Quality Assurance and Prevention of Problems

Kazuyuki Suzuki
University of Electro-Communications, Tokyo, Japan,
suzuki@se.uec.ac.jp

We must make every effort to prevent serious problems of reliability and safety. The key to such prevention is "prediction" and "up-stream management." There are two approaches to prediction: induction and deduction. The inductive approach includes (1) sharing experiences and histories, (2) abstraction and generalization of individual problems, and implementation of the PDCA cycle, and (3) utilization of incident information. The deductive approach is based on scientific theory and engineering technology. And these two approaches are integrated by "up-stream management" of executive leadership, and "systems approach" which consists of seven viewpoints for prediction: purpose (desired functions), mechanisms needed to achieve desired functions, input items, internal and external stresses, failure mechanism, failure mode & top event mode, and effect. Focusing on top event mode, a procedure of preventing problems and a new scheme of reliability engineering methods are proposed.

Keywords: reliability, safety, upstream management, prediction, top event mode

1. Introduction

1.1. Quality assurance

For companies and organizations to continue growing and developing, they must supply customers and society with sufficient satisfaction and safety. They must satisfy not only the emerging needs of customers and society but also the potential needs. This means that it is necessary to create products and provide services that satisfy both customers and society, following the steps indicated in Fig. 1. However, a sudden and unexpected failure in a product or system due to a new "creation" could result in the loss of functionality and safety, which could trigger a serious accident that greatly affects society. Recently, along with social or economic change, technology has rapidly progressed, and products and systems have complicated. In addition, emerging countries' economies have been growing. It needs to create products in accordance with social conditions and necessities in the ages without spoiling reliability and safety. It is essential to ensure the reliability and safety for any product.

According to Japanese Industrial Standard (JIS) Z 8101-1981, quality assurance is defined as "systematic activities by producers to ensure the product quality demanded by customers." In order to create the product demanded by customers and society, it is important to investigate their needs. To meet them, it is necessary to do the following three "E"s in particular.

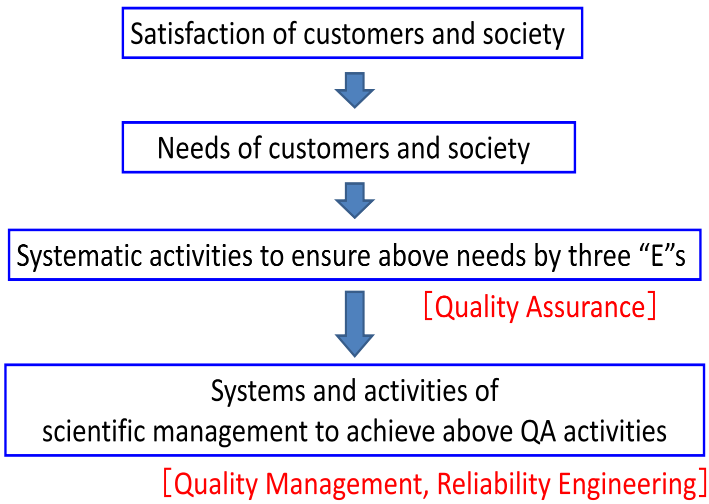

Fig 1. Relationships among quality assurance, quality management and reliability engineering

- Establish "Process" to satisfy customers' satisfaction

  After grasping the needs of customers and society, establish a process for planning, designing and manufacturing products and services that meet the needs of customers and society.

- Execution of the process and Verification & Validation

  The observance of the process is not a negligible matter. Therefore, a company should definitely follow the process. As shown in Fig. 2, not only that the product or service conforms to the specifications ("verification"), but also that the needs of customers and society are satisfied ("validation") from the viewpoints of *genba* (actual work place), *genbutsu* (real item), and *genjitsu* (actual situation) before shipping the product or providing the service is important. If the needs are not satisfied, emergency measures to correct the problem and prevent recurrence should be implemented promptly.

