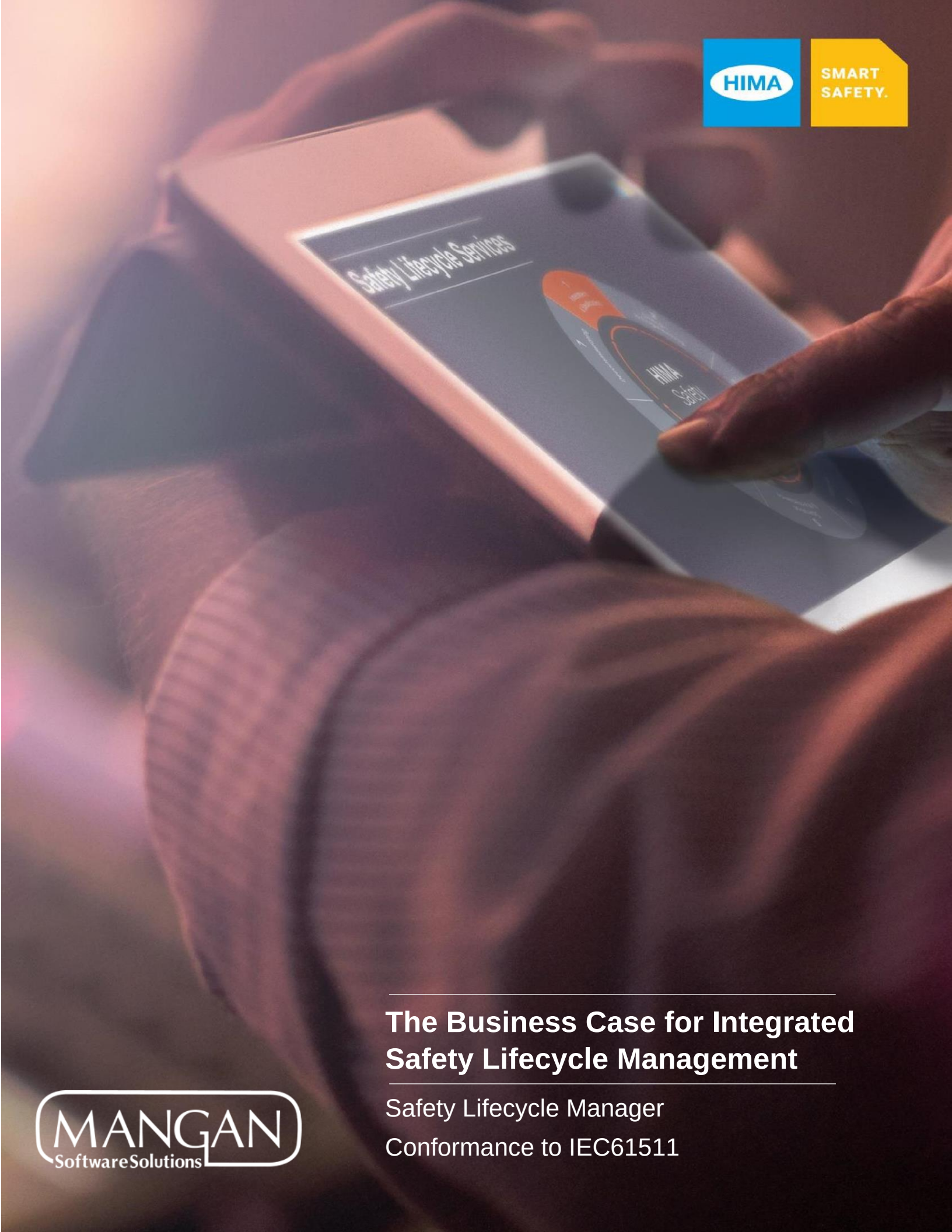

The Business Case for Integrated Safety Lifecycle Management

Safety Lifecycle Manager

Conformance to IEC61511

MANGAN Software Solutions

Integrated Safety Lifecycle Management

The Business Case

SLM® Safety Lifecycle Manager

www.Mangansoftware.com

Table of Contents

1 Abstract

Safety Lifecycle Management roles and functions cross multiple organizational boundaries and require active and continual sharing of data that often does not occur in traditional process facilities. This paper discusses the business reasons for adoption of an integrated Safety Lifecycle Management program. Among the topics discussed are management perceptions relative to Safety Lifecycle Management, obstacles that exist in traditional approaches and how compliance with National and Industry Standards and efficient management of the Safety Lifecycle are good business practices.

