LINKING ENGINEERING STANDARDS WITH PROCESS SAFETY MANAGEMENT SYSTEMS

Ian S. Sutton

Southwestern Books, Houston, Texas

ABSTRACT

The techniques of Process Safety Management (PSM) are now an integral part of the operations of process plants in the United States. As the name implies, Process Safety Management is fundamentally a *management* standard; it provides a framework which plant management can use to minimize the number of uncontrolled deviations from design or operating intent. As a management standard, PSM tends to be most effective in areas involving the performance of human beings and organizations — for example, operating procedures, training and the control of contract workers.

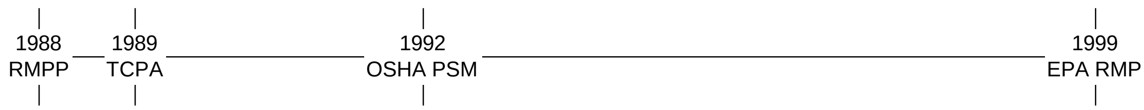
However this management focus of PSM, along with the non-prescriptive nature of the regulations in this area, means that process safety decisions tend to be based on the judgement and experience of the people working at a site or on a project. These decisions may lack quantitative, engineering rigor.

This paper suggests that the integration of engineering standards from organizations such as ASME, NFPA and API can help improve the quality of process safety analyses. Similarly, the use or process safety techniques will help design engineers utilize those same standards more effectively during the design process, particularly when a variance is being called for. The paper will discuss how Process Safety Management and Engineering Standards can be linked to one another to create a powerful, practical and useful synergy.

INTRODUCTION

For process safety professionals in the United States, the 1990s have been a decade of regulations. Some of the major regulatory events are shown in Figure 1.

Figure 1



The first regulation was California's RMPP (Risk Management & Prevention Program), followed by New Jersey's TCPA (Toxic Catastrophe Prevention Act). However, for most companies in the process industries the key historical event was the promulgation of OSHA's Process Safety Management (PSM) standard in 1992. The decade closes out with the EPA's Risk Management Program (1999).

All of these standards were retroactive, *i.e.* companies had to implement them within existing facilities, typically within a very short period of time. Since many companies were a long way from being in compliance when the standards were introduced, the upshot was that they were forced into extensive "retro-fit" or catch-up work.

With the compliance phase of process safety coming to an end, it is probably fair to claim that, in general, progress toward meeting the regulatory requirements has been good — although results do vary enormously from company to company, and from site to site.

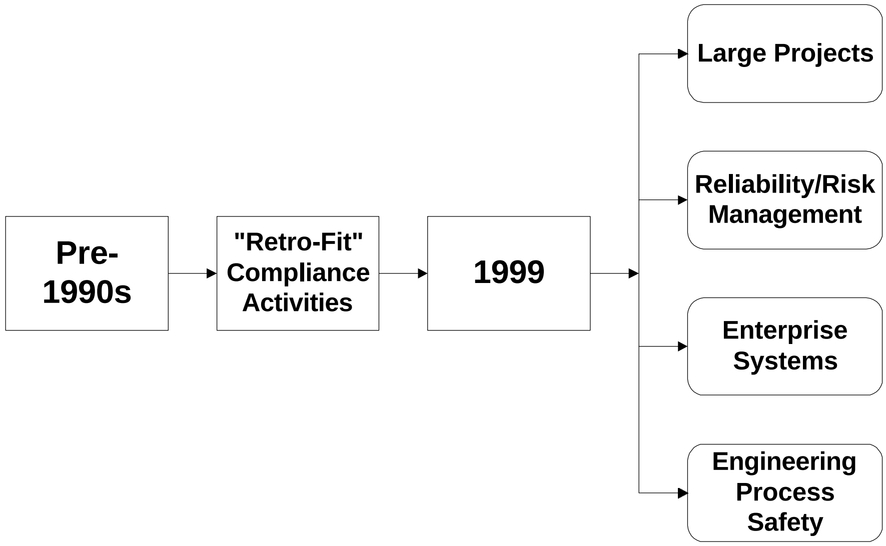
Naturally, there is always room for improvement — safety can never be "good enough", and risk can never be zero. Three areas in particular — Operating Procedures, Process Hazards Analyses, and Mechanical Integrity — continue to draw a disproportionate share of penalties from OSHA [1], and there are always on-going process safety activities such as:

- Regular audits.
- Revised operating procedures for new or changed operations.
- Process Hazards Analyses.
- Updating Process Safety Information.
- Training of new employees.