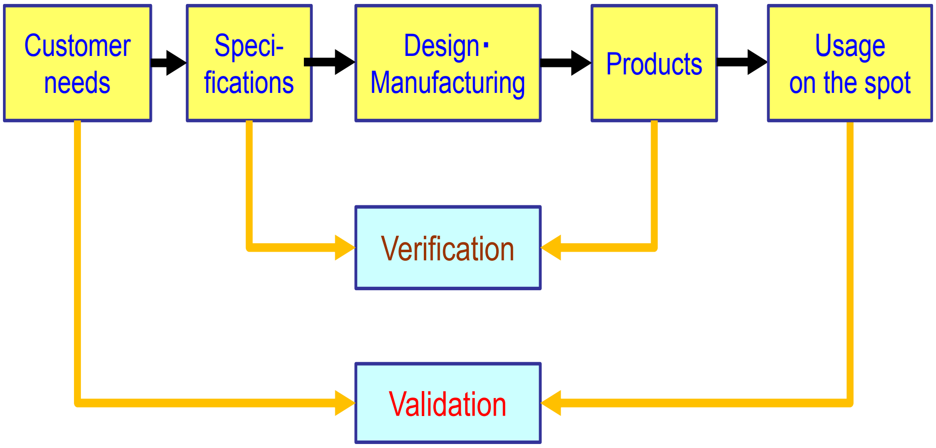

Fig 2. Verification for Specifications and Validation for Customer Needs

Kume, H.(2014), ed. By Kazuyuki Suzuki, New Reliability Handbook, JUSE Press

- Evidence for the third party

  It should be stated what kind of needs would be satisfied as a contract between a company and its customer. To show the evidence that the contract is being kept gives a sense of reliability and safety to the customers and society.

Even though ISO-9000 focuses on "evidence for the third party", quality assurance in Japan refers not only "evidence for the third party", but all three "E"s in a broad sense. Quality control and reliability engineering are kinds of scientific management systems and activities for effectively and efficiently achieving "quality assurance" that covers the three "E"s.

1.2. Ensuring reliability and safety and preventing problems

Three activities are necessary to ensure reliability and safety during a product's development, production, and usage phase:

- Prevention of problems
- Prompt and appropriate response
- Prevention of recurrence.

As shown in Fig. 3, they should be correspondingly supported by

- An "organization" for bringing together personnel within an organization
- A "system" that encourages cooperation among all departments without vertical or hierarchical limitation, with a quality assurance system as its core
- A "society" comprising cooperative customers, administrative organizations, and industries.

