International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 6, June - 2013

System Safety Management For Safety Design- An Over View Of System Safety Assessment

Er. Praveen Patel
Associate Professor, Institute of Engineering & Science, IPS Academy, Indore

Dr. Nagendra Sohani
Associate Professor, Institute of Engineering & Technology, DAVV, Indore

Abstract

Safety through design or design for safety into worksystem is an important but illunderstood concept. In this lecture material, the author demonstrates the concepts, principles and procedures for design for safety. It is hypothesised that understanding the worksystem components, functionalities and their interrelationships are the prerequisites for any design. The methodology is developed based on hazard evaluation, risk assessment, hazard control hierarchy, and the concept of alternative design solutions.

"1. Introduction"

Managing safety in industry is a perennial problem. Accident statistics support this. In India, the occupational fatality rate per 1,00,000 employees is 11 which is about 14 times more than United Kingdom. The causes of fatalities can be attributed to human related, machinery related, environment related, and organization related. The causes are not well known. The severities of the hazards are frequently anticipated. Guidelines and procedures are not evolving with the pace of industrialization. The other important issue is effort to prevent and mitigate accidents which is scattered in nature. For example, in Indian Oil and Gas Industry case, every Oil Industry follows risk assessment and management plans. But how the outcomes are used for design for safety is seldom documented. There is a need to develop a comprehensive methodology which guides practitioners in designing safety in their workplace.

In this brief lecture note, the author tries to give the outline for design for safety with an emphasis to risk management what has been practiced in high risk industries like oil refineries. The remaining of the lecture note is structured as follows. Section 2

describes the basics of design for safety with a theoretical model. Section 3 presents the principles for design for safety followed by a step by step procedure for implementing safety through design in Section 4. Finally, summary and discussion are presented in Section 5.

2. Basics for design for safety

In order to understand the basis for design for safety one has to understand a few important concepts applicable for safety design. First, safety is a relative term which indicates the degree of freedom one gets from danger while working in a work system. It necessarily means that no work system is 100% safe and posses certain amount of risk arising due to presence of hazards. Secondly, hazard can be defined as a thing or situation having potential to cause harm or danger to people, property or management. For example in oil refinery the bulk storage of flammable liquids and gases and their transportation leads to major fire hazard due to high calorific valves of them. Hazard may occur or may not. Occurrences of hazards lead to realised risk if the occurrence is associated with certain amount of loss to the management. For example depressurization within the storage facility from storage pressure and temperature leads to the boiling of flammable liquids with in the enclosed container. This is systematic process leads to BLEVE with in the tank. Finally, risk has two components: the probability of

