Improving Development Process for Product Safety

Won Jung
Department of Industrial & Systems Engineering
Daegu University
15 Naeri, Jillyang, Gyeongsan, Gyeongbuk, 712-714. S. Korea
wjung@daegu.ac.kr

Abstract

In designing and evaluating a new product, the company needs to give thought to the entire spectrum of produceability, usability, and ultimate reliability, as well as safety of users. For each design review(DR) stage, a formal, systematic, documented review and evaluation of a product design is conducted to assure that the product is safe and reliable, that costs and materials have been optimized, and that the design complies with its specifications and requirements.

This paper presents how to improve development process for product's safety and reliability. The process requires gathering the appropriate information, determining the limits of the product, estimating risk associated with the task-hazard combinations, and reducing risk according to a prioritized procedure.

Key words: Product safety, Design Process, Development process, Risk analysis

1. Introduction

Products can possess both inherent hazards and the potential for contributing to or initiating other hazards. The existence of hazards is determined from experience, analysis, and careful study. The failure of a product or product component can constitute a hazard if safeguards have not been provided in anticipation of failure. Such product failures consist not only of those due to physical causes, such as stress or fatigue, but also the those arising because of inadequate consideration of human factors when the product was designed. The evaluation of hazards from product failures needs to be carried out by the designer in an organized and methodical fashion.

Many technical methods are developed for risk analysis such as FMEA(Failure Modes and Effects Analysis)[11], FTA(Fault Tree Analysis), ETA(Event Tree Analysis), HEA(Hazard Effect Analysis)[1], S-H(Soft-Hard)[1], PHA (Preliminary Hazard Analysis) [5], MOSAR (Method Organized for a Systemic Analysis of Risks)[9], and HAZOP (Hazard and Operability Study)[8]. These methods are practically used to define risk factors and(or) to analyze hazardous situations in the field usage. However, the use of these methods can not be a enough activity for risk prevention. More things should be done technically and systematically through the life cycle of products.

Even for the system installation, operation, maintenance and certification approval according to ISO9001 is basic prevention and protection activity for the product safety, it cannot be a complete prevention activity for the product safety and liability. Quality management system is quality standard of product and service and is not suitable to substitute standard for the specific product safety. The standard is merely basic requirements.

In undertaking activities to lessen the risk of product liability, the first necessary action for success is for the top management of the company to formulate company policy statements and to identify a person of sufficient authority to be responsible for product safety. Then a formal listing of product liability management activities should be prepared.

This paper presents procedures of risk analysis in the design and development stage for improving product's safety and reliability. The design stage is the least expensive time to propose a change to a product, and the most effective and economical place to catch and address potential reliability and safety concerns. The procedure require gathering the appropriate information, determining the limits of the product, estimating risk associated with the task-hazard combinations, and reducing risk according to a prioritized procedure.

2. Product design and development process

Product development process has revolved around strictly technical considerations, such as strength

of materials, manufacturability, component stability and strength, testing methods, and costs. In an era in which the manufacturer is extremely vulnerable to product liability action, this traditional approach must be broadened to include more attention to standards and codes, hazards analysis, express and implied warranties, warnings and labels, failure analysis, and design review. This section presents the procedure of risk reduction process during the product design and development.

2.1 Risk management

Risk management programs are established to allow companies to make informed decisions to:

- •Eliminate or minimize loss of life, accident, or injuries to people
- •Reduce damage to equipment, property or the environment
- •Save sources

Ultimately, a company performs risk management and risk assessment activities to make the exposure to hazards acceptable. Acceptable risk is: 1) less than or equal to the maximum tolerable risk and 2) as low as reasonably practical.

The risk management program's integration with the design process phase can be illustrated with the use of a matrix. Refer to the risk management program matrix in <Table 1>. The design process phases are placed across the top of the matrix using their reference number. Along the left-hand side, the risk management activities are listed. The risk management activities that are associated with each design process phase are identified with a dot.

