SAFETY CASES - OVERVIEW

In Brief

A Safety Case is not typically a mandatory requirement, especially in North America but without question, a Safety Case is a 'Best Practice'. That having been said some industries are now regulated to conduct 'Safety Cases'. Regulatory requirement is necessarily increasing as disaster after disaster, demand further safety precautions. Consequently, explicit Safety Cases are compulsory for various and diverse applications including but not limited to the nuclear industry, [off shore] oil and gas, military systems, rail, air, marine transport systems and pipelines to name but a few.

It is imperative that an adequate and comprehensive Safety Case is produced specific to a system, in order to demonstrate the overall safety of the particular system and/or a process. A Safety Case is a 'living document' that evolves over time in association with the 'safety life-cycle' of the operation. The Safety Case records the 'Safety Argument', the basic structure of which will remain similar throughout the Safety Case's evolution, regardless of how much the status of the evidence changes and evolves with time.

A Safety Case can be divided into several components covering specific subsystems, which in turn, refer to other supporting documents such as design documents, operating procedures, audit reports, corrective actions and other quality documents, reports and tests, etc.

Typically there are many variants of a Safety Case, but most, if not all, fall into one of two categories, as follows:

- those which are used to demonstrate the safety of an on-going service, are known as a **Unit Safety Cases (USC)**; and,
- those which are used to demonstrate the safety of a substantial change to that service (and/or underlying system), are known as **Project Safety Cases (PSC)**.

The two categories are interrelated, as explained below:

Unit Safety Case: An Organisation may decide to produce and maintain, a **Unit Safety Case** in order to show that the on-going, day-to-day operations are safe and that they will remain so indefinitely. A Unit Safety Case would include typically, a prior Safety Assessment (to show that a service and/or system is predicted to be safe) together with the results of safety audits, surveys and operational monitoring (to demonstrate that, up to that point in time, it actually has been safe). It should also validate that processes are in place to ensure that all future changes to the system and/or processes, will be managed safely via (*inter alia)* a Project Safety Case.

Project Safety Case: An Organisation may also decide to produce a **Project Safety Case** when a particular or substantial change to an existing safety-related service and/or system (including the introduction of a new service and/or system) is to be undertaken. A Project Safety Case would normally consider only those risks created or modified by the change and rely on an assumption (or evidence from the corresponding Unit Safety Case) that the pre-change situation is at least tolerably safe. A Project Safety Case is normally used to update a Unit Safety Case and is usually subsumed into it.

The proposed expansion plan should encompass the full production of a "Unit Safety Case", which would focus on the issues of the expanded operations, the overall facility and its consequent effects on the safety of the operation. Typically a formal Safety Case either 'Unit' or 'Project', is prepared by the project proponent or service provider to demonstrate to the

Regulatory Authorities, Clients and/or other interested parties - including the General Public - that a specific project or service, can meet all safety requirements as well as provide assurance that all risks can be managed to as Low As Reasonable Practical (ALARP). However, as Lord Justice Cullen wrote during his inquiry over the Piper Alpha incident:

"Primarily the Safety Case is a matter of ensuring that every company produces a formal safety assessment to assure itself that its operations are safe.

Only secondarily is it a matter of demonstrating this to a regulatory body. That said such a demonstration both meets a legitimate expectation of the workforce and the public and provides a sound basis for regulatory control."

Implicit to this obligation is the requirement on those with managerial control to demonstrate positively that the relevant Safety Regulations are satisfied. In essence, there is a "*burden of proof*" on Service Providers whether they are Certificated under (for example) Transport Canada or not certified to any specific criteria, to show that acceptable levels of safety are, and continue to be, achieved.

A Safety Case simply stated, is the documented assurance (i.e. argument and supporting evidence) of the achievement and maintenance of safety. It is the primarily means by which those who are accountable for service provision or projects, must assure themselves that those services or projects are delivering (or will deliver) and will continue to deliver, an acceptable level of safety. A Safety Case can also be envisioned as an extension of a truly effective Safety Management System (SMS).

