composed of two components and there are four possible system states. Success sate of a component is represented by "0", and failure is represented by "1".

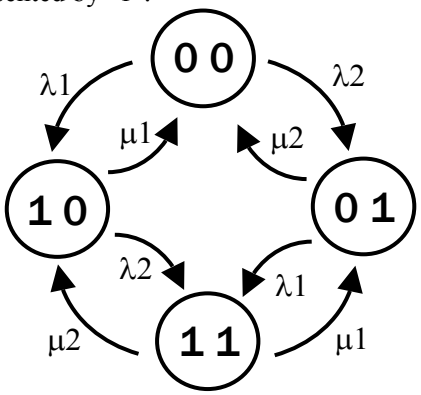


Fig. 3 Example of a Markov diagram.

Markov model is a quantitative analysis technique and suitable for analyzing systems with complicated maintenance policies and possible dependencies between components.

A Markov model can calculate: the probability that the system is in a specific state at a given time, the distribution of steady state after long time operation, the average time the system stays in specific state, the average number of times the system visits specific state during certain time duration, and also the average time the system reaches a specific state.

5.5 Event tree analysis (ETA)

Event-tree (ET) / fault-tree (FT) methodology is the most popular approach to probabilistic safety assessment (PSA)[7]. An event tree is a graphical representation of the logic model that identifies and quantifies the possible outcomes following an initiating event.

ETA is an inductive procedure that shows all possible outcomes resulting from an initiating event, taking into account whether installed safety barriers are functioning or not, as well as additional events and factors. By studying all relevant initiating events, which have been identified by some other technique, the ETA can be used to identify all potential accident scenarios and sequences in an intricate system.

Design and procedural weaknesses can be identified, and probabilities of the various outcomes from an initiating event can be determined.

5.6 Fault tree analysis (FTA)

Fault tree analysis method was developed by Bell Telephone Laboratories in 1962 when they performed a safety evaluation of the Minuteman Launch Control System. The Boeing Company further developed the FTA technique and made use of computer programs for both quantitative and qualitative analysis.

Fault trees use a deductive approach as they are constructed by defining TOP events (undesired event) and then use backward logic to define causes. Event tree analysis and fault tree analysis are, however, closely linked. Fault trees are often used to quantify system events that are part of event tree sequences[8].

FTA shows the relation between the system failure (TOP event) and failures of the components (basic events) of the system. A basic event is not restricted to a pure component failure, but it may also represent human error or external loads. As the constructed diagram assumes a tree-like structure, it thus bears its name as a fault tree analysis.

5.7 GO methodology

The GO method[9] is a success-oriented system analysis that uses seventeen operators to aid in model construction. It was developed by Kaman Sciences Corporation during the 1960s for reliability analysis of electronics for the Department of Defense in U.S.

The GO methodology is an effective method of system reliability analysis and can be used in the repairable system. The GO model can be constructed from engineering drawings by replacing system elements with one or more GO operators. With the probability data for each operator, the probability of successful operation of the system can then be calculated.

The GO method is used in practical application where the boundary conditions for the system to be modeled are well defined by a system schematic or other design documents. However, the failure modes are implicitly modeled, making it unsuitable for detailed analysis of failure modes beyond the level of component events. Furthermore, it does not treat common cause failures nor provide minimum cut sets regarding the system.

5.8 Petri net

A Petri net is a mathematical modeling for the description of distributed systems. Petri net was invented in 1939 by Carl Adam Petri at the age of 13. Petri net is a directed bipartite graph, in which the nodes represent transitions (*i.e.* events that may occur, signified by bars) and places (*i.e.* conditions, signified by circles).

Petri nets are a promising tool for describing and studying information processing systems that are characterized as being concurrent, asynchronous, distributed, parallel, nondeterministic and/or stochastic. As a graphical tool, Petri nets can be used as a visual-communication aids similar to flow charts, block diagrams, and networks. In addition, tokens are used in these nets to simulate the dynamic and concurrent activities of systems[10]. Petri nets can be applied to PSA[11].

