

Safety analysis methods and applications at the design stage of new product development —Introducing the FMFEA and S-H Matrix Method—

Hiroshi Wada*

Safety analysis requires a thoroughly methodical investigation—more so than even Reliability analysis. Such analysis must include the ability to deal with problems involving human error. This report will introduce the FMFEA (Failure Mode Factors and Effects Analysis) and the S-H (Software and Hardware) Matrix Method. These safety analysis methods serve as one part of the design review process in the design stage of new product development. Problem areas can only be discovered using analytical methods, but at the same time the approach must be efficient. This report will also include a review of the key application points for these methods.

1. Introduction

Product safety design is based on inherent design technology that starts from a consideration of reliability and progresses by applying reliability design methods.

When processes that can result in a lack of safety are spotted, a specific phenomenon (e.g., component failure or administrative or handling error) can usually be linked to personal injury through specific conditions or through a cause-effect relationship. Safety analysis methods must be able to follow these processes that create safety risks and determine in advance whether they will result in a lack of safety in product design.

First, we shall look at two safety analysis methods created by the author based on the widely used FMEA (Failure Mode and Effects Analysis) and FTA (Fault Tree Analysis). Specifically, we shall examine in detail the requirements for applying these analysis methods effectively.

2. Developing safety analysis methods

2-1 FMEA, FTA and ETA

FMEA and FTA are typical reliability analysis methods that are widely used. ETA (Event Tree Analysis) was developed in the US in 1974, and has since spread all around the globe, although this method is still not well known in Japan.

The FTA and ETA reliability analysis methods can be applied to safety analysis by limiting the phenomena to which they are applied. Table 1 shows a comparison of the features of these methods.

Table 1 Features of typical analysis methods

Item	FMEA	FTA	ETA
Purpose of analysis	Reliability	Reliability, Safety	Safety, Reliability
Starting point of analysis	Component failure mode	Product failure, Injury	Component failure mode
Direction of analysis	Components → Product (Bottom up)	Product → Components (Top down)	Components → Product (Bottom up)
Qualitative/Quantitative	Qualitative analysis	Both	Both
In advance/After the fact	Advance analysis	Both	Both
Printed form	FMEA table	FT diagram	ET diagram

*Kansai Management Consulting Association

2-2 Crucial elements in safety analysis

Safety analysis methods must possess the following three elements.

- (1) The ability to analyze even factors with scarce probability of occurrence
- (2) The ability to systematically develop complex failures and processes, not simply a single failure effect
- (3) The ability to illuminate the relationship between man and machine (e.g., misusing the product)

2-3 Designing safety analysis methods

FMEA analyzes failure of the relevant components that are selected according to the overall composition of the product, and so this method can be broadly applied. However, the method is not well-suited to investigating types of causes and effects systematically.

In contrast, FTA and ETA are much better at making systematic investigations. However, these methods suffer from a limited range of analysis.

Table 2 shows the strengths and weaknesses of each of these methods for safety analysis.

By judiciously combining these methods, we should be able to obtain a more satisfactory safety analysis method.

Table 2 Evaluation of adaptability for use as safety analysis methods

Item	FMEA	FTA	ETA
Width of range	Applicable components selected from function block diagram ○	Limited to top event (for analysis target) ×	Limited to initial event (for analysis target) ×
Ability to detect potential problems	Insufficient effects analysis (limited to single failure) △	Cause analysis done logically and systematically ◎	Effect analysis done logically and systematically ◎
Analysis of safety in misuse	None ×	None ×	Applicable to misuse at initial event (limited) △
Flexibility (simultaneous use for reliability)	Reliability only ×	One or the other ×	One or the other ×

Evaluation symbols: ◎: Optimum ○: Suitable △: Marginal
×: Not suitable

FMFEA¹⁾ was developed in 1995 to handle items (1) and (2) in section 2-2.

The S-H Matrix Method²⁾ is a safety analysis method developed in 1988 to handle item (3) in section 2-2, and is now widely used.^{3), 4)}

3. FMFEA

3-1 Application of FMFEA

3-1-1 Summary of FMFEA

FMFEA is a safety analysis method used to analyze factors and effects of failure modes of structural components. This method utilizes a combination of FTA and ETA. (Refer to Fig. 1.)

