Practising **Safe** Engineering

By Ir. Ke Geok Chuan, Director, Forensic Engineering Division, DOSH Malaysia

Adoption and upholding safe engineering practices can mitigate a number of disruptive engineering failures and incidents. Utilisation of hazard and risk analytical tools at the design stage, and lessons learnt from past reported cases can also help in enhancing safe engineering practices for the overall benefit of the community.

Safety is defined as free from harm or risk of injury. Unfortunate engineering failures and incidents have contributed to unnecessary loss of life and serious damage to properties, casting a pall over the public confidence in the engineering profession.

Engineers who design, or make, or put to practical use products in the workplace should ensure the safe design, fit for purpose, and safety of use through safe engineering practices. This requires understanding the risk, the analysis of the severity of the risk, evaluation of proper protective measures, compliance solutions and means to acceptable standards and codes, maintenance regimes to be instituted and training to be provided to personnel.

Safe engineering involves all relevant branches of engineering and specialists capable of assessing, designing and project managing all aspects of the products in the workplace. Practising safe engineering can improve the safety of work sites, manufacturing facilities, work environment and products as regulations and safety standards change and assure that engineered systems can still provide acceptable levels of safety. The term product is used here to refer to any designed system, plant, component, part, or something that is engineered, manufactured, constructed, fabricated, imported or processed and that is usually sold to user. A system is an orderly arrangement of components that interact among themselves and with external components, other systems, and human operators to perform some intended function. An industrial plant may be treated as a system consisting of a number of components or as a super-system consisting of a number of systems. [5]

DUTY OF CARE

Engineers owe statutory duty of care to persons at work, other persons, and the public at large. [2], [3], [6] To discharge such legal obligations, to the standard as far as practical they have to ensure all reasonable and proper steps have been taken; for example, beginning at the conceptual stage to evaluate the risk of a petroleum processing system and to ensure that all the legal and contractual requirements, including the non-mandatory requirements such as management systems and safe engineering practices, have been duly complied with and followed respectively. While statutes and regulations may differ to some degree or intent, all without exception are concerned with ethical practice of engineering as it relates to public safety, health and welfare. These requirements are the cornerstone of sound engineering practice.

Technical expertise is indispensable for a professional engineer but at the same time detailed knowledge is worthless without the skills to properly employ it or the ability to convince people and the industry that its fruits are worthwhile.

Thus engineers should work closely with the clients at all levels to develop practical compliance solutions and strategies to safeguard mutual interest. They have to accept responsibility for making safe engineering decisions that conform with safety, health, and welfare requirements of the public and disclose promptly active and latent factors that might endanger the public or the environment.

There should be no compromise for any slack or shortcomings in their statutory and professional duties. Failure to comply could lead to punitive action to be taken by the relevant enforcing authorities or professional bodies.

ADOPTION OF HAZARD AND RISK ANALYSIS METHODOLOGY

All too often products have been built in which attention to hazards, safety, and loss prevention have not been given as much attention as it has to performance in the design of the components. The purpose of a hazard and risk analysis of a product is to study the effects that each component has on the operation of every other component and the independent effect that each component has on the working of the product. [5]

What are the hazard and risk evaluation requirements of products that can be used and followed by the engineering profession? Engineering professionals must have specific and value-added knowledge of the plant, processes or the system, risk, complexities, intricacies and a host of others. Each of these areas concern the engineering background and together are essential in establishing, controlling, maintaining and sustaining a safe environment or safe workplace.

When undertaking hazard and risk analysis, engineering professionals must also have knowledge of the vicissitudes of the engineering phenomenon and the environment which precipitate accidents. They must be able to recognize the hazards or risks in an operation before they result in accidents. Thus they must possess an understanding of pertinent safety requirements, safety codes and safety standards, management system and also global good engineering practices.

Here it is appropriate to emphasize that safe engineering is controlled risk-taking. Under this concept, engineering professionals implement hazard and risk control so as to limit accidental harm to people, products, environment and property. Prevention is not the key here, but limitation of hazards and risks are. An effort to control hazards and risks may produce their eradication, but not always.

Safe and sound engineering concepts applied to hazard and risk mitigation principles are an obvious and effective way to control construction mishaps, for example. Once the source of hazard or risk is apparent, the provision and use of safe engineering controls during design, manufacturing, erection, construction and usage to mitigate or eliminate the dangerous conditions means product, personnel, environment and the community are no longer threatened by that particular hazard or risk.