In the context of a Safety Management System, the Safety Case can also be employed as a means of documenting and recording the 'effective safety' of a service and/or system. Conversely, the implementation of a SMS provides evidence to support a Safety Case. Although not completely mandated under the Canadian Aviation Regulations (CAR), most Certificate Holders have now implemented, to some degree or another, a recognisable SMS in addition to a Quality Management System (QMS). Nevertheless, it is not generally recognised that a Safety Case is a critical sub-component of a SMS (or its systems) and therefore, the Safety Case has only recently became common practice, as a result, of being endorsed by the former Minister of Transport – The Honourable Denis Lebel P.C., M.P.

Since a principal objective of safety regulation is to ensure that those who are accountable for safety discharge their responsibilities properly; then it follows, that a Safety Case - which also serves the above purpose - should moreover assist as a means for verifying safety requirements.

The development of a Safety Case is not an alternative to carrying out a Safety Assessment. Rather, it is a means of structuring and documenting a summary of the results of a Safety Assessment, along with other activities (e.g. simulations, surveys, etc.), in a way that a reader can readily follow the logical reasoning as to why a change (or on-going service) can and should be considered safe.

Tort Law, Due Diligence, Duty of Care & Subsequent Liability

The principal reason for developing and implementing a SMS and creating a Safety Case (for the purpose of this discussion), is to ensure that the people working within, and those that are associated with a project/service, are kept safe and '*free from harm'*. This is especially true with regard to '*due diligence*' and '*duty of care*' under *'tort law'*.

Many variations exist with regard to interpretation and meaning of these terms; therefore, legal advice should always be sought for a formal definition. However, the following definitions are appropriate in the context of this discussion and overview.

Due Diligence; OH&S Legislation – Canada:

Due diligence is the level of judgement, care, prudence, determination and activity that a person would reasonably be expected to conduct under a particular circumstances.

Applied to Occupational Health and Safety (OHS), due diligence means that an employer shall take all reasonable precautions, under particular circumstances, to prevent injuries or accidents in the workplace. This duty also applies to situations that are not addressed elsewhere in the OHS legislation. For example, to exercise *due diligence* within the confines of OHS, an employer must implement a plan to identify possible workplace hazards and carry out the appropriate corrective action to prevent accidents or injuries arising from these hazards.

However, in aviation under the Aeronautics Act (ANA) and the Canadian Aviation Regulations (CAR) *due diligence* also means:

> A defence which may be raised when someone is accused of doing something negligently or, in respect of aviation matters, if someone is accused of having contravened either a provision of the Aeronautics Act or a provision of the regulations.
>
> Under the Aeronautics Act - s.8.5 - ***No person shall be found to have contravened a provision of this Part or of any regulation or order made under this Part if the person exercised all due diligence to prevent the contravention.***

The dictionary definition of *due diligence* (Black's Law Dictionary) is as follows:

> *Such a measure of prudence, activity, or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent man under the particular circumstances; not measured by any absolute standard, but depending on the relative facts of the special case.*
>
> Whether or not a person has exercised an appropriate level of care, so as to be able to successfully raise the *due diligence* defence, will always be a matter of fact (evidence) and will depend on the circumstances of the situation.

Why does due diligence have special significance?

"*Due diligence*" is important as a legal defence for a person charged under either the OHS legislation or the ANA / CARs. If charged, a defendant may be found 'not guilty' if he or she can prove that *due diligence* was exercised. In other words, the defendant (Document Holder) must be able to prove that all precautions, reasonable under the circumstances, were taken to protect the health and safety of workers and the General Public.