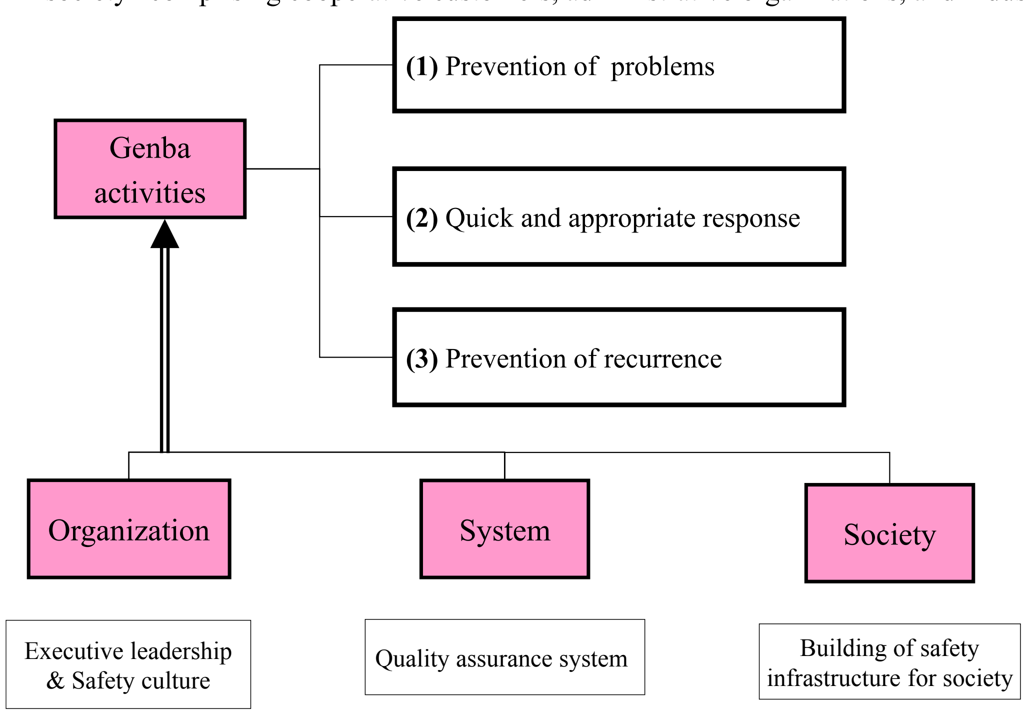

Fig. 3 Scheme for achieving reliability and safety

It is said that most problems, especially quality problems, are preventable during product development if the relevant executives are committed to solving quality problems and if the quality of products is comprehensively and collaboratively examined by all departments during the planning phase. In other words, “upstream management” that provides sufficient planning and designing for development of products during the upstream phase is vital to ensuring reliability and safety. By utilizing the knowledge and ability of an organization based on a quality assurance system, we should accurately grasp the information related to *genba* (actual work place), such as potential and emerging user needs, technology, commodity market trends, usage methods, and environmental condition. We can then determine a quality policy and quality target. To collect and share information beyond department boundaries during the upstream phase holds the key to achieving reliability and safety.

Generally it is impossible to prevent problems that cannot be predicted. In other words, we can prevent problems, detect signs of problems, and prevent or lessen the unfavorable effects of problems if we can predict the undesirable “fatal event” occurring on products or systems in future. In addition, we can take countermeasures if we understand the mechanism that is causing the problem in a product or its constituent elements that may lead to a serious situation. It is said that 90% of the problems related to product development are due to the inability to predict problems in advance (in the case of failure modes and effects analysis (FMEA), this corresponds to not being able to detect the failure mode, ref. §3.2). It is also said that 95% of the problems are preventable if the failure mode is detectable. This leads to three important points:

(i) Try to predict
(ii) Predict effectively and efficiently
(iii) Share information about successful problem prevention due to prediction.

It is easy to implement (i) and (iii) by the executive leadership, but implementing (ii) is difficult.

This paper presents two approaches to prediction: an inductive approach and a deductive approach. It also describes upstream management and a systems approach that integrates the two proposed approaches. The aim of the inductive approach is to prevent problems by generalizing, abstracting, and sharing information acquired through the investigation of past problems, focusing on three aspects: *genba*, *genbutsu*, and *genjitsu*. The aim of the deductive approach is to prevent problems on the basis of predicting potential problems from scientific principles and theories. The systems approach examines the secureness of reliability and safety during the upstream phase, starting from the purpose of the product or system, and predicts problems by integrating the inductive and deductive approaches during the development phase.

2. Preventing Problems on basis of Prediction

Implementation of these approaches to preventing problems should take into consideration the followings.

A: Inductive Approach

A1) Prevention by sharing problem-related information beyond organizational boundaries

A2) Prevention by thoroughly performing the plan-do-check-act (PDCA) cycle

A3) Prevention by utilizing incident information

B: Deductive Approach

B1) Prevention based on the deductive approach

2.1. Prevention by sharing problem-related information beyond organizational boundaries

Problems can be categorized as

a) Experienced in the past

b) Not experienced.

Furthermore, b) can be divided into four categories:

b1) Not experienced by self
(Others may have experienced it)

b2) Not experienced by team or organization to which individual belongs
(Other teams or organizations may have experienced it)

b3) Not experienced by type of industry
(Other types of industry may have experienced it)

b4) Not experienced by any type of industry, or country

Most problems can be categorized as a), b1), b2), or b3). This means that it is important to share problem experiences between organizations to enable lessons to be learned from them so that future success can be achieved. First of all, we should consider taking measures for problems categorized as a), b1), b2), or b3) and then for those categorized as b4).

We need to collect information on problems and failures categorized as a), b1), b2), and b3), investigate the mechanism of problem occurrence with the help of individual's knowledge and expertise from various departments, share the collected information, and then implement three measures aimed at

"Preventing problem occurrence"

"Detecting problems early"

"Preventing unfavorable effects."

The important point is how organizations take into consideration individual failure and success regarding problem prevention for future improvement. For example, organizations should question whether the database (DB) on past failures and successes is up-to-date. Instead of relying on someone (such as development designers) checking the DB, a system and process should be implemented for automatically extracting information on past failures and successes. It is equally important to devise a method that prevents advancing to the next step.

2.2. Prevention by thoroughly performing PDCA cycle

A process should be implemented for tracing back to the mechanism and system, analyzing the cause of each problem in the past, and preventing recurrence on the basis of the analysis. This process should be standardized, and this standardization should be applied to every company. This will enable companies to take appropriate measures when the same or similar problems occur in the future. The basis for this is the PDCA cycle.