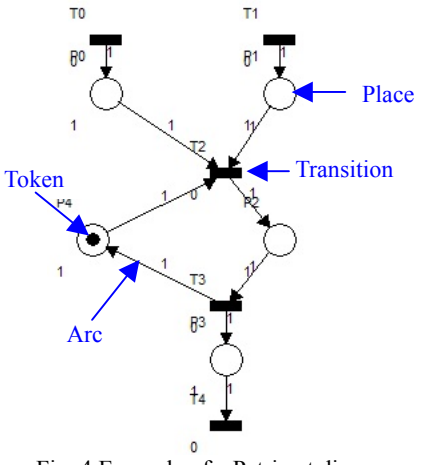


Fig. 4 Example of a Petri net diagram.

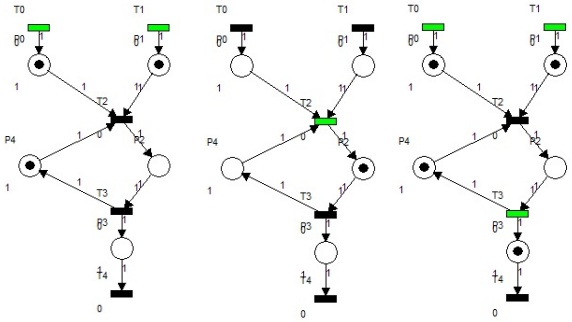


Fig. 5 Movement of tokens in Petri net diagram.

Figure 4 is an example of Petri net diagram. If all the places directed to one transition are filled with tokens, the transition fires and tokens disappear, and new token(s) appear in the connected places. From the initial state of the Fig. 4, this Petri net continues to produce token endlessly as shown in Fig. 5. "Fire" is indicated by green color transitions.

5.9 Bayesian network (BN)

BN is also a directed acyclic graph, in which the nodes represent events and arc connects events. It can calculate the occurrence probabilities of events represented by a node based on Bayesian method. Each node is associated with a probability function that takes as input a particular set of values for the node's parent variables and gives the probability of the variable represented by the node.

The BN can be used to find out updated knowledge of the state of a subset of variables when other variables (the evidence variables) are observed. This process of computing the posterior distribution of variables given evidence is called probabilistic inference. A Bayesian network can thus be considered a mechanism for automatically applying Bayes' theorem to complex problems[12].

Figure 6 is an example of a Bayesian network which expresses the probabilistic relationships of blood type between families. With the updated knowledge of one person's blood type, other members' blood type can be estimated. ET, FT can be also expressed by BN with more simple form. Large number of sequences can be handled by conditional probability.

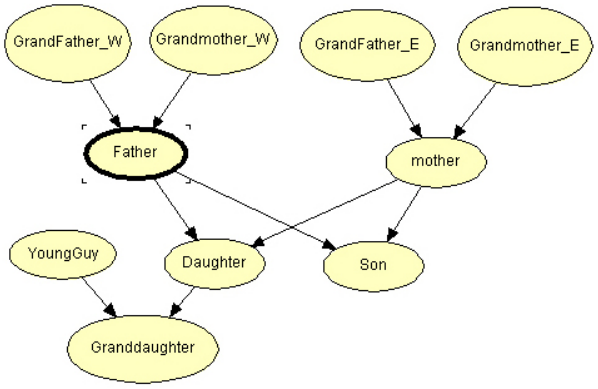


Fig. 6 Example of Bayesian network.

5.10 Digraph matrix

Digraph matrix is a graphical combinatorial failure space model of a system. The model consists of nodes and AND gates connected by directed edges. Cycles, or directed loops are permitted in the models. Each node represents a failure. The digraph edges show how the occurrence of a failure can flow through the system to cause other failures.

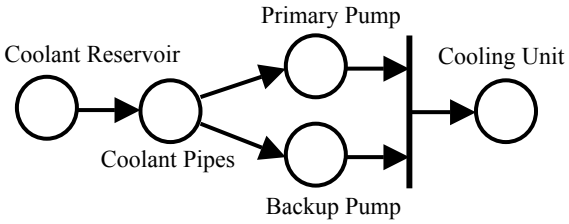


Fig. 7 Example of a Digraph matrix.

AND gates are drawn as bars, and nodes are drawn as circle as shown in Fig. 7. Digraph nodes can be in one of two states, true or false. If a node is true (= marked), it means the failure has occurred.

Digraph solution algorithm developed at NASA/Ames Research Center was applied to the Space Shuttle and Space Station Freedom programs as real time diagnosis applications[13].

5.11 Dynamic event tree

Conventional ET is a quasi-static approach and based on a few thermal-hydraulic calculations, for the most conservative/limiting case.