Nevertheless, in spite of these on-going activities, now is a good time for those companies that have broadly achieved compliance to catch their breath, review what they have achieved, and decide how to develop their process safety programs in the coming years. Some options are shown in Figure 2.

Figure 2

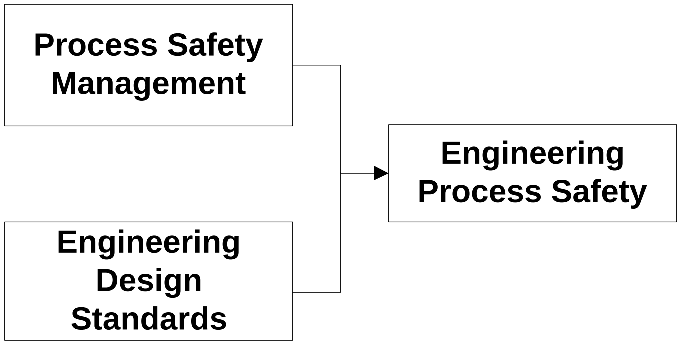
Areas for Developing Process Safety



This paper discusses the fourth of the options shown in Figure 2: the linking of process safety management with engineering standards. The term "Engineering Process Safety" has been used [2] to describe this concept — which is illustrated in Figure 3.

Figure 3

Elements Of Engineering Process Safety



PROCESS SAFETY MANAGEMENT

The principles of Process Safety Management are explained in standard references on the topic, including those from Sutton [3], and in the many publications from the AIChE-CCPS [4]. Some of the key features of process safety management — particularly as they impact Engineering Process Safety — are outlined in Table 1.

Table 1

Features Of Process Safety Management

MANAGEMENT STANDARD	Process Safety Management is basically a *management* standard. Process safety regulations rarely provide detail as to how a facility should be run — instead they require that managers design, implement and administer a program that is appropriate to the specific needs of a site. Hence process safety must contain the basic elements of any management program, including setting goals, assigning resources, development of a schedule, and regular audits. Being a management standard, process safety is not fundamentally about safety as such — it is about making sure that the managers and employees are in control of the plant for which they are responsible. They know what they want to do, and they set about doing it. When they are in control, all aspects of the operation — safety, production, productivity and environmental performance — will improve.
NON-PRESCRIPTIVE	Process safety regulations are generally non-prescriptive, i.e. they provide very little detail as to what actions to take. OSHA and the other regulatory authorities recognize that they cannot possibly write regulations that are sufficiently detailed to cover the myriad of covered processes and operations. Therefore the regulations simply require that management at each facility develop and administer a program that results in a safe operation; the details will be worked out by the managers and employees.
PERFORMANCE-BASED	Because process safety is non-prescriptive, it must be performance-based. Since no detailed performance parameters are provided, the only way of measuring success is through overall results. If a facility has an accident it is, by definition, out of compliance. (However, the opposite is not true; no plant can ever be perfect, therefore no plant can ever claim to be truly in compliance. The only measure of success is success.)
HUMAN PERFORMANCE	Process safety emphasizes issues such as operating procedures, training and contractor management. The focus on human issues could help explain some of the difficulties with implementing process safety. Many managers have a technical background, and do not have the training to handle “soft” issues.
OPERATIONS FOCUS	Because process safety has been a catch-up activity for most companies during the 1990s, most attention has been paid to improving or “retro-fitting” existing processes. For example, in most of the literature to do with Management of Change, there is an implicit assumption that what is being changed physically exists, i.e. an item of equipment that is currently operating is to be modified in some way. Yet change is constantly occurring during the design phase of new projects. Engineering companies usually have well-established change management programs, but generally these have not yet been effectively linked to Management of Change procedures.