The P (plan) of PDCA consists of "purpose" and "process standard." "Process standard" is defined as

I. Criteria

for example

i) Design criteria, safety criteria

ii) Evaluation criteria, reliability criteria

iii) Applicable criteria of error proofing, fail safe, etc.

i), ii), and iii) are determined on the basis of a quantitative measure for achieving the purpose

II. Establishment of a means for achieving the process standard

A method, procedure, and system of technical standards, design rules, etc.

It is essential to work on accumulating expertise, knowledge, and experience related to standardization and to implement the PDCA cycle by sharing the acquired information with others.

2.3. Prevention by utilizing incident information

Industrial accidents are said to obey Heinrich's Law: for every accident that causes a fatal or serious injury, there are 29 accidents that cause not fatal but serious injuries such as fracture and 300 accidents that cause scratch. This ratio of 1:29:300 is the same for problems related to reliability and safety. Before the occurrence of serious accidents related to reliability and safety, it is necessary to sensitively collect much incident information that corresponds to scratch and then establish systems for detecting signs of serious accidents from the collected information as quickly as possible. Technical standards and evaluation criteria should be examined, and swift action should be taken when signs of impending serious problems are detected.

2.4. Prevention based on deductive approach

In most cases, problems can be predicted on the basis of the environment and usage conditions. In other words, the stress-failure mechanism-failure mode should be changed from implicit knowledge to explicit knowledge, which should be organizational knowledge that can be shared and used practically. Please refer to Suzuki (2004). Table 1 shows a list of "the stress-failure mechanism-failure mode" focusing on temperature and humidity. For more information, refer to Suzuki (2004).

Table 1. Stress-failure mechanism-failure model

Stress (Usage, Environmental condition)		Failure Mechanism				Failure mode
Large classification	Small classification	Large classification	Small classification	Phase I (Micro)	Phase II	Phase III (Marco)
Temperature + humidity	High humidity + high temperature	Corrosion	Local corrosion	Generation of a pit	Acceleration by battery action	Fissure, crack, fracture
			Concentration cell corrosion	The fall of local dissolved oxygen	Formation of a concentrated cell	Fissure, crack, fracture
		Moisture absorption	Hydrolysis	Generation of hydrophilic group	Water absorption	Fissure, crack, fracture
	High humidity + normal temperature		Mold	Decomposition	Bad insulation	Fissure, crack, fracture
	High humidity + temperature cycle		Dew formation	Water obsorption	Insulation resistance degradation	Short circuit
			Suction phenomenon	Pressure difference	Ingress of water/gas	Power down

3. Systems Approach with Seven Viewpoints for Prevention

3.1. Predicting problems

The development of systems and products starts with setting the purpose and defining the function, followed by determining ways to achieve it ①. Next, development and design are performed to realize the function. In other words, a functional achievement mechanism is pursued ②. Then, consideration must be given to what kind of items such as Material, Machine, Man, Energy can fulfill the functional mechanism ③. In the process of achieving the function, a combination of internal stresses, such as those due to heat and humidity, and the external stress caused by environmental conditions and other factors can bring about a physical, chemical, and/or metallic change, leading to failure ④. This process is called the “failure mechanism” ⑤, and a failure configuration that can be detected from outside is called a “failure mode” ⑥-1. A failure mode advances to a “top event mode” ⑥-2, which can cause a serious accident or failure. Moreover, it has a negative effect on people ⑦-1. The effect on the environment should also be considered ⑦-2 as well as the effect on function and performance ⑦-3.

That is, it is essential to focus on the process (See Fig.4):

① Purpose and function
② Functional achievement mechanism
③ Item
④ Stress
⑤ Failure mechanism
⑥ -1 Failure mode
  -2 Top event mode
⑦ Effects on people, environment, and function & performance

It is important to be able to predict what kind of problems may occur on the basis of fundamental scientific principles. Although these seven viewpoints are important for achieving reliability and safety and preventing the occurrence of problems, this paper focuses on "top event mode" and "failure mode."