2 The Safety Lifecycle

2.1 Overview

Development of Industry Safety Standards since the early 1980's has provided a standardized method of approaching the design and ownership of Safety Instrumented Systems (SIS). These requirements are outlined by the Instrumentation, Systems and Automation Society (ISA) in ANSI/ISA 84.00.01-2004 to ensure uniformity in the field of instrumentation. The Safety Lifecycle applies to all phases of the life of a Safety Instrumented Function (SIF) and addresses organizational, as well as, SIS design issues. The Safety Lifecycle starts during conceptual design for a process application and continues through preliminary and detailed design phases, construction and installation, commissioning, operation and modification and decommissioning.

The requirements of ANSI/ISA 84.00.01-2004 developed from a series of incidents in the processing industries which demonstrated that older practices were not sufficient to properly design and maintain safety functions. These gaps have been addressed by the development of a performance based standard – the standard does not specify exactly what to do or how to do it, but does establish performance based criteria for the lifecycle of these functions. Key concepts include:

- A qualified organization shall exist to support each portion of the lifecycle, and shall have formalized qualification requirements and responsibilities.
- Safety functions shall be identified based upon analysis of the hazards presented by a specific process application. The performance requirements for safety functions shall be based upon this analysis.
- Safety function design shall meet independence and reliability criteria that are defined based upon the hazards being mitigated. The ability of the safety functions to meet these criteria shall be formally assessed by an independent qualified team.
- Safety functions shall be maintained and tested to assure performance to the levels defined for them. Performance shall be reviewed, and where necessary, corrections made to improve performance.
- Management of Change shall be a formal process for all modifications to safety functions. Decommissioning shall also be subject to Management of Change.