CREATIVE	A well-run process safety program encourages all employees to "think the unthinkable", and to come up with new ways of operating. Creative thinking is usually generated through team activities such as Process Hazards Analyses.
QUALITATIVE	Process safety activities are generally qualitative. Many of the elements, such as operating procedures and training, are difficult to measure quantitatively. Lack of quantification can lead to circular reasoning, as can be seen with the following example to do with Process Hazards Analyses: 1. Could high pressure lead to an accident? 2. What is high pressure? 3. High pressure is that pressure which could lead to an accident.

ENGINEERING DESIGN STANDARDS

Engineering Design Standards are published by authoritative organizations and professional bodies. Table 2 described some of the salient features of Process Safety Management. The corresponding features for Design Standards are shown in Table 2, and compared with their process safety equivalents.

Table 2

Features Of Engineering Design Standards

PROCESS SAFETY	**ENGINEERING STANDARDS**	
MANAGEMENT STANDARD	*TECHNICAL STANDARD*	Engineering Design Standards are primarily technical. They are not concerned with the management of process plants. As with Process Safety, however, Design Standards are not just about safety. If a plant is well designed and well constructed, all aspects of its performance will be enhanced.
NON-PRESCRIPTIVE	*PRESCRIPTIVE*	Engineering standards are prescriptive — they provide specific, detailed guidance as to what must be done. They do not allow much scope for individual initiative or for making choices.
PERFORMANCE-BASED	*COMPLIANCE-BASED*	These standards are also concerned primarily with compliance to the prescriptive standards — not with an overall quality performance goal.
HUMAN PERFORMANCE	*EQUIPMENT*	Whereas Process Safety has a strong focus on human performance issues, Engineering Standards are concerned almost entirely with equipment specifications. Even in those areas in which humans are involved, the focus is on precise standards to do with human factors and ergonomics.

OPERATIONS FOCUS	*DESIGN FOCUS*	Engineering Standards tend to be most used during the design of new plants, and in major revamp projects.
CREATIVE	*PROCEDURAL*	Process Safety encourages initiative and creativity. Such is not the case with Design Standards, where a precise following of a set of rules is called for.
QUALITATIVE	*QUANTITATIVE*	Engineering Standards are quantitative. They provide numerical solutions to technical questions.

Five different levels of Design Standard are shown in Table 3.

Table 3

Levels Of Engineering Design Standards

REGULATIONS	Regulations must be followed — they are the law. However, regulations often fail to provide sufficient detail to serve as functional design standards. Military Standards are often an exception.
CODES AND STANDARDS	Codes and Standards are developed and published by professional bodies such as: • ASME (American Society of Mechanical Engineers) • NFPA (National Fire Protection Association) • API (American Petroleum Institute) • IEEE (Institute of Electrical Engineers) Documents from these organizations typically do provide. They are also authoritative; they may not have the direct force of law, but engineers must have good reasons for not following their guidance.
COMPANY STANDARDS	Company Standards are developed when a company has a proprietary process or chemical for which custom standards are needed because little or no public information is available. Company standards may also be written when management feels that publicly available standards are not appropriate for some reason.
OPEN LITERATURE	Many books, articles and papers on all aspects of design safety are published. Such publications can carry considerable authority, particularly if sponsored by a recognized society such as the Center for Chemical Process Safety (CCPS).
INDUSTRY INFORMATION	Industry Information can come from Trade Associations and from vendors. Trade Associations, such as the Chlorine Institute, collect and evaluate information from their member companies. This information can be invaluable because it is based on extensive experience. Vendors can also be very helpful. Naturally, they have a commercial ax to grind, but this does not mean that their insights and information are without value.

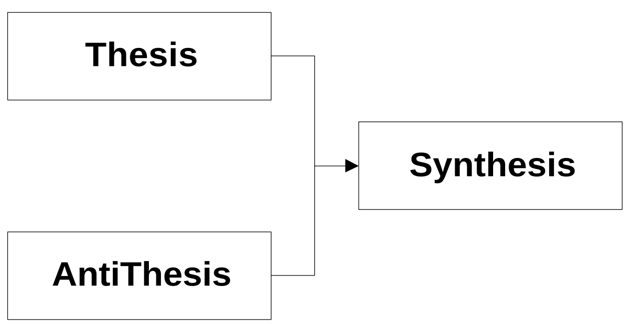
ANALYSIS	Finally, engineering systems can be analyzed from first principles to see if a proposed design is safe or not. Analysis is often used when it is suspected that the situation in question is outside the standard's normal range. For example, an NFPA standard may provide guidance as to how far items of equipment should be from one another. However, if the fuel involved is an unusual chemical, a fire model can help determine what the safe distances from a fire should be.