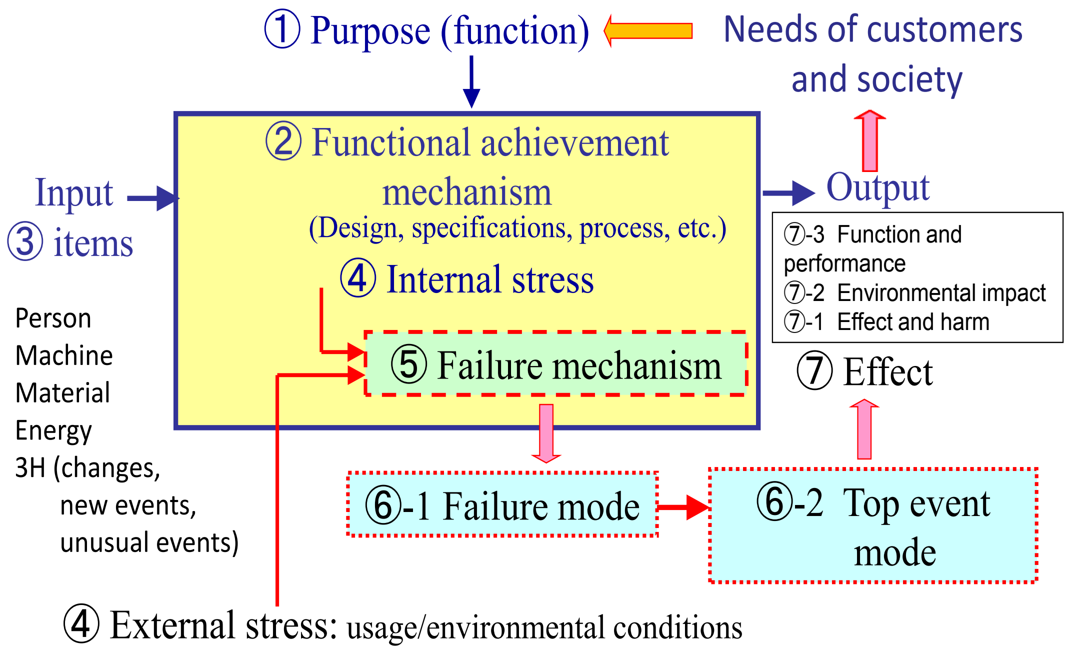

Fig. 4 Seven viewpoints for prevention

3.2. Failure mode

In JIS Z8115-2000, failure mode is defined as "a classification of failure phenomena…for example, disconnection, short circuit, breakage, friction, and deterioration." The word "mode" originates from the meaning of "measure" and refers to having the capacity to be measured and observed.

In the case of household water pipes, the damage that can be observed is fracturing, cracking, deforming, and clogging. These phenomena can also occur in town gas pipes and blood vessels. Concerning the parts that are generally referred to as "pipe," the damage can be categorized into these four classifications. Regarding the human cerebrovascular system, the clogging of a water pipe corresponds to the clogging of a blood vessel in the brain. In this way, failure mode is defined as the generalization and abstraction of malfunctions that occur in components of products and systems to facilitate the prediction of malfunctions in various components. Although data on failure mode may be limited, it can still be stored in a DB and used as organizational knowledge for use in predicting and evaluating problems. This leads to being able to identify the cause of the problem that may happen on products or systems, which may lead to a serious accident.

Failure mode extracted by surveying 27 articles and its frequency are shown in Table 2. The column blank means failure mode as a system.

Table 2. List of Failure Modes based on 27 Articles

Fracture	82	Slack	2
Crack	65	Electric discharge	2
Degradation	25	Delay	2
Surface Damage	21	Radiation injury	1
Thinning	19	Contamination	1
Deforming	18	Blister	1
Short circuit	16	Liquefy	1
Ignition Heat Emitting smoke	14	Decarbonization	1
Opening/Disconnection	11	No output	
Noise	9	Excessive output	
Dielectric breakdown Insulated degradation	7	Too little output	
Exfoliation	6	Output instability	
Omission	6	Vibration	
Fading/discoloration	4	Loss of function	
Insulated degradation	4		
Leak/short circuit	5	Total)	323

3.3. Top event mode

What events should not be allowed to occur in existing systems and plants? What events must be prevented in products and systems now under development? For example, airplanes should not crash, ships should not capsize, and vehicles should not roll over. In the case of an airplane crash, the contributing factors and measures differ depending on whether the engines shut down or control systems break down. This paper focuses on the sequence of events that leads to serious accidents and damage occurrence, with particular emphasis on the event immediately before the occurrence of the accident or damage occurrence, which is named as “top event mode.” The top event mode concept can be applied in many areas, such as systems, products, and structures. It corresponds to the event for which preventive measures must be taken, such as fail-safe design and event tree analysis (ETA). For an airplane crash, the top event mode is either “the engines shut down” or “the control systems break down”. For example, loss of all power supply for nuclear power plant, and malfunction such as the signal turns green even though it should be red for rail road, correspond to top event mode.