There are several methods available for performing the hazards or risks analysis and reducing the risks to a level as far as practicable. The most common types include Fault Tree Analysis (FTA), and Failure Mode and Effects Analysis (FMEA) which were briefly illustrated and explained here.

FAULT TREE ANALYSIS

A Fault Tree Analysis (FTA), also known as cause-and-effect analysis (Fig. 1.0) is one of the complex analytical tools to determine the inter-relationships and outline the possible sequence of events between the different possible causes contributing to a potential or actual failure. A FTA is a deductive, top-down method of analyzing product design and performance. It starts by specifying a top event to analyze (such as an overpressure),

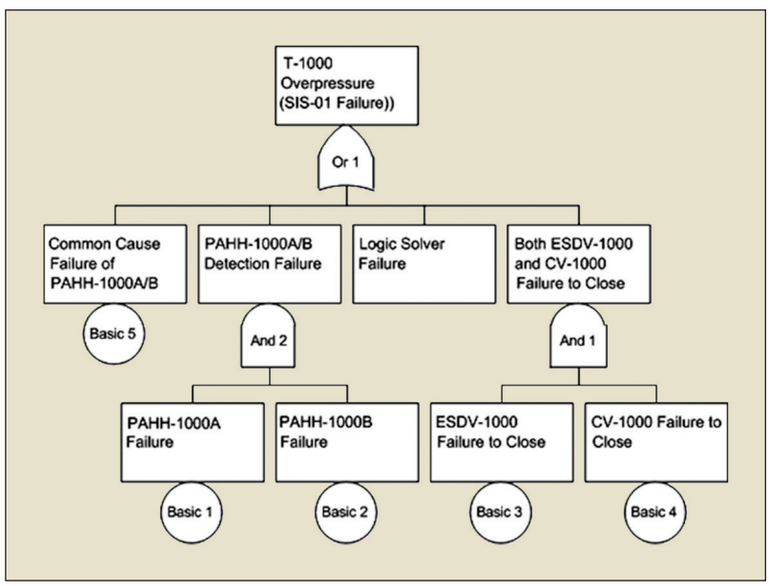

Figure 1.0: Fault Tree diagram showing causal connections for an overpressure process system.

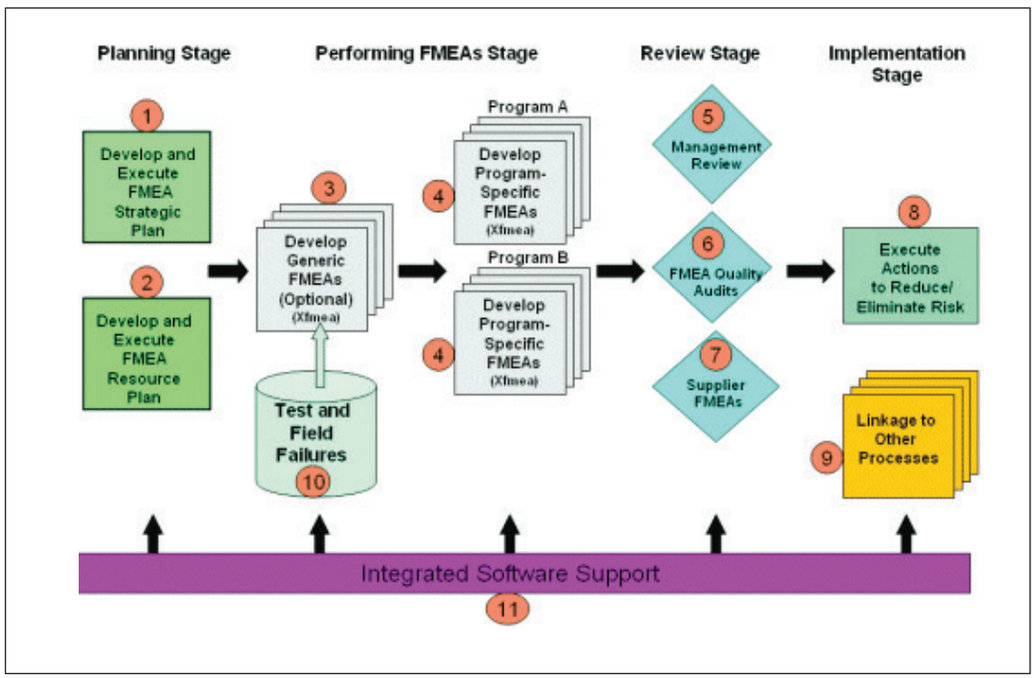

Figure 2.0: A typical effective FMEA process diagram.

followed by identifying all of the associated elements in the product that could cause that top event to occur. Fault trees provide a convenient symbolic representation of the combination of events resulting in the occurrence of the top event. Events and gates in fault tree analysis are represented by symbols. The entire product, as well as human interactions, are analyzed when performing a fault tree analysis. While building the fault tree and performing the analysis, a review of information regarding codes, standards, and research documents associated with processes, procedures, and equipment for the product, along with the human interface and factual evidence relevant to the actual and potential accident event, is required. [4], [5], [7].