Duty of Care. Duhaime Law Dictionary:

> *An obligation to conform to a certain standard of conduct for the protection of another against an unreasonable risk of harm.*

Tort Law. Duhaime Law Dictionary:

> *The body of the law which allows an injured person to obtain compensation from the person who caused the injury;* or:
>
> *The breach of a duty, primarily fixed by law, towards persons generally which is redressible by an action for unliquidated damages.*

'Tort' is derived from the Latin word '*tortus'*, which meant 'wrong'. In French, tort also means a 'wrong' but in civil law, what is generally defined by common law as 'torts', is recognized as civil liability and called a '**delict**'.

One substantial difference between a 'tort law' and a 'delict law' is that the former is a product of the common law, albeit now somewhat modified by statute: whereas the delict, as with most things civil under law, is purely a creature of statute.

Defence in Law:

If the worst happens and there is a serious incident, then it is likely that litigation will follow, especially in today's world. It is becoming increasingly common for Civil Cases to pursue Management in liability (primarily promoted by insurance companies), resulting in hefty fines and even impressment.

A well-constructed and maintained Safety Case provides the basis of an excellent defence for both the individual and the Enterprise. By formally documenting processes and the results of actions and events, even if an incident has occurred, it would normally be possible to demonstrate that management or other parties had given serious consideration (*due diligence*) to understanding the risks that their system(s) or decisions/actions posed and that appropriate safety mitigations were in place and operable.

For example under 'Tort Law', a *duty of care* is a legal obligation which is imposed on an individual requiring adherence to a standard of '*reasonable care*' while performing any act that could foreseeably harm others. It is the first element that must be established to proceed with an action in negligence. The claimant must be able to demonstrate a certain *duty of care* imposed by law, which the defendant has breached. In turn, breaching a duty may also subject an individual to liability.

The *duty of care* may be imposed by operation of law between individuals with no current direct relationship (familial or contractual or otherwise), but eventually become related in some manner, as defined by common law (meaning case law). *Duty of care* therefore, may also be considered a formalization of the social contract, with the implicit responsibilities held by individuals towards others within a society. It is not a requirement that a *duty of care* be defined by law, though it will often develop through the jurisprudence of common law.

The above reasoning explains why Safety Cases are often designed and organized similar to that of a legal defence. The concept being that by understanding what has to be met in the worst instance will help prepare and mitigate events before they occur.

SAFETY CASES - OVERVIEW

The importance of Hunan Factors, ergonomics in the workplace or even a Safety Management System, let alone a Quality Management Programme, and the subsequent consequences of inaction are all too often underestimated. However, there are a lot of minor improvements that can be applied to '*creep*' a culture and attitude to one more befitting this highly critical and legally defined industry, without a lot of additional work and cost. For example, a Safety Case is also a part of a 'Change Management Program' under a SMS and is subsequently another means (but not the only means) of proving a *duty of care*.

On occasion, a 'weak-link' will be identified via an audit, review process or safety report etc., wherein, an accident free period is often mistakenly identified as prevention to disaster i.e. "***we haven't had an accident around here for 20 years…***". The reality however, is really a matter of "**when"** not **"if**", and the 'when' just hasn't arrived! Should the worst-case scenario occur, it is crucial to be able to formally prove any '*due diligence*' and/or '*duty of care*' (unintentional tort) action.

Given the aforementioned, it is useful to be familiar with the application of Bill C-45 as it has teeth and it will bit hard. As a note of point, *****Bill C-45 is in addition to anything that Transport Canada may prosecute for under a Contravention. It is worth reviewing (in layman terms) the effect of the Bill.

First, it is important to identify those within the Organisation who are sufficiently important to be considered as a 'directing mind', Bill C-45 refers to a "Senior Officer" (SO), which is a more familiar expression than "directing mind". The definition of SO includes <u>everyone</u> who has an important role in:

- Setting policy; or,
- Managing an important part of the Organization's activities. (Pilot, Engineer, Administration, AE, CEO, etc. – in effect, just about everyone.)