Dynamic event tree treats the interaction of system dynamics and stochastic in the evaluation of accident consequences and their conditional probabilities. It is continuous in time/state space, that is, continuous transitions are assumed. Branches occur in time-variable phase space as shown in Fig. 8.

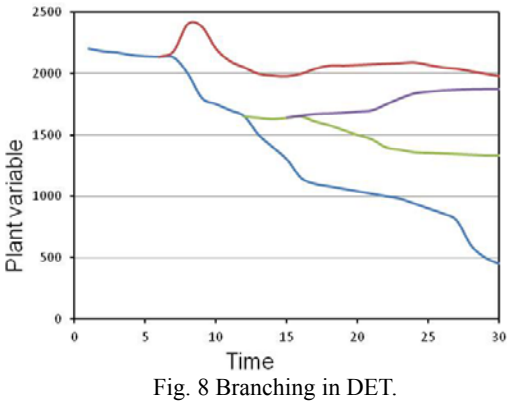


Fig. 8 Branching in DET.

Plant sate is obtained by thermo-hydro dynamic simulation Codes and combined with system transition condition. Dynamic event tree approach is a new approach to model and analyze dynamic interactions between plant, automatic systems, and operators[14].

5.12 Goal tree-success tree (GTST)

Complex systems can be best described by hierarchical frameworks. The GTST modeling is a functional decomposition framework to describe and model complex physical systems in terms of objects, relationships, and qualities. Where, "qualities" are functions and goals, "objects" and "relationships" can be represented by success trees and the master logic diagram (MLD) using logic (Boolean, physical, and fuzzy logic)[15]. Related works such as multilevel flow modeling (MFM)[16] deals with functional flow modeling in complex systems.

The GTST may be applied to show not only 'how' the system works, but also 'how well' it works. It can be applied to the analyses of capability, availability, reliability, and efficiency. In the dynamic applications, the time-dependent changes can be considered in the GTST.

A GTST is a functional hierarchy of a system starting with an 'objective' at the top. The objective describes, in an unambiguous term, the principal purpose of the system.

The decomposition can proceed to a point where system functions/sub functions have been sufficiently described such that the purpose of each physical part of the system can be explicitly and unambiguously described.

The role of the success tree (ST) in the GTST is to describe the system structure as it relates to the physical functions described in the GT part. The relationships between various nodes of a GTST are expressed through a special AND/OR gate. Unlike conventional AND/OR gates, in most cases the loss of a sub function does not necessarily mean an immediate loss of the parent function. However, the parent function will be lost after some time has elapsed.

5.13 Continuous event tree

Continuous process variables are combined with discrete system states and operator's condition[17]. Evolution of system state is simulated by semi-Markov model and system state is expressed as trajectory in a phase space. In such cases, then it is called continuous event tree.

5.14 Discrete event simulation

Discrete event simulation is rather a general methodology used in various fields. It has been widely used to model and evaluate computer and engineering systems.

The system state is assumed to instantaneously change at discrete time points. The change of the state is called "event". After an event a new system state is maintained for certain time duration. The operation of a system is represented as a chronological sequence of events.

Discrete event simulation can quantitatively represent the real world, simulate its dynamics on an event-by-event basis, and evaluate detailed performance.

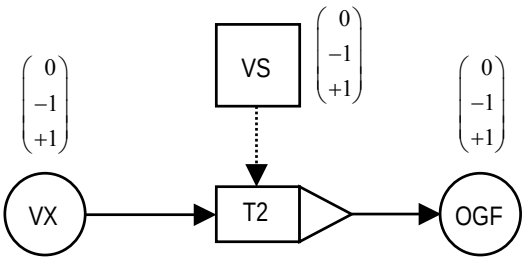
It can be applied to system reliability analysis, and there is an example of the application in nuclear fields[18].

5.15 Dynamic flowgraph methodology (DFM)

The dynamic flowgraph methodology (DFM) [19] is an analytical technique for the safety analysis of control systems. The DFM explicitly represents the cause-and-effect and timing relationships between key components and parameters and the state of these parameters.

Figure 9 shows an example of a cause relationship expressed in DFM. The process variable node (circle:VX) represents physical and/or software variables, such as pressure in a tank. The variable is typically discretized into a finite number of states (0,-1,+1 in this case). Causality edge (arrow) is used to connect process variable nodes to indicate the existence of a direct cause-effect relationship between the variables described by the nodes. The exact nature of the relationship between the nodes is

defined by a transfer box (T2). The transfer box is used to symbolize the existence of a transfer function which is defined in an associated decision table.