Figure 1.0 is an example of basic fault tree logic.

Fault-tree diagram is useful. It allows the process system engineer and his team to plan and undertake the hazard and risk analysis systematically, and provides a logical path to follow during the analysis on the product.

FAILURE MODES AND EFFECTS ANALYSIS

Failure Modes and Effects Analysis (FMEA) is a simple but useful tool or method for considering potential and actual failure modes in a product in a systematic and rational way. Potential problems can be tackled at an early stage in product design and development which is safe engineering practice rather than in a panic after the occurrence of a failure. The method stands a much greater chance of success in solving problems if the engineers know how to recognize defects, and how to correct them once identified. The findings of a FMEA evaluation are then recorded in tabular form or on a FMEA work sheet.

This technique is widely used in many industries and is required by many standards and codes of engineering practice. Next, a ranking evaluation of the various ways to reduce potential and actual risk of the product is assessed.

OTHER HAZARD AND RISK ANALYTICAL TOOL OR SOFTWARE

Further information on the hazard or risk analysis techniques appropriate to different project stages for a typical process plant is as provided in Table 2.0.

Currently, many engineering software tools integrate the use of fuzzy logic and expert database with FMEA. They may prove helpful to system safety and reliability analysts who conduct FMEAs to prioritize potential or actual failures and for corrective or remedial actions to be followed and taken on products.

A number of technical societies, industrial organisations, regulatory agencies, training and research organisations, and consultants produce publications on these methods.

Project stage	Hazard or risk identification technique
All stages	Management and safety system audits Checklists Feedback from workforce
Pre-design	Hazard or risk indices Insurance assessments Hazard or risk studies (coarse scale)
Design	Process design checks Unit processes, units operations Plant equipments Pressure systems Instrument systems Hazard and operability studies (fine scale) Failure modes and effects analysis Fault trees and event tress Hazard analysis Reliability assessments Operator task analysis and operating instructions
Commissioning	Checks against design, inspection, examination, testing Non-destructive testing, condition monitoring Plant safety audits Emergency planning
Operation	Inspection, testing Non-destructive testing, condition monitoring, corrosion Monitoring, malfunction detection, plant degradation audits Plant safety audits

Table 2.0: Hazards or risk identification techniques appropriate to different project stages [7]

> *Unlike the fairy tale Rumplestiltskin, do not think that by having named the devil that you have destroyed him. Positive verification of his demise is required.*

VERIFICATION OF SAFETY

"Unlike the fairy tale Rumplestiltskin, do not think that by having named the devil that you have destroyed him. Positive verification of his demise is required".

Source: System Safety Handbook for the Acquisition Manager, U.S. Air Force

Through safe engineering the test plans and recommended actions on products must be reviewed at regular intervals based on hazard and risk analyses, regulations, safety standards, inspection checklists, previous failures and incidents, and interface analyses. The safety effort should specify the detailed conditions under which tests are to be conducted. The engineers should review test results for any safety-related problems that were missed out in earlier analyses or other testing and monitor tests for unexpected failure modes and hazardous states.

DOCUMENTATION

One of the important steps in safe engineering practice is to collect, compile and manage all the prepared technical materials including sources of information, codes, standards, drawings, references, method statements and assumptions for the products. As this information may be reviewed by many different persons or parties from various backgrounds and disciplines, its organisation should be accessible and understandable by all. The key to this information organisation and management is simplicity to allow for timely and effective dissemination of correct and updated information and facilitating communication during meetings and conduct of site trainings.

REPORTED FAILURE AND INCIDENT CASES

Finally, this technical paper emphasizes the importance of documented forensic engineering investigations on failure and incident cases. Lessons learnt from such investigations provide an invaluable resource for the designer, engineer, operator, contractor, and others to improve engineered products by reducing risk or eliminating hazards or risks.