The definition therefore focuses on the function of the individual, rather than on any particular title. For example, the Executive Assistant to the President could have a great deal of authority and effectively speak for the President in one Organization, and yet, have only minor administrative functions within another company, such as scheduling the president's meetings. Bill C-45 makes it clear that the Directors, the Chief Executive Officer(s) (CEO) and the Chief Financial Officer (CFO) of a corporation are, by virtue of the position they hold, automatically "Senior Officers". In short, a corporation charged with an offence, cannot argue that the individuals occupying these positions actually had no substantial role in setting policy or managing the organization and therefore, were not SOs and subsequently liable.

***Bill C-45** is federal legislation that amended the Canadian Criminal Code and became law on March 31, 2004. The Bill established new legal duties for workplace health and safety, and imposed serious penalties for violations that result in injuries or death. The Bill provided new rules for attributing criminal liability to organizations, including corporations, their representatives and those who direct the work of others.*

Safety Case – What is it?

A Safety Case is simply the case that the management of an Organisation makes to demonstrate that the facility is as safe as can be reasonably expected. It is analogous to the case that

management may have to make to a court following a serious accident. If the Safety Case is accepted then a Safety Case regime is implemented.

In principle, a Safety Case can be developed for any activity. However, in practice they are generally prepared for large and complex industries such as airlines, airports, nuclear power plants, military and civilian aviation and offshore oil and gas installations, etc. Such systems are normally complex, and in the event of an incident, the consequences could be very severe to both the Organisation and the individual. Such high consequence events are sometimes referred to as Major Accident Events (MAE). For offshore work, the 'UK Health and Safety Executive' states that an MAE would generally involve one or more of the following events.

- A fire, explosion or the release of a dangerous substance involving death or serious personal injury to persons on the installation or engaged in an activity on or in connection with it;
- Any event involving major damage to the structure of the installation or plant affixed thereto or any loss in the stability of the installation;
- The collision of an aircraft with an installation or building;
- The failure of life support systems for diving operations in connection with the installation; or,
- Any other event arising from a work activity involving death or serious personal injury to five or more persons on the installation or engaged in an activity in connection with it.

Principles of a Safety Case

A Safety Case is built upon the following three principles.

1. Those who create risks are responsible for controlling those risks.
2. Safe operations are achieved by setting and achieving goals rather than by following prescriptive rules.
3. All risks must be reduced such that they are below a threshold of acceptability.

The Cullen Report (1990) that analyzed the Piper Alpha disaster in detail, stressed that the quality of the offshore Safety Cases in use at that time needed much improvement (indeed, it could be said that it was the Cullen Report that initiated present day Safety Cases). The report stated,

"Primarily the Safety Case is a matter of ensuring that every Company produces a formal Safety Assessment to assure itself that its operations are safe".

Two aspects of the above quotation are particularly noteworthy:

First - the company that owns and operates an Organisation has to assure itself that the facility is safe. At root, a Safety Case is developed for the Organisation's personnel and company management, not for outside parties, although this is not uncommon. A Safety Case is not fundamentally a regulatory tool, although Regulators often use it. For example, operators of large and expensive deepwater facilities in the Gulf of Mexico frequently develop analyses and reports, which are very similar to Safety Cases. They do this - in spite of the lack of regulatory requirements - simply to assure themselves, that they have identified all the factors that could lead to the loss of their very expensive facilities.

Second - the facility management has to develop a Formal Safety Assessment of the operation for which it is responsible. This means that a framework for understanding risk, and what levels of risk are acceptable, has to be developed. Just following appropriate regulations and standards is not sufficient. This requirement means that Safety Cases are basically non-prescriptive but performance based. Instead of following detailed rules, the owner (duty holder) or Airport Authority etc. sets their own standards. The duty-holder's performance is then assessed against that standard. i.e. '*Are they doing actually what it is they say they are doing'*?