This method is able to both discover and predict problems using a systematic progression of detailed analysis. In addition, safety (preventing personal injury) and reliability (preventing product failure) can be analyzed simultaneously.

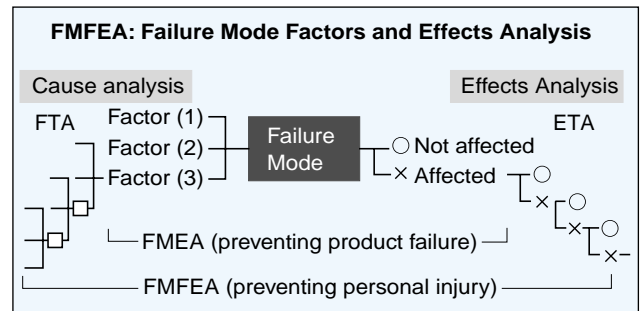


Fig. 1 Concept of FMFEA

Table 3 presents a comparison and evaluation of the differences between FMEA and FMFEA. Fig. 2 shows a printed form for FMFEA with an example of use.

Table 3 FMFEA vs. FMEA

Item	FMFEA	FMEA
Components covered	New crucial* functional units are selected from a function block diagram.	Components are selected from a function block diagram.
Failure mode	Takes up a single failure mode with a basic and proper function obliterated. ◎ No individual differences. ○ Doesn't require a lot of time.	Determined by activities such as brainstorming to leave nothing out. (If something is overlooked, it interferes with analysis.) ↓ The failure mode and its factors are mixed together disjointedly (unequal order). ▲ Something could be left out. △ Takes time.
Cause analysis	Utilizes FTA. ◎ Systematic and logical △ Takes time.	▲ Does not investigate deeply.
Effects analysis	Utilizes ETA. ◎ Systematic and logical △ Takes time.	▲ Does almost none.

Evaluation symbols: ◎: Excellent ○: Good △: Poor
▲: Unacceptable

* Crucial here must be defined in advance, e.g., having safety functions, or controlling something else.

FMFEA		Product name (Model number)	Component name	Function	Failure mode	Investigators	Day, month, year	Approved	Drafted	Page
5-dimensional	4-dimensional	3-dimensional	2-dimensional	Effects analysis	2-dimensional	3-dimensional	4-dimensional	5-dimensional		
Counter-measure 2 Error proof at design stage Pinhole Coating flaw Insulation degradation	Slit too shallow Slit too narrow Brush material Commutator surface too rough Brush attached backwards Holder pressure too great Brush sintering Layer short Coil winder tension too great	Commutator clogging Brush wear (0.2φ) Coil wire broken Leader line broken	Defective brush/commutator contact Electrical wire broken	Heater Not cooling (overheating) Electrical system (no current) Motor Lock (overcurrent) Mechanical system (lock)	X - Overheat protector stays ON O - Turned OFF X - Body heat distortion O - No heat distortion X - Coil overheats O - Not overheating X - Spark from layer short O - No spark (only open circuit)	Counter-measure 1 Thermal fuse test X - Stand-by mode Upper outlet O - Lower outlet X - Above body ignition point O - Below ignition point X - Thermal fuse stays ON O - Turned OFF X - Ignition on end plate O - No ignition	X - Thermal fuse stays ON O - Turned OFF X - Ignition at body O - No ignition X - Exceeds coil insulation heat resistance temperature O - Within heat resistance temperature X - Flashpoint at body O - Doesn't reach flashpoint	X - Mica doesn't block heat ⇒ A O - Heat is blocked X - Sintering continues O - No sintering X - Coil layer short ⇒ B O - No layer short X - Sintering continues O - No sintering		
Counter-measure 3 Coil winding process check	Insufficient slack in wire Claw clasping too strong Broken line at claw edge Bearing sintering defect Bearing oil impregnation insufficient Shaft surface rough Brush wear dust Bearing off center Shaft bent Ferrite chipping Foreign matter from opening Rotor coating dust Ferrite adhesion U-separator off Sintering roundness precision	Insufficient slack in wire Claw clasping too strong Broken line at claw edge Bearing sintering defect Bearing oil impregnation insufficient Shaft surface rough Brush wear dust Bearing off center Shaft bent Ferrite chipping Foreign matter from opening Rotor coating dust Ferrite adhesion U-separator off Sintering roundness precision	Electrical system (no current) Motor Lock (overcurrent) Mechanical system (lock)	X - Overheat protector stays ON O - Turned OFF X - Body heat distortion O - No heat distortion X - Coil overheats O - Not overheating X - Spark from layer short O - No spark (only open circuit)	X - Stand-by mode Upper outlet O - Lower outlet X - Above body ignition point O - Below ignition point X - Thermal fuse stays ON O - Turned OFF X - Ignition at body O - No ignition X - Exceeds coil insulation heat resistance temperature O - Within heat resistance temperature X - Flashpoint at body O - Doesn't reach flashpoint	X - Mica doesn't block heat ⇒ A O - Heat is blocked X - Sintering continues O - No sintering X - Coil layer short ⇒ B O - No layer short X - Sintering continues O - No sintering				
Counter-measure 4 Ferrite process check	Ferrite adhesion U-separator off Sintering roundness precision	Ferrite deviation	Checks and Countermeasures 1. Thermal fuse test (e.g., position mode gap, time, temperature, and blow-out condition during operation) 2. Investigate error-proof design for preventing backward attachment of brush. 3. Check winding process (e.g., jigs, winding tension, clasp strength of commutator claw). 4. Check ferrite sintering process (e.g., roundness and adhesion)	Person in charge	Date					