ENGINEERING PROCESS SAFETY

Figure 3 showed how Process Safety Management and Engineering Design Standards can be combined to create Engineering Process Safety. When such a combination results in a new concept that has its roots in the two original topics but that is different from either, a *dialectic* or *Hegelian synthesis* has taken place, as shown in Figure 4 [a]

Figure 4

Hegelian Dialectic



[a] Hegel was a German philosopher who lived from 1770-1831. He postulated that all progress comes from the resolution of tension between opposites. In his terminology, the two original ideas are the Thesis and AntiThesis. Their resolution is referred to as a Synthesis, as illustrated in Figure 4. The discipline of chemical engineering is itself a fine example of an Hegelian dialectic. By the end of the 19^{th} century the science of chemistry had made great strides, with many new processes ripe for commercialization. However, chemists did not know how to scale up their bench-scale processes by the many orders of magnitude needed in order to build chemical plants. In response to this problem — the Thesis — mechanical and civil engineers provided their expertise on topics such as equipment and foundation design. Although their contribution resolved some of the problems of commercializing chemical processes, they were unable to address unique problems such as the calculation of the number of trays in a distillation column. Hence these traditional engineering disciplines were the AntiThesis. The Synthesis that rose from this tension in the 1920s and 30s was the discipline of chemical engineering, which contains within itself elements of both chemistry and traditional engineering, but is separate and distinct from both.

FEATURES OF ENGINEERING PROCESS SAFETY

For the synthesis of Engineering Process Safety to be effective, it must address those situations that cannot be completely resolved by the sole use of either Process Safety Management or by the use of Engineering Design Standards. Some areas to consider are discussed below.

Management Discretion

Managers sometimes find themselves under pressure to make decisions that do not strictly adhere to the standards that their company has declared it will follows. For example, a Production Manager may be asked to increase production rates of a certain chemical by increasing a reactor's temperature to a level not seen before. He has to decide whether this decision is acceptable with regard to safety.

His first step is to evaluate the design in terms of Design standards. He will ask a mechanical engineer to check the Maximum Allowable Working Pressure of the reactor at the new temperature (using ASME Section VIII, Division 1or some other authoritative standard such as API 510), and to check on relief valve sizing (using API 520). He may also ask an Instrument Engineer to make sure that the emergency response system can still respond quickly enough (ISA 84 may be used for this.)

The manager's next step is to use process safety techniques to provide another "view" of the same decision. He may choose to assemble a Process Safety team (which will include the mechanical and instrument engineers) to conduct a qualitative analysis. The team will consider issues such as whether the operators need more training, or whether the current Emergency Response Plan is adequate in the event that the high pressure does lead to an accident. The team may also choose to review incident data from other, similar facilities.

Having "framed" the problem in terms of both Engineering Design and Process Safety, the manager is now in a position to agree or disagree to the request to increase reactor temperatures. He still has a decision to make, but the decision will be as informed as possible.

Multi-Discipline Issues

The example provided in the previous paragraph was quite simple, yet it illustrated one of the major problems to be found in analyses such as these: the need to integrate input from different engineering disciplines, particularly when new equipment is to be installed. All but the most minor changes will require the involvement of experts from the electrical, mechanical, piping, instrumentation and process departments. On the operations side, personnel from operations, maintenance, safety and the laboratory usually need to be involved.

Related to the problem of multi-discipline input is that of resolving tensions between two or more standards bodies, each of which may give different guidance to a particular issue. For example, if a company wishes to install a new electrical transformer, the spacing requirements are discussed by two authoritative bodies: NFPA (National Fire

Protection Association) and IEEE (Institute of Electrical Engineers). These two standards are different, and can lead to different conclusions in certain situations.