At present, the term 'Safety Case' is not widely used in North America. Nevertheless, the Safety Case approach to the development and application of a Safety Management Systems is in fact, used in a wide range of industries. For example, the nuclear and space industries prepare 'Safety Analysis Reports' (SARs) and 'Mission Safety Evaluations' (MSEs) respectively. These documents have the same intent and general structure as a Safety Case. One major oil and gas company also developed the "HSE case", which is essentially the same as a Safety Case; they just choose to use a different name.

Safety Case Definition

A Safety Case can be defined as follows:

A documented body of evidence that provides a demonstrable and valid argument that a system is adequately safe for a given application and environment over its lifetime.

Another definition, provided by the UK Ministry of Defense (MOD 2004) is:

A structured argument, supported by a body of evidence that provides a compelling, comprehensive and valid case that a system is safe for a given application in a given operating environment.

Yet another definition is provided by the Government of Western Australia (Department of Consumer and Employment Protection 2005):

A Safety Case regime is an objective-based regime whereby legislation sets broad safety objectives and the operator, who accepts direct responsibility for the ongoing management of safety, develops the most appropriate methods to achieve those objectives.

Confused? It can be seen, that although the above definitions have much in common, there is not a single agreed-upon definition as to what constitutes a Safety Case. Heiler (2005) states:

*Arguably, then, the question is not what **is** a Safety Case regime - but rather what kind of Safety Case regime is being contemplated. . .*

In other words, each operator must determine the nature of the Safety Case for his or her particular situation. There is no "one size fits all" Safety Case structure or design, that can be 'cut and pasted', each Safety Case must be designed and constructed to suit not only the Organisation it is intended to defend but equally, to manage and mitigate all potential hazards and risks.

Multiple Safety Cases

An Organisation can also generate a series of Safety Cases, one for each of the major phases in its design, construction, operation and decommissioning/abandonment. Updates to Safety Cases

may also be required if there is a significant change in conditions, such as those that often follow a major expansion, or the introduction of a new service/product etc.

A Safety Case should not focus on promoting a particular design or operations option. Instead, it should provide a discussion on the merits of different options and a justification that the chosen option is indeed the one that reduces risk to a level that is acceptable. For facilities that are already operating, the Safety Case should go beyond the original design information and be incorporate into the actual operating experience.

Purpose of a Safety Case

The principal reason for developing and implementing a Safety Case is to ensure that the people on and/or around an Organisation or operation are safe.

Defense in Law

If the worst happens and there is a serious incident, it is likely that litigation will follow. A well-constructed and maintained Safety Case provides the basis of an excellent defence. Even though an accident has occurred, the Safety Case can demonstrate that management had given 'serious consideration' to understanding the risk(s) that their system posed, and that appropriate mitigations were in place.

Conversely, even if an incident has not occurred, it is wise to design and organize the Safety Case as if it was to be a part of a legal defence. The advantage of doing this before an incident occurs, is that management has the time and flexibility - that it would not have - were it having to prepare a court defence.

Business Case

A Safety Case is also a business case, *i.e.*, it can be used to show investors, Customers, insurers and corporate managers that the risk associated with an expensive operation, such as an airport expansion or even a fuel farm on a property, has been analyzed, and that it is at an acceptable level of safety.

Different Industries

General Safety Case principles are applied quite broadly. Safety Cases were first developed in the nuclear and aerospace industries, and can be developed for any type of complex industrial activity that poses a high risk to workers and/or the community. For example, in addition to nuclear and aviation, dedicated Safety Cases have been developed for pipelines, railways and mining operations.

The nuclear power industry was probably the first to use the Safety Case. In the United Kingdom, the Nuclear Installations Act of 1965 required applicable facilities to create and maintain a Safety Case in order to obtain a license to operate. The nuclear industry has placed particular emphasis on the use of 'Quantitative Risk Assessment' (QRA) with the use of techniques such as 'Fault Tree' and 'Event Tree Analysis'. Because nuclear power plants are technically quite similar to one another, this industry has also been able to set up reliability data bases to which most facilities contribute.