Fig. 2 FMFEA printed form with example

3-1-2 Failure mode selection

When using FMFEA, the analysis begins with the components being investigated and their failure modes, making selection and sampling crucial. FMFEA follows the procedure listed below. (Refer to Fig. 3 and Table 3.)

- (1) Select as subject of the investigation a new unit with an important function. (Predefine “important”, e.g., having safety functions, or controlling something else.)
- (2) Check basic proper function of that unit.
- (3) Define a single failure mode with “failure = loss of function”.

Even when limited to a single failure mode, using this type of definition makes it possible to include such failure modes as secondary function failures and subordinate component failures in a follow-up analysis of details using FTA.

The problem areas and countermeasures obtained through focusing on important points are checked for other relevance, developed horizontally, and then standardized.

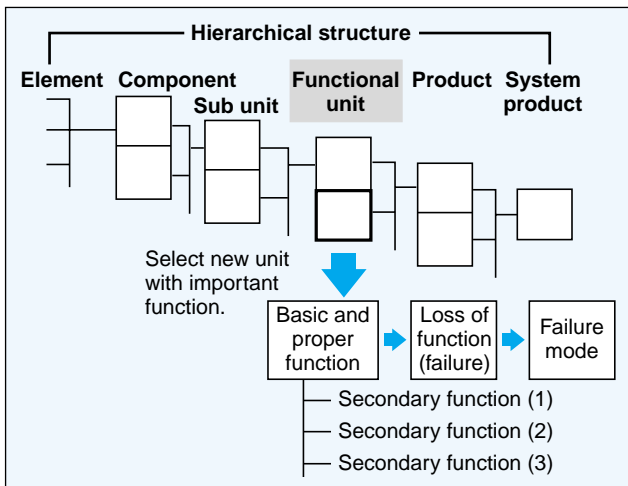


Fig. 3 Selecting the failure mode

3-2 Applying FMFEA — “Concurrent FMFEA”

3-2-1 Process FMEA

Process FMEA is used to prepare for new product manufacture, and constitutes an advance means of investigating and controlling production quality in production processes and assembly. This aim is achieved primarily by the production department.

Process FMEA differs in purpose from design FMEA (which is generally known as simply “FMEA”), but the printed forms used are almost identical. (Refer to Fig. 4.)

Table 4 compares the differences between the two.

Table 4 Differences between design FMEA and process FMEA

Item	Design FMEA	Process FMEA
Purpose	Checking reliability design	Checking process control
Time period	Design stage (before design completion)	Production preparation stage (after design completion)
Department in charge	Design department	Production department
Starting point of analysis	Component failure mode	Manufacturing error

The “process control table” serves the same purpose as process FMEA. (The “process control table” is also known as the “QC process table”. The printed form in Fig. 4 is one example.) All factories create these tables, regardless of whether they utilize process FMEA.

When used as the substance of advance investigations for new product quality assurance, these process control tables contain more detail than process FMEA, and this author believes that they are sufficient for that purpose.