There are two ways in which an issue such as the above can be resolved. First, other standards and experts can be invoked in order to see if they provide guidance. In this case, the Dow Fire and Explosion Index may be of use. Fire protection engineers may be able to add professional opinions.

The second method of resolving differences is through the use of process safety techniques such as Incident Investigation, Mechanical Integrity and Hazards Analyses. The resolution of the problem can also be aided can also be supported by input from professional associations and transformer manufacturers.

Design / Operations Integration

By integrating design and operating disciplines, both can help one another. For example, on many projects, the design engineers do not have sufficient operating experience to know how to write the operating procedures for the items that they are designing. However, the operating personnel do know how the plant should work, and they should have an Operating Procedures standard. They can help the designers come up with a plant that is workable and safe.

On the other side, design engineers can help the operating disciplines. For example, the problems that PHA teams face with terms such as “high pressure” can be resolved if knowledge of maximum allowable working pressures can be provided by the designers.

Similarly, if an operations team is evaluating the effectiveness of a Hot Work procedure such as cutting a pipe, the team members can supplement their own knowledge and experience with information and instructions from the many OSHA regulations to do with Hot Work and Line Break policies.

LINKING ENGINERING STANDARDS WITH PROCESS SAFETY

Based on the above discussions, the following four-step approach can be used to implement Engineering Process Safety.

1. Areas Of Application
2. Design Safety Requirements
3. Process Safety Analysis.
4. Synthesize Resolution.

1. Areas Of Application

The first step is to identify suitable area for the application of the techniques discussed above. These will often be areas where management is not able to directly follow a code direction if they want to make an improvement. Representative example area include:

- Raising production rates (as discussed with the increased reactor pressure above). Such decisions often place the operation in a range that it has never been at before, so there are questions as to the safety of the new conditions.
- Equipment spacing is a chronic problem for many companies. Rather than build new plants, they choose to expand the facilities that they already own. Unfortunately, there is often not enough space in which to install new equipment while adhering to design standards (usually because some other equipment is in the way, or because the expansion is near a property limit). Not only are there standards to do with secondary containment, but process safety items such as emergency response can help define a resolution.
- Secondary containment (such as dikes and containment walls around tanks) can create design problems. For example, it may be proposed to reduce the size of the containment area by having pumps available to remove any spills.
- Fire damage limits are provided by code bodies such as NFPA. However, many plants handle very specialized chemicals, and it may be appropriate to develop mathematical models to provide a "second opinion" regarding the standards. The use of DIERS technology to supplement standards such as API 520 is another example of this type of cross-check.

2. Design Safety Requirements

The next step is to determine what engineering standards and guidance are available. Some standards are well known, but others (particularly information from vendors) may not be known about. An index is needed which will call out which standards are needed at which stage in the design process.

Once the standards have been identified, they should be categorized into those which are a "must do" (ASME standards are an example of this), and those which are more flexible (such as guidance from vendors or manufacturers). Those areas which can be properly assessed with Good Engineering Judgement should be clarified.

3. Process Safety Analysis

The techniques of process safety management can then be used to provide an independent and qualitative assessment of the decision process.

4. Synthesize A Resolution

Finally, the manager responsible for making the design or operating decision must pull together all the different types of input, resolve conflicts and tensions, and make a decision. The decision is not made for him by all the work that has just taken place, but it is as well bounded as possible — he is as well-informed as possible, hence everyone will have confidence in the final decision.

CONCLUSIONS

If the strengths of Process Safety Management (team work, creativity and performance-based results) can be combined with the rigor and objectivity of Engineering Design standards, a Synthesis of the two may result in which a new topic — Engineering Process Safety — may develop. This will draw on the features of both approaches to help process plant managers achieve higher levels of safety in the plants for which they are responsible.

REFERENCES

[1] Chemical Process Safety Report, October 1998

[2] Sutton, Ian S. Engineering Process Safety. Chemical Engineering. March 1999

[3] Sutton, Ian S. Process Safety Management. Houston, Texas: Southwestern Books, 1997.

[4] http://www.aiche.org/docs/ccps/