OGF: Gas outflow through valve, VX: Valve position, VS: Condition

Fig. 9 Causal relationship expressed in DFM.

Condition edges (dotted arrow) is used to link condition nodes (square: VS) to transfer boxes. Its presence indicates the existence of multiple versions of the transfer function depending on the value taken by the condition node. A condition node represents physical and/or software parameters. They are used to represent component failure states, changes in modes of operation, *etc*. Any condition node which is not linked upstream to a process variable node is treated as a random variable.

Moreover, transition box is defined, which is associated with decision tables and time lags between input and output variable nodes.

The DFM has been used for the safety analysis of aerospace and nuclear systems. It lacks the capability to represent the stochastic characteristics of the system components. On the other hand DFM possesses the clear benefit of calling the attention of the analyst to the physics of the problem.

5.16 Cell-to-cell mapping technique (CCMT)

The CCMT is a systematic procedure to describe the dynamics of both linear and non-linear systems in discrete time and discretized system state space.
It provides a very effective means to account for epistemic uncertainties, non-linear aspects of the system dynamics and stochastic fluctuations in dynamic system operation[20].

The CCMT produces a model that is compatible with the conventional discrete-state Markov approach for representing hardware/software/firmware failures. A system stochastically evolutes through the transition probabilities among the possible system states in a user specified time intervals.

The transitions between the states (nodes) can be represented graphically by directional links (edges). They are identified by the topology of the underlying user-constructed system model that describes the system behavior.

Figure 10 shows the image of system state transition in a phase space. CCMT provides risk-analytical capabilities that supplement those provided by traditional probabilistic safety assessment (PSA) techniques for nuclear power plants.

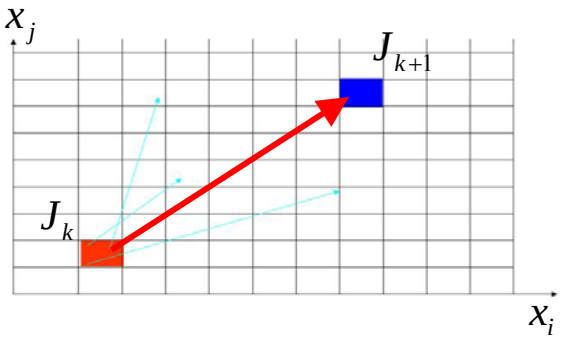


Fig. 10 System state transition in CCMT.

5.17 Dynamic logical analysis methodology (DYLAM)

The DYLAM also combines physical behavior of a system with the probabilistic phenomena: random transitions in the component states (nominal, failed on, failed off, stuck, *etc*.). All the knowledge of the physical system under study is contained in a numerical simulation[21].

Once the simulation program is linked to the DYLAM code, becoming a subroutine of the DYLAM program, this drives the simulation, with a time loop, taking into account the time history of the logical states of the components by assigning initial states.

Top conditions of the system (top event in the DYLAM terminology) can thus be analyzed very easily in terms of process variable values, such as "temperature above a certain value" or "'pressure

below a given threshold". Many top conditions can be analyzed simultaneously.

One characteristic of DYLAM is to follow all the different paths resulting from the initial states of the components of the system and from transitions in-time of the component states and to drive the corresponding simulations.

For each path a time-dependent probability of the system is evaluated, so that the probability of occurrence of a certain top event is simply obtained by adding the probability of the corresponding top sequences.

Owing to its dynamic features, the DYLAM analysis can be deemed a complementary to the ET-FT techniques when the detailed modeling of complex scenarios or the assessment of time dependent top probabilities is needed.

The DYLAM has been applied to nuclear, chemical and aeronautical domain, by introducing human errors. It has been also applied to the dynamic reliability analysis of a Boeing 747 executing the approach to landing procedure.

5.18 GO-FLOW methodology

The GO-FLOW is a success oriented system analysis technique, and is capable of evaluating a large system with complex operational sequences. The modeling technique produces a chart which consists of signal lines and operators, and represents the engineering function of the components/ subsystems/ system [22].

The operators model function or failure of the physical equipment, logical gates, and a signal generator. Fourteen different types of GO-FLOW operators are currently defined. Specific probabilities of component operations or failure are given as input data of GO-FLOW chart information. A finite number of discrete time values (points) are required to express the system operational sequence. Figure 11 shows an example of a GO-FLOW model which expresses a simple lamp system.