3-2-2 “Concurrent FMFEA” practices

In Fig. 2 (an example of FMFEA), the cause analysis section on the left contains many controlling items related to processing, assembly, equipment, inspection and management. The effects analysis section on the right is related to product design.

When FMFEA is done at the design stage, process FMEA can be done concurrently. Process control for a new unit with an important function is performed from the design stage, and process design for the new product as a whole can be done using the conventional “process control table”.

This author proposes calling this new system “Concurrent FMFEA”⁽⁵⁾. Fig. 5 (next page) shows two flowcharts.

Concurrent FMFEA obtains the following results.

- (1) Production engineers obtain process information and they can be reflected in the design (improving design quality and completion rate).
- (2) From the early stages, design intention can be

Process FMEA													
No.	Process flowchart	Process name	Name of equipment and jigs	Process functions	Manufacturing error modes	Manufacturing error causes	Effects on product	Ranking			RPN	Countermeasures	
								Cause	Effects	Detection		Person in charge	Date

Process control table														
No.	Process flowchart	Process name	Name of equipment and jigs	Component name; materials name	Process control item					Inspection control item				
					Control points	Control standards	Control methods	Control specifications	Documents	Inspection items	Inspection standards	Inspection methods	Inspection equipment	Documents

Fig. 4 Printed form for Process FMEA and process control table

transmitted to the production process (improving process quality).

- (3) Factors causing production errors can be thoroughly investigated. Additionally, the relationship between production errors and product safety can be systematically analyzed (improving product safety assurance).

Process and design FMEA are carried out concurrently for secondary results, and this contributes to reducing the time required for new product development. This can also reduce the expense and loss of time accompanying product design changes. Concurrent FMFEA can contribute to management as a method of CE (concurrent engineering).

3-2-3 Development toward Design-In

The concurrent FMFEA system can apply not only to intra-manufacturer coordination (e.g., process and design departments), but also to inter-manufacturer coordination (e.g., component and product manufacturers).

FMFEA is utilized as a design-in tool for the component manufacturers to participate in design at the design stage of the product manufacturer. FMFEA is carried out jointly with the component manufacturers handling the cause analysis and the product manufacturer handling the effects analysis.

The responsibility of the component manufacturer is stated in the Product Liability Law as well, and the FMFEA serves as a link for the product safety assurance of the component manufacturers.

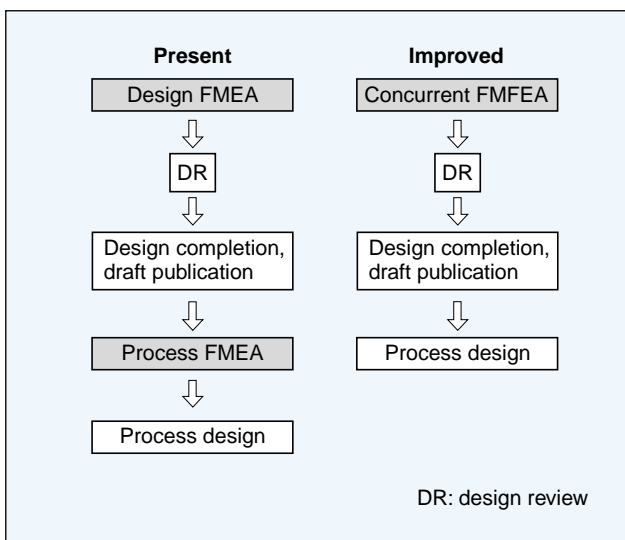


Fig. 5 Effect of concurrent FMFEA

4. The S-H Matrix Method

4-1 Utilizing the S-H Matrix Method

4-1-1 Misuse and product safety design

Uses and features of new products are determined at the planning stage, and so the manner in which the new product is meant to be used should already be conceptualized. The manufacturer must presume misuse and promote product safety design using the following notion. (Fig. 6)