The procedure of the risk management according to the European standard[7] is shown in <figure 1>. The steps of procedure to arrive the risk assessment are;

a) Gather the appropriate information to conduct this procedure

b) Determine the limits of the product

c) Identify and document the hazards associated with the tasks to be performed over the life cycle of the product.

d) Analyze the risk associated with the identified individual tasks and related hazards for severity of harm that can occur and the probability of such an occurrence

e) Evaluate the each risk in order to determine whether it is tolerable or not.

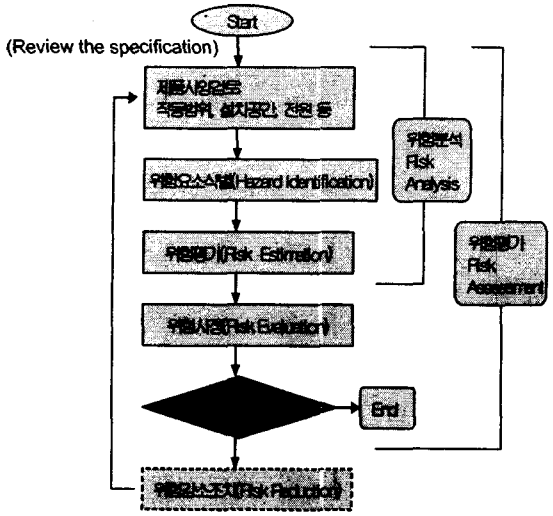
2.2 Information for risk assessment

The information for risk assessment should include, but may not be limited to, the following:[3]

- •limits of the system
- •requirements for the lifecycle of the system
- •design drawings, sketches, system descriptions or other means of establishing the nature of the system
- •information concerning energy sources
- •any accident and incident history
- •any information about damage to health
- •system layout and proposed building/existing system integration

<Table 1> Matrix of risk activities vs. design phase

	Design program phases								
Risk Activity	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Risk management plan	•	•	•	•	•	•	•	•	•
Assign qualified personnel	•	•	•	•	•	•	•	•	•
Identify risks	•	•	•	•	•	•	•	•	•
Identify risk controls	•	•	•	•	•	•	•	•	•
System architecture and spec.	•	•	•	•					
System verification plan		•	•	•	•	•	•		
System validation plan				•	•	•	•		
Sub-system architecture and spec			•	•	•				
Sub-system verification plan				•	•	•			
System verification methods and results						•	•	•	
Risk integrity evaluation								•	•
Residual risk									•
Assessment report									•

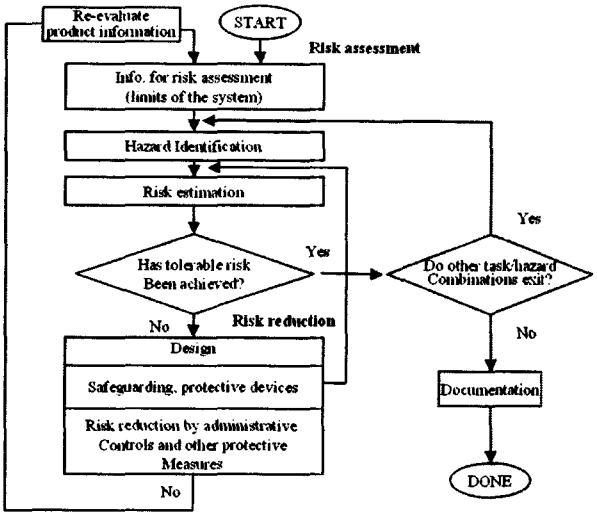


<Figure 1> Procedure of risk management

2.2 Information for risk assessment

The information for risk assessment should include, but may not be limited to, the following:[3]

- •limits of the system
- •requirements for the lifecycle of the system
- •design drawings, sketches, system descriptions or other means of establishing the nature of the system
- •information concerning energy sources
- •any accident and incident history
- •any information about damage to health
- •system layout and proposed building/existing system integration



<Figure 2> Risk assessment and risk reduction process

The risk assessment process begins with determining the limits of the system. These limits are use limits, space limits, time limits, environmental limits and interface limits etc. <Figure 2> shows risk assessment and reduction process.