Within the 'onshore' oil & gas process industries in Europe, the Safety Case approach was introduced as part of the Seveso Directive in 1986. It has since been replaced by the Seveso II Directive of 2003 – Prevention, preparedness and response. The Seveso Directives apply to

industrial establishments where dangerous substances are present in quantities exceeding their identified threshold levels.

The [Directives] led the UK to create the CIMAH (Control of Industrial Major Accident Hazards) Regulations in 1984. These Regulations required manufacturers of hazardous chemicals to create a safety report in effect a Safety Case. They also had to show how the hazards were being effectively managed. CIMAH was replaced by COMAH (Control of Major Accident Hazards) in 1999.

Effectiveness of Safety Cases

The development of a Safety Case does not of itself - improve safety. Safety Cases are only as good as the commitment made to their preparation and implementation, an observation that is illustrated by the crash of a Royal Air force Nimrod aircraft in 2006 in which, fourteen crewmembers perished.

A Safety Case had been prepared for the Nimrod. It turned out, however, that the quality of that Safety Case was gravely inadequate, leading to the following statements,

. . . the Nimrod Safety Case was a lamentable job from start to finish. It was riddled with errors. . . Its production is a story of incompetence, complacency, and cynicism.

The Nimrod Safety Case process was fatally undermined by a general malaise: a widespread assumption by those involved that the Nimrod was 'safe anyway' (because it had successfully flown for 30 years) and the task of drawing up the Safety Case became essentially a paperwork and 'tickbox' exercise.

Comments such as these emphasize that for a Safety Case to be effective, the following three points must always be considered.

Commitment:

The development and on-going implementation of a Safety Case can be expensive and time consuming if not accomplished by professionals. A Safety Case requires the commitment of time and other resources from key personnel, people whose services are always in demand elsewhere in the organization. In addition, just as employee, participation is a key element in a SMS, so worker involvement is crucial to the effective application of a Safety Case.

On-Going Activity:

Once written, the Safety Case should be used as an on-going operational and training tool. There are all too many examples where a comprehensive Safety Case is developed and then it just sits on a shelf gathering dust, with no one paying any further attention to it. In such situations there is a danger that operational personnel may take the attitude, "*We know we are safe because we have a Safety Case*".

Up to Date:

A Safety Case must be maintained and be kept current. This is not a difficult task when a major change to an operation or Organization is being made. However, it is possible that a succession

of minor changes over a period of years (Safety Creep) could materially affect the safety of an Organization, rendering the plan ineffective or even obsolete.

Features of a Safety Case

The following are core features of a Safety Case.

- Duty-Holder Responsibility;
- Participation and Commitment;
- Information Availability;
- Non-Prescriptive and Performance Based;
- Risk Management System;
- Management Systems;
- Living Document; and,
- Auditor/Assessor Responsibility.

At the heart of the Safety Case approach is an understanding that is the operator of an Organisation, not the Regulator, who decides how to ensure safe operations. The Organization that prepares and manages the Safety Case is known as the "Duty-Holder". Generally, the duty-holder is the owner/operator of the facility. However, this responsibility may be delegated within reason. For example, in the North Sea, many of the larger oil companies have sold some of their older fields to smaller Organizations. These Organizations, in turn, frequently do not have the internal resources develop or manage a Safety Case. Therefore, these companies may choose to hire a third party to act as the duty-holder. One of the responsibilities of the third party will be to develop and manage the Safety Case. (Strange but True.)

Nevertheless, the ultimate responsibility for preparing the Safety Case lies with the duty holder. Part of the assumed responsibility is to make sure that employees are fully involved in the preparation of the Safety Case. However, the detailed development of the information to be used in the Safety Case, and of the technical analyses, will generally be accomplished by specialist personnel hired for the purpose. For the highly specialized portions of the work, it is likely that the services of a Consulting Company will be required.