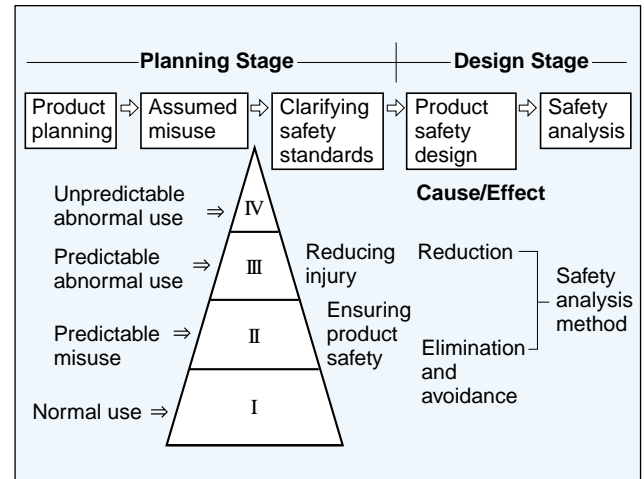


Fig. 6 Misuse and product safety design

Planning stage: What types of misuse are likely for this product? → Clarify safety standards and criteria.

Design stage: Create and evaluate safety in design, based on standards and criteria. → Apply safety analysis methods.

4-1-2 Summary of the S-H Matrix Method

Misuse causes additional stress to components, leading to failure. Such failure can result in a loss of safety or the misuse itself can be a direct safety hazard even when not resulting in failure. An example of the latter is “thoughtlessly” touching flammable material with a hot item and causing ignition.

A failure analysis method such as FMFEA overlooks this latter type of investigation. The S-H Matrix Method is an analysis method using a matrix to diagram the relationship between safety and misuse, and this method can cover the blind spots of unsafe misuse that does not lead to failure. Fig. 7 shows a model printed form, and Fig. 8 (next page) shows an example using a home appliance product.

H	S	Normal use		Misuse A	Misuse B
		Cause Detection	Effect Composite		
All components normal					
Component (1) failure mode					
Component (2) failure mode					

S: Software (method of use)
H: Hardware (component construction)

Fig. 7 Model printed form for the S-H Matrix Method

S-H Matrix Method		O: occurrence D: detection		E: effects C: composite		Evaluation		Occurrences: promotion of failure mode, 3 pts Detection: ease of finding, 3 pts		Effects: Severity, 5 pts Composite = Occurrence x effects x detection		X, Δ: depending on the size of the evaluation countermeasure (No size for composite)		Product name (model number) Automatic hot water function		with built-in		Performed (Year, month, day, member)		Approved		Checked		Drafted		Page							
		NO	NO	A	B	C	D	E	F	G	H	I	Countermeasures	Person in charge																			
Component name	Safety functions	Kind of misuse	Failure mode	NO	A	B	C	D	E	F	G	H	I	Items for design investigation (1) Current leakage detector circuit (2) Overheating safety design review (3) Single cut-off relay → dual cut-off. (4) Inner cover detector		Safety test performance (1) Wrong voltage (200 V) test (2) Current leakage test, tracking test (3) Supply water test (4) Connector loose test		Date															
NO														⊙: Most important (requires design change) ○: Important																			
1	All functional units	Normal	Normal	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1					
2	Heater	Insulation degradation (pipe failure)	Normal	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1					
3	Heater thermistor	Overheating prevention, reversible type	Not operating (open)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1				
4	Water thermistor	Temperature adjustment from 45 to 95°C	Not operating (open)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1				
5	Thermostat	Overheating prevention, 110°C, backup for No.4	Not operating (short circuit)	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1			
6	Thermal fuse	125°C, 15 A, backup for No.5	Not operating (short circuit)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
7	Pressure switch	Detects use with no water.	Not operating	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
8	Relay	15 A, single cut-off	Not operating (short circuit)	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
9	Seal mechanism	3 used, Si rubber	Water leakage	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
10	Heater connector	SUS304, locking type	Overheating due to contact defect	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
11	Grounding mechanism	Prevents electric shock.	Broken wire, left open	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
12	Lid SF switch	Won't start when open, prevents opening and releasing water while running.	Not operating (short circuit)	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Fig. 8 S-H Matrix Method printed form with examples

4-1-3 Procedure

- (1) Make a list of items for S (misuses) and H (functional units).
- (2) Investigate in order the matrix formed by the S column and the H column.
- (3) Investigate each matrix column for the following four elements: probability of occurrence, severity of effects, detection and composite.
 - Probability of occurrence: the degree that misuse promotes component failure (ranked by the 3 point method).
 - Severity of effects: the degree of safety risk caused when misuse and components failure overlap (5 point method).
 - Detection: the degree of difficulty for the user to find the unsafety (3 point method).
 - Composite: Total of the three (Maximum $3 \times 5 \times 3 = 45$)