2.3 Risk assessment

A large portion of the risk management activities is risk assessments that are performed throughout the design activity. Risk assessments can be quite comprehensive endeavors. However, risk assessments cover three areas that answer three corresponding fundamental questions. Refer <Table 2> below:[12]

<Table 2> Risk assessment area questions

Hazard identification	What can go wrong?
Rating the hazard	How often and how damaging is it?
Hazard control	What can be done to prevent the hazard?

1) Hazard identification

The type of hazards to be reviewed during the design process shall include the following:

<Table 3> Types of hazards

Chemical	***Mechanical***
Corrosive	Weight
Toxicity	Speed or acceleration
Flammability	Stability
Pyrophoricity	Vibration
Explosive	Rotation
Oxidizing	Translation
Photoreactive	Reciprocation
Hydroreactive	Pinch or nip points
Carcinogenic	Punching, shearing
Shock sensitive	Sharp edges
	Cam action
Electrical	Stored energy
Shock	Entrapment
Short circuit	Impact
Sparking	Cutting actions
Arcing	
Explosion	***Miscellaneous***
Radiation	Noise Light intensity
Fire	Stroboscopic effect
Insulation failure	Temperature effect
Overheating	Pressure, suction
	Emissions
Radiation	Ventilation
Alpha, gamma, beta	Ignition sources
X rays	Decomposition
Infrared, ultraviolet	Slipperyness
Radio and microwaves	Moisture
	Aging

2) Risk estimation

Risk estimation for a given hazardous situation is used to determine risk. It should account for all modes of operation and work methods for situation when it is necessary to suspend or modify one or more protective measures. The elements of risk which are to be considered are the severity of harm and the probability of occurrence of that harm.

<Table 4> Suggested hazard severity and probability categories.

Severity		Probability	
i.d.	Name	i.d.	Name
I	Catastrophic	A	Frequent
II	Critical	B	Probable
III	Marginal	C	Occasional
IV	Negligible	D	Remote
		E	Improbable

<Table 5> Hazard risk assessment index

Severity / Probability	I Catastrophic	II Critical	III Marginal	IV Negligible
A frequent	1	3	7	13
B Probable	2	5	9	16
C Occasional	4	6	11	18
D Remote	8	10	14	19
E Improbable	12	15	17	20

Hazard risk index Acceptance criteria

1-5 Unacceptable, Corrective action required to eliminate the risks

6-9 Undesirable, Corrective action required to mitigate the risks

10-16 Acceptable with review

17-20 Acceptable without review

2.4 Risk reduction

If the risk is determined to not be tolerable, it is necessary to reduce that risk by implementing protective measures. In determining if the risk is tolerable at each step of the risk reduction process, it is necessary to evaluate the application of the protection way against the following factors;[3]

- •risk-reduction benefit
- •technological feasibility
- •economic impact
- •ergonomic impact
- •productivity
- •durability and maintainability
- •usability

The type of the protective measure is determined by the nature of the task and associated hazards for the product under consideration. Protective measure should be selected to provide the desired degree of risk reduction. Protective measures should be applied in the hierarchical order of the following items;

- •Eliminate the hazard or reduce the risk by design
- •Apply safeguards
- •Implement administrative controls or other protective measures

The very important thing in the risk reduction process is to consider user side point of view. Even though designer consider all aspect of design factor of safety, he cannot sure environment and condition of users. It is very important to have input data from the user's side and inform to the user how safe they can use this in products. The information and recommendation of the above situation follows;[3, 7]

- Additional safeguards
- Organizational matter, Safety working procedure, Warning, Supervision, Sign and Permit-to-work systems
- Training
- Personal protective equipment
- Working environment
- Keep and control the good health

A user's input is that information received from either the user community regarding the intended use of the product in general or that which is received from a specific user. Those protection way required due to the specific process not envisioned in the intended use of the product. In addition, the supplier/user should take into account that adding a safeguard may add additional hazard or increase risk from other hazards. Risk reduction taken by the user is to be considered collectively since not all elements may be implemented or in the order portrayed.