Table 1: Safety design strategies

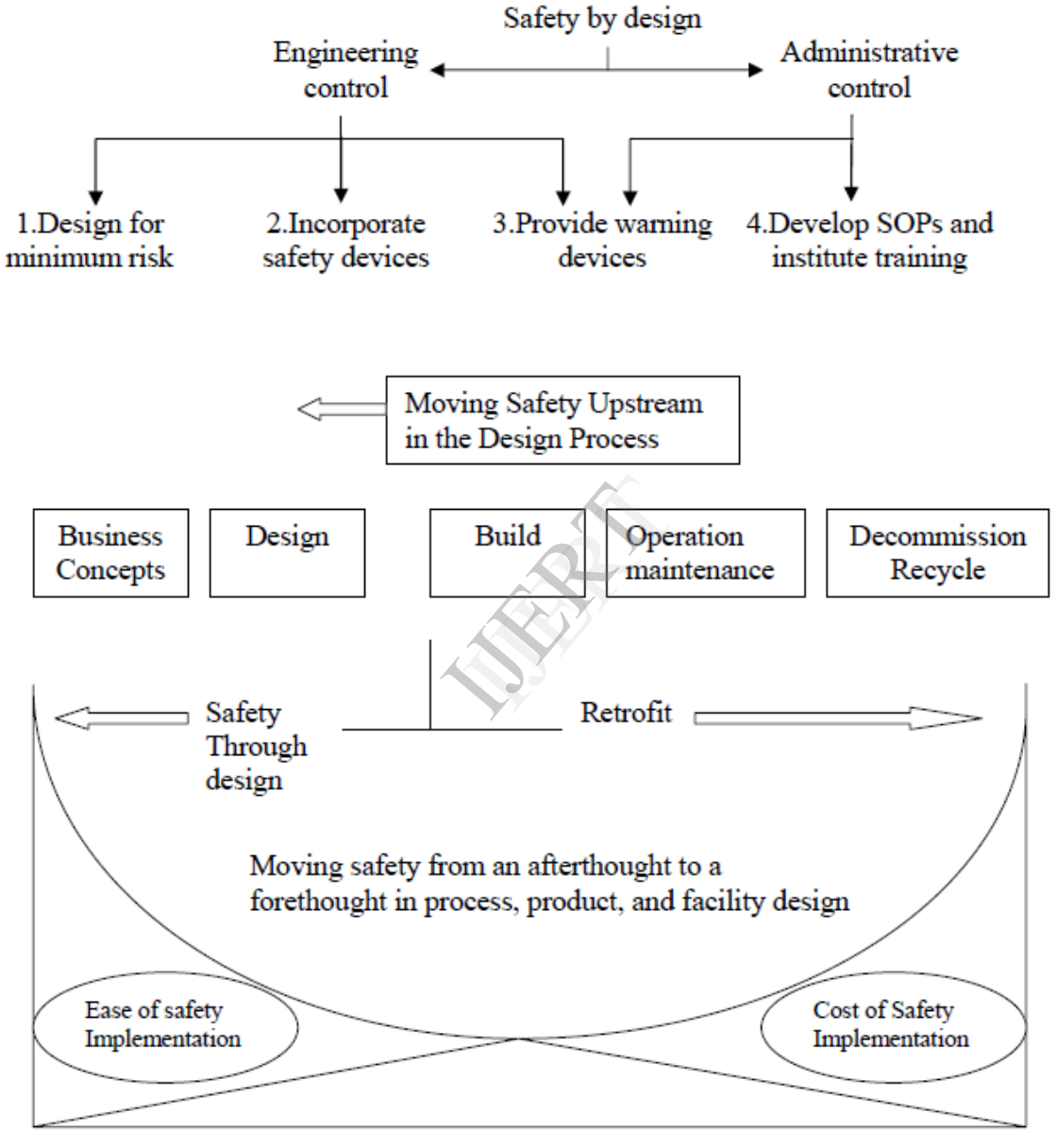

Fig. 1: Model for Safety Through Design (adopted from Manuele, F. A., 1999).

hazards occurring and the consequence of the hazard occurring. Design for safety essentially talks about design for minimum risk.

There are synonymous for design for safety. Safety through design is one of them. Design for safety or safety through design is well defined by Manuele (1999) and is given below.

> *Safety through design is defined as the integration of hazard analysis and risk assessment methods early in the design and engineering stages and the taking of the actions necessary so that the risks of injury or damage are at an acceptable level. This concept encompasses facilities, hardware, equipment, tooling, materials, layout and configuration, energy controls, and environmental concerns. What is proposed for safety through design is not a program, with its attendant whistles, bells, slogans, and banners running to a sputtering end, to be forgotten as many programs are. What is needed is an agreed-upon and well-understood concept, a way of thinking that is translated into a process that effectively addresses hazards and risks in the design processes.*

Manuele (1999) model for safety through design is shown in Figure 1. The life cycle of a worksystem comprises stages namely, business concepts, design, build, operation and maintenance, decomposition/recycle. Considering safety aspects during the first two stages and make it works is known as 'safety through design', while the same in the later stages is known as retrofit. Safety through design has both the advantages of ease of safety implementation and lower cost of safety implementation.

3. Principles of design for safety

There are four design strategies: (i) Design for minimum risk, (ii) Incorporate safety devices, (iii) Provide warning devices, and (iv) Develop SOPs and institute training. These strategies can be linked with the engineering and administrative controls and is shown in Table 1.

There are nine principles (P1-P9) of safety by design. These principles are based on the concept of energy interactions as suggested by Haddon (1966) in his energy control model. The nine principles are as follows:

P1: Prevent the creation of hazard in the first place (Avoid hazard)
P2: Reduce the amount of hazard brought into being (Limit the energy)
P3: Substitute with less hazardous material Business
P4: Prevent build-up of energy
P5: Prevent the release of hazard that already exists
P6: Modify the rate of release of hazard from its source
P7: Separate in time or space the hazard and that to be protected
P8: Separate the hazard and that to be protected by interposition of a material barrier
P9: Modify basic relevant qualities of the hazard

An example from chemical industry is given in Figure 2. The traditional concept of mining risk in chemical plant is by providing layers of protection to protect people, property and environment from hazardous materials, storage and installations.

4. Procedures for design for safety

The process of design for safety has been evolving. The evolution is taken place in terms of development of tools and techniques and procedures of implementation. As implementation issue is industry/plant specific, the procedures may differ from industry to industry, plant to plant, and also for section to section.

A general framework (step-wise) is as follows:

Step-1: Understand your worksystem, plant, or organization in depth.
Step-2: Identify hazards and hazardous sources
Step-3: Develop framework to quantify the occurrence of hazards and hazardous situations
Step-4: Anticipate likely accident scenarios based on hazard potential and system protection configuration
Step-5: Anticipate likely losses against each scenario and develop a framework for their quantification
Step-5: Quantify risk and make decision for each scenario
Step-6: List down unacceptable accident scenarios based on risk-based decision
Step-7: Prioritize scenarios for minimizing risk
Step-8: Consider the highest risk scenario and correlate with the hazards causing the risk
Step-9: Prioritize hazards based on risk contribution
Step-10: Consider the most risky hazard and identify feasible design principles
Step-11: For each design principle applicable, identify available design solutions
Step-12: For each design solution, plan out its technical and economic feasibility