4-2 Points for effective utilization

4-2-1 Selecting S and H items

- (1) Misuse “S”
 - Limit items to those involving misuse specific to that product. Make a separate investigation according to the manual and design standards for misuse common to a product group.
 - Limit items to those involving misuse linked to components overheating (ignition) and insulation degradation (electric shock). Injuries, burns and other harm can be checked directly through separate safety tests.
 - Put items in groups and list only the representative items.
- (2) Subject components “H”

Select items using the same method as for FMFEA. (Refer to 3-1-2, (1).) However, when using the S-H Matrix Method, do not limit subject components to new items.
- (3) Investigating the matrix formed by S and H
 - The matrix diagram has the advantage of being the basis for an effective investigation even with only a small list of elements (S and H items). This approach provides for preventing omissions and checking relevance. Therefore, the problems can be found easily in the matrix.
 - On the other hand, when the relationship between misuse and unsafety is weak, the problem points do not become obvious even when listing a large number of elements. A long list in that case only makes the problem seem more complicated.

4-2-2 Utilizing this method at the planning stage

As discussed in 4-1-1, misuse should be hypothesized at the new product planning stage, and product design should start by clarifying safety standards. The S-H Matrix Method printed form (S column) should be used for these purposes, and these can be checked through a design review at the planning stage.

4-2-3 Combining with the FMFEA

Combining the merits of the S-H Matrix Method misuse analysis with the thoroughly systematic failure analysis of FMFEA can produce superior results. When product and component manufacturers cooperate to perform this type of analysis, they complement each other and create a more effective analysis. The framework for that process is:

[Product planning stage (before starting design)]

- (1) Forecast misuse and environmental conditions according to the uses and features of new products.
- (2) Create groupings of misuses, classify them, and put them in the S column.
- (3) Clarify the safety standards for (2).

[Detail design stage (before issuing drawings)]

- (4) Perform S-H Matrix Method investigation.
 - List important functional components and failure modes in the H column.
 - Investigate the S-H matrix in (2).
- (5) Select the key functional components based on the results of the S-H Matrix Method.
- (6) Perform the FMFEA investigation based on the key functional components thoroughly.

5. Conclusion

This report has introduced two new methods for analyzing safety, and discussed the main points for utilizing these methods.

The following points are key to regularly utilizing these safety and reliability analysis methods and linking them to the design review:

- When examples, experience and special methods are required → have the best specialist technicians participate in planning.
- When inference to find problem points are required → attach importance to hypothesis and verification.
- When elimination of waste and efficient practical use are required → concentrate on important points and then develop horizontally.
- When improvement methods appropriate to the product and purpose are required → establishing a “company style” method can be considered especially important.

[Bibliography]

- 1) Hiroshi Wada, “A Proposal of Safety Analysis Method ‘FMFEA’”, The Journal of Reliability Engineering Association of Japan, Vol.18, No.2, p.100-105, Reliability Engineering Association of Japan, 1996
- 2) Hiroshi Wada and Osamu Shiramizu, “Development and Application of Product Safety Analysis Method”, Total Quality Management, Vol.40, No.11, p.311-315, Union of Japanese Scientists and Engineers, 1989
- 3) Hirota Shimizu, “A Case Study of the Application of Product Safety Analysis(SHFEA)”, The Journal of Reliability Engineering Association of Japan, Vol.19, No.2, p.2-9, Reliability Engineering Association of Japan, 1997
- 4) Tohru Muramatsu and Takayoshi Nagai, “Product Development of ‘Nice Mama’ Kitchen Garbage Disposal Machine for Household Use”, Total Quality Management, Vol.49, No.12, p.88-89, Union of Japanese Scientists and Engineers, 1998
- 5) Hiroshi Wada, “A Proposal of concurrent FMFEA (Failure Mode Factors and Effects Analysis)-Simultaneous Practice Design and Process FMEA-”, The Journal of Reliability Engineering Association of Japan, Vol.20, No.4, p.232-233, Reliability Engineering Association of Japan, 1998