2.5 Documentation

Records retention and specific aspects of document control can play major roles in a product liability lawsuit.[9]
Documents are crucial for explaining the development and entire life cycle of a product.
They can serve as evidence that the manufacturer made every effort to assure a well-thought out safe and reliable product.
Various records can identify problems experienced in the development and testing of a new product, along with the actions taken to correct the problems.

<Table 6> Supplementation factors for product safety

ISO 9001		Supplementation factors for PL
Items	Requirements	
7. Product realization 7.1Planning of product realization	Plan and develop the processes needed for product realization	- Define hazards and estimate mishap probability - Estimate risk level by products - Estimate risk level by quality characteristics - Select safety process/ safety control items - Review QC process chart/ identification control
7.2 Customer-related processes	- Determination of requirements related to the product - Review of requirements related to the product - Customer communication	- Review of safety items in customer requirements - Process of safety related code, regulation - Process of corresponding customer complaints - Recall system - Process of communication system with safety related customer - Critical situation control or mishap management
7.3 Design and development	- Design and development planning -Design and development inputs, outputs and review - Design and development verification, validation - Control of design and development changes	-Safety review -Prototype safety test -Documentation and maintenance of product design and development -Management and control of warning, instructions

Such documentation can be effective in proving that the manufacturer operated in a very concerned and responsible manner.

3. Improving quality system for product safety

Generally the documented development process in Quality System of Korean manufacturer has many weaknesses. In the section 7.3.2 of ISO9001:2000[10], describes that "Design input relating to the product requirement shall be determined and records maintained. This input should include applicable statutory and regularly requirements". Design engineers look over the safety aspects of new products since there is no clearly mentioned process to fulfill the safety matter in advance. <Table 6> presents the safety factors that the quality system should make up for the weak points in the current quality system.

4. Conclusion

Product safety management involves a formal overview of an entire program of activities designed to lessen product liability risk. With the proper endorsement by management, engineering, sales, and services the climate is created for everyone to become conscious of the need to give product safety its proper priority.

One of the most significant products of the safety effort is the documented system of procedures and processes which will be created and continuously updated. If a risk analysis process is properly designed and systematically followed, the quality system(ISO, QS etc) will be one of the most effective tools in the prevention of safety problems. We would recommend management to include safety as a primary specificatión in identifying the needs during all phases of the product's existence

References

[1]日本科學技術聯盟(1995),
製造物責任と製品安全, 日科技聯出版社
[2]AkaoYoji(1988), Quality Function Deployment, Productivity Press
[3] ANSI B11.TR3-2000, Risk assessment and risk reduction-A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine tools
[4] Siemens AG(1999), System Integrated: The safety program for Industries throughout the world
[5] DOD(2000), MIL-STD-882D, System Safety Program Requirements, DOD
[6] EN 414 Safety of machinery-Rules for the drafting and presentation of safety standard
[7] EN 1050, Safety of machinery-risk assessment
[8] Fullwood, R. R.(2000), Probabilistic Safety Assessment in the Chemical and

Nuclear Industries, Butterworth-Heinemann
[9] Goodden, Randall(2001), "Product liability prevention-the next dimension in quality, ASQ Quality Press.
[10] ISO9001:2000 Quality management system
[11] Stamatis, D. H.(1995), Failure Mode and Effect Analysis, ASQ Quality Press
[12] Wortman, B.(1999), The Reliability Engineer Primer,Quality Council of Indiana.