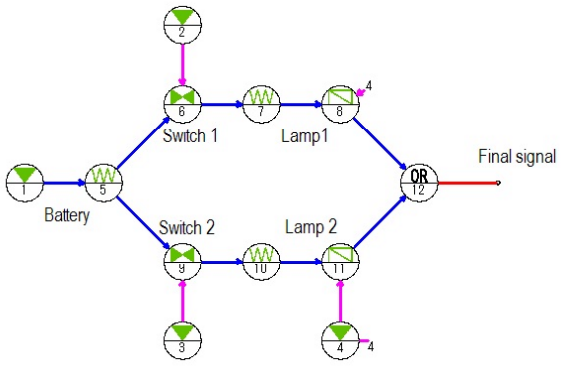


Fig. 11 An example of GO-FLOW chart.

An analysis is performed from the upstream to the downstream signal lines. In most cases, only one, or at most few of all the defined signals are of interest (final signals). An analysis is completed when the intensities of final signals at all the time points are obtained.

The GO-FLOW methodology is a valuable and useful tool for system reliability analysis and has a wide range of applications. Recently an integrated analysis framework of the GO-FLOW has been developed for the safety evaluation of elevator systems under the contract of the Ministry of Land, Infrastructure, Transport and Tourism, Japanese Government [23].

5.19 Summary of the system reliability analyses

Many system reliability analysis methods have been proposed. Some of them are traditional and well known methods while some of them are newly developed for special purposes. Table 3 shows the main characteristics of these methods for the reader's convenience.

6 Summary

In this article, overall explanations are given for a plethora of matters relating to system reliability analysis. They include systems engineering and related technological fields, such as operations research, Industrial engineering.

Many system reliability analysis methods incorporating advanced methods are explained. If you find out a promising method for your analysis purpose, please examine more details by references.

More details on plausible analysis methods can be found in the references. The findings presented herein are the essence obtained in my research activities. It is the author's hope that the paper can serve as a reference for the reader's future research activities.

7 Answer of the questions

(Question 1) 2 dollars
(Question 2) 0 dollar
(Question 3) 1.2 dollars
(Question 4) If strong and slowdown economical conditions are evenly expected, the aggressive policy gives the expected value of profit as 3.5 (= 0.5×10 + 0.5×(-3)). Negative policy also gives the same value 3.5 (=0.5×5 + 0.5×2). Therefore, if the president has confidence that economical conditions will be strong, he should select the aggressive policy.

Table 3 Summary of system reliability analysis methods

Methods	Qualitative /Quantitative	Graphical /Table/Others	Deterministic /Probabilistic	Relation to PSA	Characteristics and Limitations
FMEA	Qualitative	Table		Pre-analysis	Do not treat combination of component failure
FMECA	Quantitative		Probabilistic		
HAZOP	Qualitative				
Reliability Block Diagram	Qualitative & Quantitative	Graphical	Probabilistic	System analysis	Not precisely expressed logical combination
Markov Model	Quantitative	Graphical & Mathematical	Probabilistic	System state analysis	Not practical
Event Tree				Scenario analysis	Difficult to treat dependent failure
Fault Tree				System analysis	Difficult to treat time dependency and phased mission problem
GO					Success oriented, No information of minimum cut sets
Petri net	Qualitative	Graphical	Stochastic /Deterministic	System state analysis	Complex system dynamics can be simulated
Bayesian Network	Quantitative	Graphical & Mathematical	Probabilistic	Possible to both scenario and system analysis	Bayesian inference is possible
Digraph Matrix	Qualitative	Graphical	Deterministic	System state analysis	This method was used by NASA
Dynamic event tree	Quantitative	Graphical & Mathematical	Probabilistic	Scenario analysis	Combination with thermo-hydro dynamic simulation
Goal tree – Success tree				System analysis	Success oriented, Time evolution can be considered
Continuous event tree		Mathematical		Scenario analysis	Phase space consideration Semi-Markov model
Discrete event simulation					General method
DFM		Graphical & Mathematical		System analysis	Decision tables are necessary, not possible to model stochastic characteristics of components
CCMT					Phase space consideration Markov approach
DYLAM		Mathematical		Scenario analysis	Combination with thermo-hydro dynamic simulation
GO-FLOW		Graphical & Mathematical		System analysis	Success oriented, Dynamical analysis

References

[1] GREEN, A., and BOURNE, A.: Reliability Technology, New York, John Wiley & Sons, 1972.