FAILURE OF ENGINEERING AND CONSTRUCTION STRUCTURES

In recent years there have been number of high profile engineering and construction failures such as the collapse of false work structure for the Batu Maung interchange work for the Penang Second Bridge project (Photo 1.0), collapse of the West Wing of the Sultan Mizan Stadium, Trengganu during the demolition of the space frame structures, collapse of hypermarket's floor slab temporary support structures during concreting work in Johor, and others.

Similar cases can be avoided or prevented from happening again by having engineers who have been appointed for the mega-project construction work to prepare and undertake first the hazard and risk evaluation for the product. The preparation of amended construction or workshop drawings with complete supporting calculations, and method statements should highlight the outcomes from the hazard and risk analysis report. The client will then have an Independent Consultant to undertake thorough checks on the proposal. Engineering drawings of the products will also be scrutinized and proper care taken to ensure that checks

Photo 1.0: Front view of the scene showing collapse of supporting false work structure for Batu Maung Interchange work, Penang Second Bridge project

and validation to the regulations, specifications, calculations, dimensional tolerances have been made. In addition, the consultants should review all risk evaluation reports to ensure that the products have not contributed to, or have caused problems later on during the construction phase.

During the construction stage, proper steps must be taken to ensure that all personnel involved in the execution, inspection, supervision and management of the project possess the relevant and requisite competency, skills, expertise and knowledge. Lastly, but not least safe engineering practices must be upheld at all times during the duration of the construction work.

In the case of demolition work, available standard MS 2318: 2012: Demolition of Buildings-Code of Practices should be followed by all parties involved in the work. Complete and detailed construction drawings for the building or engineering structure to be demolished with the structural stability analysis report and dilapidation survey report (if available) that have been undertaken to be handed over by the client to the contractor or its appointed consultant.

The failure and incident cases that have occurred in the construction industry covering a period of 20 years bring into focus the low priority placed by the industry stakeholders. There were 20 serious incidents which caused 74 fatalities and 54 injuries from 1993 to 2013 (Table 1.0). Except for the Highland Tower incident that occurred post-construction, all other incidents occurred during the construction of the projects.

COLLAPSE AND FAILURE OF HEAVY LIFTING MACHINERY

In recent years there have been several cases of serious tower crane failures and sudden failure of lattice boom members of crawler cranes (Photo 2.0) in construction sites around the Klang Valley. In the latter case, it was determined that the failed machine had undergone extensive and improper repairs and welding on the lattice load bearing members.

No.	Incident Details	Year	Fatalities	Injuries
1.	Collapse of Highland Tower Building, Taman Hillview, Ulu Klang	1993	48	-
2.	Collapse on Putra-LRT Launcher, Bukit Gasing, Petaling Jaya	1996	-	2
3.	Collapse of formwork during concreting in KL Sentral project, KL	2005	-	2
4.	Fall of steel system formwork from 20-storey building, Plaza Damas on the public, KL	2006	1	1
5.	Collapse of eight 40m long and 70 tonnes huge concrete beams near Nilai collapsed.	2007	-	-
6.	Collapse of loading/working platform, Kipmart project, Tampoi	2007	3	-
7.	Collapse of scaffoldings at the Pavilion shopping centre project, KL	2007	2	10
8.	Collapse of gondolas at a project site, Bukit Antarabangsa, Selangor	2008	3	-
9.	Collapse of floor slab during concreting, 23-storey hotel, Kuching	2008	-	6
10.	Collapse of TNB transmission tower during installation, Kapar	2008	1	1
11.	Collapse of TNB ERS tower during installation, Inaman, Sabah	2008	1	4
12.	Collapse of scaffoldings, Ukay Perdana, Selangor	2008	-	12
13.	Collapse of Jaya Supermarket during demolition work, Petaling Jaya	2009	7	5
14.	Collapse of tower crane onto public area, Penang	2010	2	-
15.	Collapse of concrete floor slab, UMT, Terengganu	2009	1	-
16.	Collapse of formwork slab during mass concreting, NU Sentral project, Kuala Lumpur	2011	-	1
17.	West wing Stadium roof collapse during dismantling work, Terengganu	2013	-	5
18.	Batu Maung Interchange (Package 3A) False work collapse, Penang	2013	1	4
19.	Collapse of excavated slope on the worker, Sierra Ukay, Ampang	2013	3	1
20.	Mydin Hyper-mart Floor Slab Collapse, Johor	2013	2	-
TOTAL			74	54

Table 1.0: List of serious construction and engineering failures and incidents in Malaysia

Photo 2.0: The crawler's lattice boom structure failed and landed on the car.