Participation and Commitment:

The active participation of all employees and contract workers is a key in the success of any safety program, including Safety Cases. This means that not only are employees informed and trained about the Safety Case but they also actively participate in its application and are encouraged to think of ways of improving system safety. Ideally, the Safety Case will lead to the augmentation and/or creation of a Safety Culture.

The commitment of management is also required. Given that the development and implementation of a Safety Case is critical to safety, management must commit the necessary funds and time of key personnel.

Although the goal of high employee participation is commendable, it must also be recognized that many sections of a Safety Case are highly technical and realistically, these sections are only going to be understood thoroughly by safety specialists.

SAFETY CASES - OVERVIEW

Information:

The Safety Case contains all the information needed in support of the arguments presented. In some ways, it is analogous to a case that an attorney may make after an incident in which they argue that an Organisation either did or did not do an adequate job of managing safety.

Non-Prescriptive and Performance Based:

Safety Cases are largely non-prescriptive; that is, rather than listing the detailed regulations, codes and standards that have to be followed they instead address the requirement, "***Do whatever it takes on your facility not to have accidents***". It is up to the managers, technical experts and the operations/maintenance personnel to determine how this will be accomplished. (Of course, detailed rules do have to be followed when they apply; the Safety Case is not a justification or excuse for avoiding compliance.)

Non-prescriptive management programs are always performance-based because the only measure of success is success. Hence, success is only achieved by not having incidents. Nevertheless, from a theoretical point of view, such a goal is impossible to achieve. No matter how well run an operation may be, incidents will occur, as risk can never be totally reduced to zero. All incidents however, can and must be mitigated.

The success of prescriptive programs can be measured - at least in the short term - by compliance with relatively detailed rules. One difficulty that a prescriptive approach faces is that technology changes rapidly, whereas the writing of policy, rules and regulation is a slow and painstaking process. This means that prescriptive standards may not be sufficiently up to date to address current issues. Such a problem does not occur with non-prescriptive programs, such as Safety Cases. The management of the risk is the responsibility of the Organization that creates the risk. If the Organization has developed the technology that creates the risk, then that same Organization should also create the 'risk management systems' needed to control the risk.

Nevertheless, the use of 'prescriptive standards' offer a number of advantages. First, given that standards are generally designed and developed by 'subject matter experts', the standard's subsequent application will ensure that high levels of safety will be achieved, even if the persons designing and running the facility are not themselves industry experts.

Second, the use of prescriptive standards increases efficiency and reduces design time. Rather than having to develop safety concepts and standards from scratch, the designers and operators can quickly and efficiently apply recognized references.

Finally, a prescriptive system allows for operations to be audited more quickly and consistently. The quality of the Audit does not depend as much on the training and knowledge of the auditor as it would in a non-prescriptive environment. Moreover, when all components are designed and operated to the same standards it is relatively easy to Audit them as the auditor simply has to look up the appropriate code or rule, and consequently draw a quick conclusion.

Additional Insight

Risk Management System:

The risk management system, which includes both technical and managerial systems, is generally organized as follows:

- Identify the hazards;

- Determine the level of risk associated with each hazard;
- Describe how the risks are controlled; and,
- Describe the SMS that ensures that the controls are effectively and consistently applied.

The risk management system usually include a quantitative analysis, *i.e.*, the risk associated with each of the hazards in an Organisation is estimated numerically and given a value, typically in the form of so many fatalities or environmental releases per thousand years. These individual risks are then added to one another to give an estimate of the overall risk.

Management Systems:

Systems for controlling risk should concentrate on management systems rather than just on hardware and instrumentation. Therefore, a Safety Case must show that the correct management system for controlling safety processes are in place and effective. Such a system is often referred to as a SMS and contains the primary system under which hazards are identified and risks continually and systematically assessed. Identified risks can be either eliminated or controlled at the appropriate points in the facility life, ranging from initial design, through construction, commissioning, operation and abandonment of the facility. The SMS must be comprehensive, integrated and contain feedback loops that continually measure performance and drive change.