Almost top event modes for existing products and systems are predictable from past events. Even with new products, “top event mode” can be deductively predicted on the basis of the principles of the function or functional achievement mechanism or inductively predicted on the basis of the failure mode and similar cases in the past.

Table 3. Serious Product Accidents* and Top Event Mode
[E1 misuse, E2 carelessness] [May 2007 - Jan. 2012]

Product category	Top event mode	Effect
Combustion appliances** (79)***	Ignition (46), self-ignition (16), abnormal combustion (15)	Fire broke (77)
	incomplete combustion (1), skin contact (1)	Others (2)
Home appliances** (32)	Ignition (6), self-ignition (20)	Fire broke (26)
	incomplete combustion (6)	Others (6)
Total (111)		

*NITE (National Institute of Technology and Evaluation) www.nite.go.jp/index-e.html/
**based on E1 misuse ***number

Table 3 lists the top event modes caused by misuse (E1) and carelessness (E2) taken from the NITE's listing of serious product accidents. In particular, of the top 10 accidents related to combustion appliances and home electric appliances, there were 111 incidents, and fire broke out in 103 of them. The event immediately before the fire breaking out for which preventive measures must be taken is the top event mode. It can be divided into three categories: ignition (52 cases), self-ignition (36 cases), and abnormal combustion (15 cases). Furthermore, "the error mode," which is the contributing factor that leads to the top event modes and them caused the effect (fire broke and others), can be listed as shown in Table 4: prohibited (33 cases), with something on (19 cases), insufficient (14 cases), incomplete (13 cases), and heat the prohibited thing (11 cases). These five categories cover 81% of the 111 incidents.

Table 4. Error Mode and Error

Error Mode	Error	Number
prohibited	utilization for other purpose, installation in the prohibited place, sleep near the source of heat, inappropriate (ignition/fuel/remodel), heating without using a specialized pan	33
with something on	Refueling without extinguishing fire, leaving a thing un attended with heat	19
insufficient	Insufficient cleaning, Insufficient ventilation	14
incomplete	Incomplete closing of a lid, utilization with breakdown/deterioration, incomplete repair	13
heat the prohibited thing	heat/dry towels with oil	11
non confirming	heat/dry without checking oil removal after washing towels	3
over durability years	use with the state of being incomplete from long use (from 11 to 27 years)	7
excess	use over quantity of electricity	5
unstable	unstable installation place	3
blocking	blocking inlet port/exhaust port	3
	Total)	111

4. Potential Hazard

In JIS Z 8051-2004, hazard is defined as a “potential harmful source.” Here we consider the term hazard from the perspective of problem prevention and define it as “a source that can have a damaging effect or as a condition, factor, or scenario that can have a damaging effect” (Makabe et al. (2002)). The question is how to prevent a hazard from occurring. In this paper, hazard can be seen in Fig. 4, specifically ①–⑤. In this paper, from ① to ⑤ is collectively called “potential hazard”. The path from potential hazard to effect in Fig. 5 is based on Fig. 4.

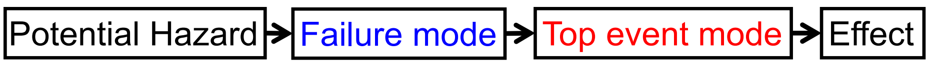

Fig. 5 Path from potential hazard to effect

A problem related to reliability and safety can lead to an accident due to product design or to an accident due to misuse or carelessness. To better understand these two kinds of accidents, one should consider “error mode” as well as “failure mode” (Fig. 5).