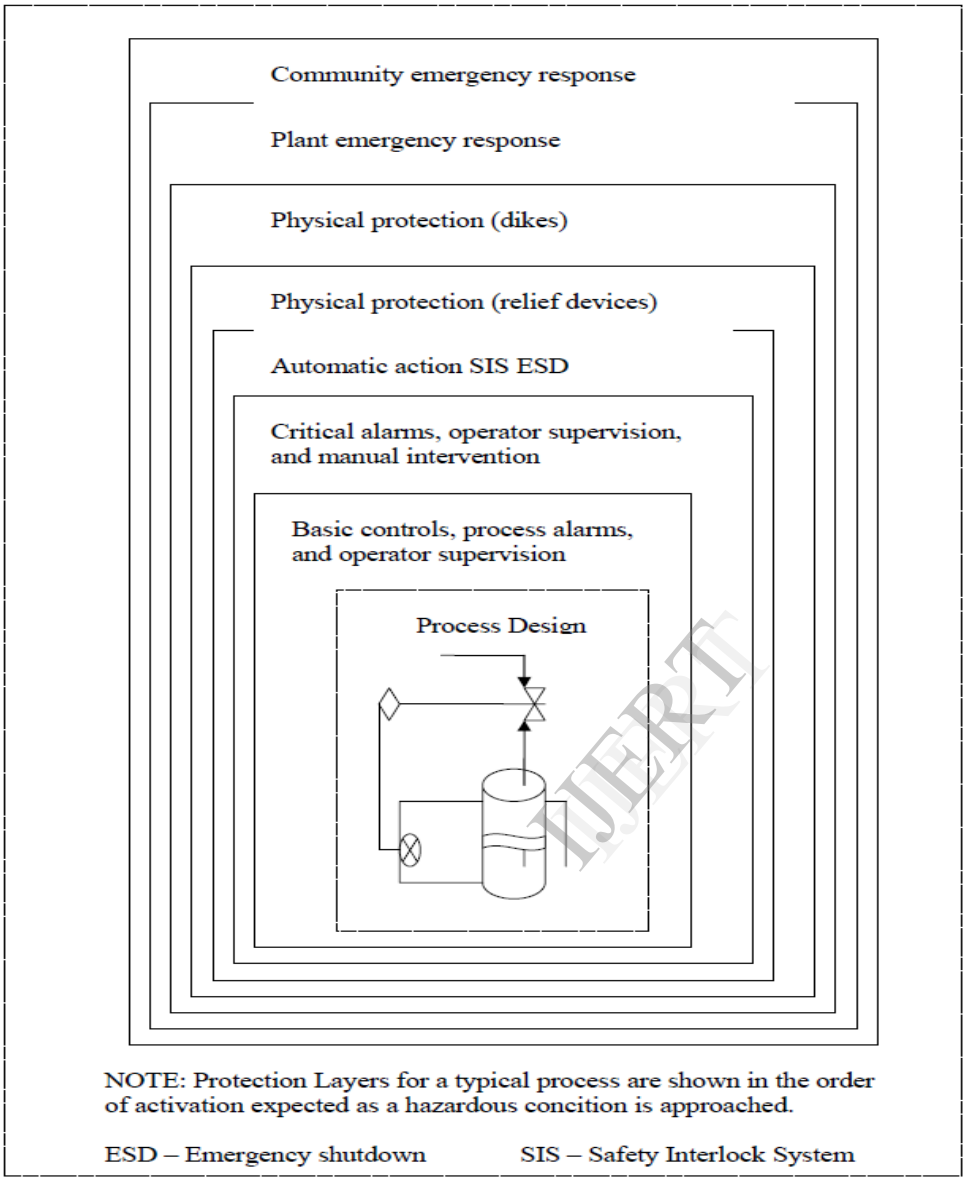

Fig. 2: Example layers of protection for a chemical process (adopted from Hendershot, D. C.,1999).

Step=13: Rank the design solutions and chose the best ones
Step-14: Repeat the process for other hazards
Step-15: Repeat the process for other scenarios
Step-16: Check dependency amongst design solutions (coupling) as and when required in the previous stages.

5. Conclusions

This paper describes the conceptual framework for System Safety Management for Safety Design. The concept of safety design is not new but what is missing till date that there is no clear cut approaches to guide for designing and implementing worksystem safety. The steps given in this paper is therefore valuable for both design and manufacturing/production engineers.

6. References

[1] Haddon, W. J. Jr. (1966). The prevention of accidents. Preventive Medicine. Boston, Little Brown.
[2] Hendershot, D. C. (1999). Safety through design – Application in the chemical industry. In Safety Through Design (Eds. Christensen W C and Manuele F A). National Safety Council (NSC), NSC Press, pp 195-215.
[3] Manuele, F. A. (1999). What is safety through design: what's in it for you? In Safety Through Design (Eds. Christensen W C and Manuele F A). National Safety Council (NSC), NSC Press, pp 3-8.
[4] John Ridley (2003). Safety at Work. (Taylor & Francis)