[2] VON NEUMANN, J., and MORGENSTERN, O.: Theory of Games and Economic Behavior, New Jersey, Princeton University Press, 1944.

[3] MARTIN, J., OSBORNE, M. J., and RUBINSTEIN, A.: A Course in Game Theory, Cambridge, MIT Press, 1994.

[4] U. S. NUCLEAR REGULATORY COMMISSION: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, NUREG-75/014, 1975.

[5] MIL-STD-1629A: Procedures for Performing a Failure Mode Effect and Criticality Analysis. Department of Defense (USA), November 1980.

[6] BRITISHI STANDARD BS: IEC61882:2002 Hazard and Operability Studies (HAZOP studies) - Application Guide British Standards Institution, 2002.

[7] U. S. NUCLEAR REGULATORY COMMISSION: An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants, Appendix I Accident Definition and Use of Event Tree, WASH-1400, NUREG-75/014, 1975.

[8] U. S. NUCLEAR REGULATORY COMMISSION: An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants, Appendix II Fault Tree Methodology, WASH-1400, NUREG-75/014, 1975.

[9] GATELY, W. V., and WILLIAMS, R. L.: GO Methodology Overview, EPRI NP-765, 1978.

[10] MURATA, T.: Petri Nets: Properties, Analysis and Applications, Proceedings of the IEEE, 77, 1989: 541-580.

[11] KOHDA, T., and INOUE, K.: A Petri Net Approach to Probabilistic Safety Assessment for Obtaining Event Sequences from Component Models, in "Probabilistic Safety Assessment and Management, Vol.1 and 2", G. Apostolakis(ed.), New York, Elsevier, 1991:729-734.

[12] JENSEN, F. V.: Bayesian Networks and Decision Graphs, New York, Springer, 2001.

[13] IVERSON, D. L., and APATTERSON-HINE, F. A.: Advances in Digraph Model Processing Applied to Automated Monitoring and Diagnosis, Reliability Engineering and System Safety, 1995, 49:325-334.

[14] METZROTH, K., DENNING, R., and ALDEMIR, T.: Dynamic Event Tree Analysis as a Risk Management Tool, Proceedings of the American Nuclear Society (ANS) ICAPP 2010, Topical Meeting International Congress on Advances in Nuclear Power Plants, San Diego, 2010.

[15] MODARRES, M., and CHEON, S. W.: Function-Centered Modeling of Engineering Systems Using the Goal Tree–Success Tree Technique and Functional Primitives, Reliability Engineering and System Safety, 1999, 64:181–200.

[16] LIND, M.: An Introduction of Multilevel Flow Modeling, Nuclear Safety and Simulation, 2011, 2:22-32.

[17] DEVOOGHT, J., and SMIDTS, C.: Probabilistic Dynamics as a Tool for Dynamic PSA, Reliability Engineering & System Safety, 1996, 52:185–196.

[18] MCINTYRE, T. J., and SIU, N.: Electric Power Recovery at TMI-1 A Simulation Model, Proceedings of International ANS/ENS Topical Meeting on Thermal Reactor Safety, San Diego, U.S.A., 1986, VIII.6-1～7.

[19] YAU, M., GUARROD, S., and APOSTOLAKIS, G.: Demonstration of Dynamic Flow Graph Methodology using the Titan II Space Launch Vehicle Digital Flight Control System, Reliability Engineering & System Safety, 1995, 49:335–353.

[20] BELHADJ, M., and ALDEMIR, T.: Some Computational Improvements in Process System Reliability and Safety Analysis using Dynamic Methodologies, Reliability Engineering & System Safety, 1996, 52:339–347.

[21] COJAZZI, G.: The DYLAM Approach for the Dynamic Reliability Analysis of Systems, Reliability Engineering and System Safety, 1996, 52:279-296.

[22] MATSUOKA, T., and KOBAYASHI, M.: GO-FLOW A New Reliability Analysis Methodology, Nuclear Science and Engineering, 1988, 98:64-78.

[23] MATSUOKA, T.: GO-FLOW Methodology -Basic Concept and Integrated Analysis Framework for its Applications, Nuclear Safety and Simulation, 2010, 1:198-206.