The components of an SMS have been defined by many authorities including Transport Canada and the UK Ministry of Defence (MOD 1996). Typically components are as follows:

- Policy;
- Organization;
- Implementation;
- Measuring; and
- Review and development.

An SMS will include items such as the following:

- Safety policies and the organizational and facility safety objectives;
- Organization reporting structures - roles and responsibilities;
- Risk assessment and risk management;
- Methods of employee involvement in risk management;
- Employee selection, competency, training and induction;
- Integration of contractor and support services in risk management;
- Design, construction and commissioning procedures;
- Safe operational procedures for normal and abnormal circumstances;
- Systems of maintenance, inspection and modification;
- Systems of managing change to ensure safety;
- Methods, systems and procedures for ensuring the occupational health of employees;
- Emergency response including controls, personnel evacuation , escape and rescue;
- Incident investigation and reporting, corrective and follow-up action; and,
- The method of performance review and audit including review in the light of external experience.

The SMS should ensure that all necessary linkages between system elements are identified and where appropriate, should draw on the principles of quality management.

SAFETY CASES - OVERVIEW

Living Document

A Safety Case is a living document that describes the safety of an operation from the initial concept design, all the way through normal operations, to the eventual termination and shut down/abandonment of the facility. The Safety Case needs to be modified and upgraded as needed in order to ensure that risk and safety are properly managed at all times.

It is relatively easy to update the Safety Case when a major change to an organisation is being made. However, it is possible that a succession of minor changes over a period of years could materially affect the safety of an organisation such that the Safety Case will need to be updated.

Auditor / Assessor Responsibility:

All management systems must be audited. As one plant manager said, "*There is always news about safety - and some of that news will be bad*". The only way to find that bad news is to carry out audits and reviews.

Auditors fall into one of three types. The first is someone from within the immediate Organization who is charged with checking the quality of the program. The second type of Auditor works for the company or duty-holder that owns the facility but is in a separate (often corporate) Organization. This type of Auditor may also be a company hired by the facility management to mimic a regulatory Audit. The third type of Auditor is a government agency or other regulatory authority.

With respect to Safety Cases, the Auditor or assessor, who can represent either a government agency or a non-governmental body, has three key roles:

1. Provide guidance to the owner as to what is required in the Safety Case.
2. Formally accept (or reject) the Safety Case after it has been prepared and presented by the operator. Not only must the Safety Case as written be accepted, the operator has to demonstrate that his Organization has the ability, management commitment and resources to implement the Safety Case requirements.
3. Ensure that the operator is actually doing what he said he would do in the Safety Case once operations commence. Such reviews should occur on a regular basis. The UK HSE (Health & Safety Executive), for example, requires that, "*the duty holder must carry out a 'thorough review' of the current Safety Case at least every 5 years or as directed by HSE*".

Implicit in the Safety Case regulatory approach is that the Safety Case be evaluated and accepted (or rejected) by the Regulator. Having a Regulator accept a Safety Case regime can be tricky because, if there is an incident, the company involved can claim that some of the responsibility for the event lies with the Regulator. To get around this dilemma, the UK HSE states that,

. . . *"acceptance" requires satisfaction with the duty holder's approach to identifying and meeting health and safety needs. HSE "accepts" the validity of the described approach as being capable, if implemented as described, of achieving the necessary degree of risk control, but HSE does not confirm the outcomes of that approach.*

The acceptance or rejection of a Safety Case implies that the Regulator has personnel who are qualified to evaluate the complex and sophisticated analyses that are a part of any Safety Case.

The active participation of the Regulator in this manner differs from other standards such as OSHA's process safety management program or Recommended Practice 75 from the API. In these cases, the Regulator does not check or validate the program, but merely requires that a program exists. Only if there is an accident is the program scrutinized by the Authority.

Overall, the assessor's job is to ensure that management systems are in place, that they are effective and they are being followed. Rather than checking on the details of the safety program, the assessor will evaluate management systems for their their effectiveness.