Safe engineering practices on the machine, structures and component bearing loads and safety engineered devices would have confined or localized the failure. Undertaking safe engineering practices ensures that the design and condition for the repairs of the machine have been exhaustively examined, checked and validated within the required regulations, standards and code of practices and documented repair procedure. Ageing assessment of plant and equipment in use if properly managed will ensure their continued strength and integrity.

Also, any machine equipped with an electrical or electronic device that signals a machine to stop or an interlock should be examined and signed off by an authorized person or Professional Engineer (PE) as is practiced in some countries.

COMBUSTIBLE DUST EXPLOSIONS

The safety of such hazardous plant or product begins with the planning stage covering design, installation, hazards and risks analysis to the usage of appropriate non-explosion safety devices compliance to standards, proper earthing and bonding systems, and appropriate management, use and maintenance of the system by competent and trained personnel.

The real point of these incidents, ranging from grain dust (wheat, corn) to metallic (aluminium) and wood dusts that have occurred in Malaysia at regular intervals, requires all engineering professionals to know all that needs to be known about the presence of combustible dusts that exist in the industrial environment. Photo 3.0 shows a typical combustible dust explosion that happened in a factory in Penang involved in processing magnesium stearate (MgSt) and zinc stearate(ZnSt) materials. The explosion and ensuing fire caused widespread and heavy damage to the factory's processing plant with the loss of three lives and serious injuries to two workers.

Stringent fire safety engineering as per local fire regulations includes installation of fire-fighting systems, providing adequate means of escape, and fire detection and warning methods. Such combustible dust installations, with a high risk

Photo 3.0: Scene after the explosion and fire in the MgSt and ZnSt processing plant.

of explosive atmospheres being present, require engineering specialists capable of assessing, designing and project managing all aspects of potentially explosive process risk. There is a Malaysian Standards, MS IEC 60079-10-2:2010 for such combustible dust atmospheres which engineers and plant owners should follow.

Process system safety is concerned with understanding the consequences of failure as it affects people, environment and property. Hence, for such combustible dust process plants the engineers must undertake assessments of the risks associated with the zoning and location of a product (system), relative to people and other highly hazardous systems. This is important in the design of safe systems to determine what can go wrong and how to mitigate actual or potential losses.

Consequently, chemical plant and refinery explosions that have happened globally in the past have brought about inherent safer design concepts which are similar to process safety systems in the mitigation, if not the elimination of hazards, but are primarily directed toward the controlled release of unwanted energy.

CONCLUSION

Hazard and risk analysis requirements have to be taken seriously by engineering professionals if they are to achieve the goal of reducing product failures. Too often the method is given lip service as a mere paper exercise, so that serious failures continue to plague specific industries.

The aforesaid engineering failures and incidents that have given rise to fatalities, serious injury or property losses including incidental and consequential losses, can be mitigated if safe engineering practices are adopted and upheld. It clearly follows that hazards and risks arising from product are foreseeable and, if failure were to happen, they can be mitigated or localized and will not lead to the total failure of the product.

This paper also illustrates briefly how forensic engineering investigation can play an important role in reducing risk and improving technology

adopted for safeguarding the safety of workers, the public, the environment and property.

As society becomes more complex and as technological advancement improves the well-being of the community, the public expects engineering professionals to mitigate, if not prevent accidents and their resultant costs, loss of production and lowering of morale. Safety gains can be made when engineering professionals, exert a strong influence throughout the decision making process and ensure the consequences arising from hazard and risk are controlled to the level as far as practicable.

According to the Occupational Outlook Handbook, about 7,000 mining safety engineers and 23,000 safety engineers are employed in the United States. Safety engineers work in architectural firms and engineering design companies. The engineers also are employed at construction work sites, mines, and manufacturing facilities.

Practising safe engineering is the right thing to do and is the smart choice moving forward. Many countries require or promote safe engineering. National organisations and local professional bodies can work together to create tools, eliminate barriers, and facilitate adoption of this important practice in Malaysia. ■

REFERENCES

1. The Safety Engineer, Vol. VII, Number 2, ASSE Journal, February 1962
2. Occupational Safety and Health Act 1994, Act 514
3. Board of Engineers - Guidelines for Code of Professional Conduct
4. Guide to Best Practice for Safer Construction-from Concept to Completion, Engineers Australia.
5. S.Brown/Engineering Failure Analysis 14(2007)
6. Kevin W.Bowyer, Irah H.Donner/Practicing Safe Engineering
7. Lees FP/Loss Prevention in the process industry
8. Carl S.Carlson/FMEA Success Factors: An Effective FMEA Process