5. Schemes for Preventing Problems and New Reliability Engineering Methods

Figuring out the top event modes without excluding any modes is the key to preventing problems. In Japan, the author advocates 3H: Henka (change), Hajimete (new), and Hisashiburi (long time no use). Especially, in the case of 3H, such as new products, technological innovations, modified products, or reintroduced products, extracting top event mode should be done very carefully. The previous sections focused on the top event mode, i.e., the event immediately before a serious accident or damage occurrence, and its source, i.e., the failure mode. The failure mode, error mode, or combination of the modes that may lead to a top event mode should be identified. Then the measures for preventing problems should be taken. It is also important to investigate the reason why the failure mode or error mode occurs. After that, the measures for the source before problem occurrence should be taken. From these aspects, this paper proposes a problem preventing scheme with a procedure, and effective reliability methods in each step of the procedure.

(1) Figuring out “top event modes” without excluding any modes.

(2) Analyzing “failure mode” or “error mode” or their combinations that may lead to “top event mode” using “FTA” by top down approach.

(3) Figuring out “failure mode”, “error mode”, and their combination in each component, unit, sub-system and operation by a human. Detecting new “top event mode” using “FMEA” by bottom up approach as well as investigating what kind of “failure mode” and “error mode” lead to the top event mode in step (1).

(4) Investigating a potential hazard that may cause an important “failure mode”, or “error mode” which is extracted by FMEA or/and FTA.

(5) Implementing “Reliability Testing” to investigate what kind of mechanism leads to the important “failure mode” or “error mode”.

(6) Considering “Reliability Design” for breaking the above failure mechanism.

(7) In addition to the above actions, the advance countermeasure for the top event mode is critically important. Preparing “fail safe deign” for preventing top event mode from leading to its fatal effect.

(8) Establishing a procedure for preventing top event mode from leading to fatal effect using “ETA” at peace time. Besides, conducting a regular training based on ETA just in case.

(9) Implementing “DR (Design Review)” by using the combination of expertise and knowledge in a whole organization in order to review all the mentioned above procedures.

A new scheme for reliability engineering methods with the above procedure is shown in Fig. 6.

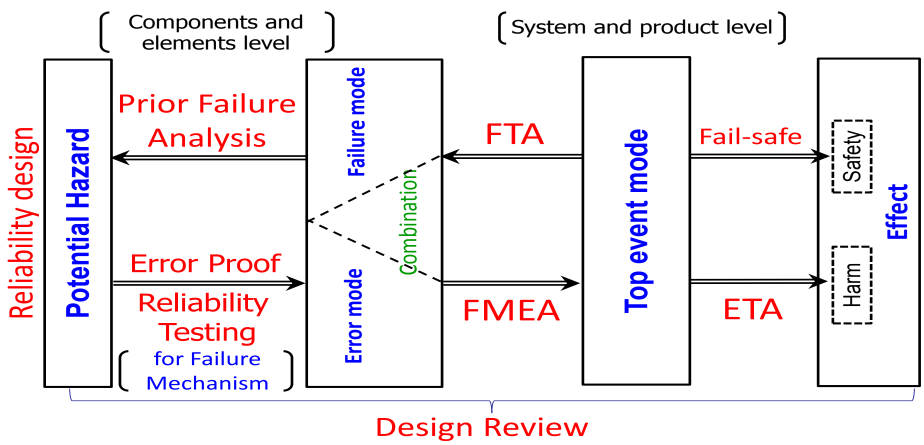

Fig. 6 Schemes for Preventing Problems and New Reliability Engineering Methods

6. Conclusion

This paper showed the importance of prediction for problem prevention. For the prediction, it is important to integrate an inductive approach and a deductive approach using upstream management and a system approach which consists of seven viewpoints. These seven viewpoints lead to four pillars; "potential hazard - failure mode - top event mode - effect," and they formulate a procedure of problem prevention and a new scheme of reliability engineering methods.

References

Makabe, H. (1989). in T. Asaka & K. Ishikawa & N. Yamaguchi (supervisor): “*New Edition; Quality Control Binran (2nd Edition)*,” p. 651, Tokyo, Japan: Japanese Standards Association, in Japanese.

Kume, H. (2014) in K. Suzuki (Editor): “*New Reliability Handbook*,” JUSE Press, in Japanese.

Makabe, H., K. Suzuki and A. Masuda (2002): “*Introductions of Reliability Engineering for Quality Assurance*,” JUSE Press, in Japanese.

Suzuki, K. (2004): “*Proactive Prevention Principles and System*,” JUSE Press, in Japanese.

Suzuki, K. (2013): "*Ensuring Reliability and Safety: Proactive Prevention*," JSQC Academic Library, Japanese Standards Association, in Japanese.