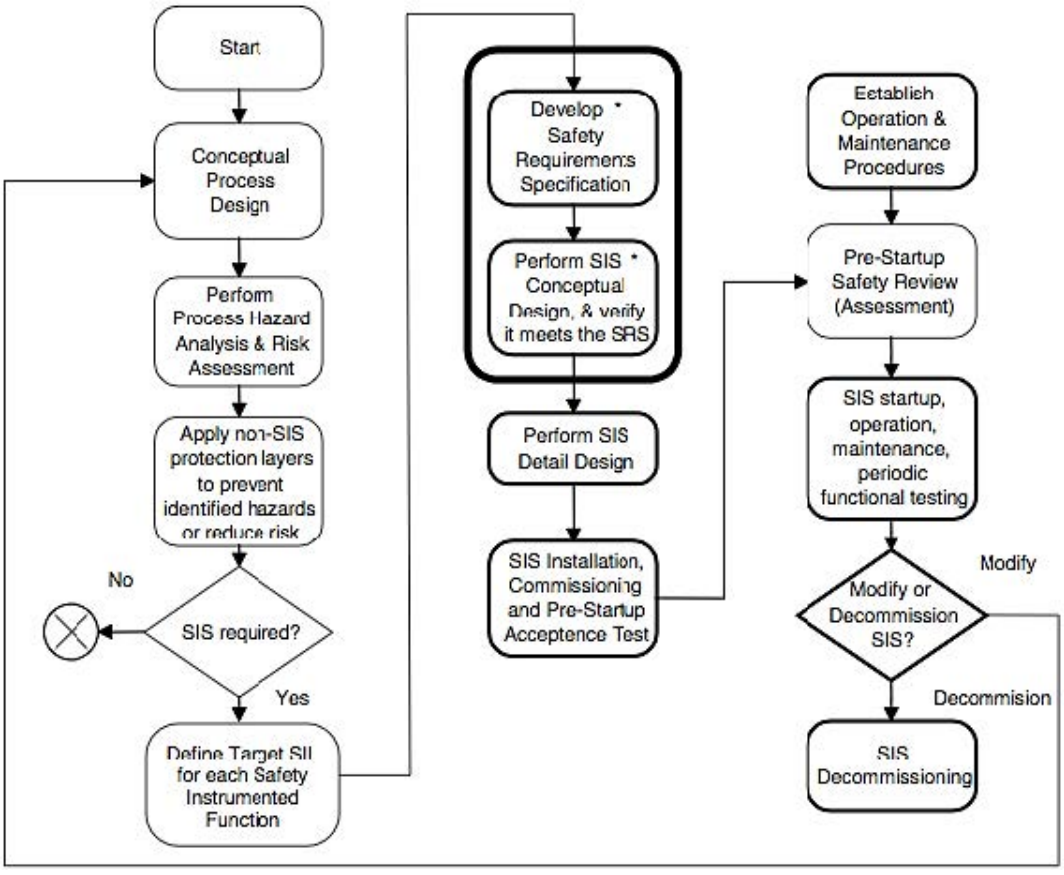

Figure 1 – IEC 61511 Safety Lifecycle

The figure shows a basic Safety Lifecycle as defined by IEC 61511/ISA 84.00.00-2004. IEC 61511 is the technical standard which covers the design and management requirements for SISs.

2.2 Compliance and Implementation

Development of SIS Standards, such as IEC 61511 and ANSI/ISA 84.00.01-2004, were a direct result of events that had root causes based in poor practices, and a lack of management and execution across the spectrum of Process Safety Management activities. The reasons for this varied across organizations, but the core issues range from fundamental lack of understanding (disregard in some cases) of basic process hazards identification, to total failures when designing, operating and maintaining the protective systems that did exist.

The faults fundamentally lay in corporate and plant site management attitudes towards process safety. Initial plant protective system designs were usually based upon historical practices and individual biases.

In some organizations, automated protective systems were actively discouraged as being impediments to production, Integrated Safety Lifecycle Management – The Business Case Page 3 of 7 and an unnecessary cost. Plant operators were credited with too much reliability in identifying and preventing major process incidences. Support for quality protective system designs and maintenance was highly variable across industries. A few organizations realized that their businesses relied heavily upon safe operations and invested in process safety organizations and practices well ahead of the rest of the industry. However, even within those organizations, facilities that were deemed to be of lower (average) hazard often did not follow these practices.

2.3 Management Views

Managers seeking a strong safety culture are looking for a way to validate compliance with applicable standards and regulations, increase collaboration between disparate business groups with roles in the Safety Lifecycle and ensure strategic alignment. A fundamental challenge to accomplishing these goals is the lack of visibility to ensure risk mitigation strategies are being followed. One way that management can address the challenges is by utilizing tools that help them standardize and automate these processes. While these tools generate greater efficiencies and cost savings, identifying the costs associated with inadequate Process Safety practices is often a challenge. Process Safety is a difficult issue to quantify. Good practices require investment and ongoing support costs, but the returns are not simple to measure on a day-to-day or year-to-year basis.

The true costs of poor practices appear infrequently, but when they do, it's in the form of extreme business impact due to plant damage, loss of production, loss of life and substantial injury, community impact and ultimately, total loss of the business. The cost benefit analysis of good Process Safety practices is even more difficult to quantify, and require a long view of the benefits of a robust Safety Lifecycle management process. Organizations need to recognize the value of avoided incidents versus reactive and sometimes ineffective prevention attempts.

2.4 The Business Case

The installation and maintenance of Safety Protective Systems, such as a SIS with its SIFs and associated Independent Protection Layers (IPL), is essentially like insurance. In insurance, premiums are paid to an external organization to assume financial risk. The insurance company determines the cost of premiums based upon the size of the potential risk and the probabilities of having to make a payout. The cost of the insurance is spread across a large number of policies, and the insurance company hopes they have gotten their probabilities and premiums correct. This is why insurance companies invest so heavily in their actuarial and underwriting departments. Those that provide industrial accident insurance actively conduct inspections and audits of their insured's practices.

Protective Safety Systems work the same way. During a Process Hazards Analysis, the impact of various hazards is identified. The methods vary, and for many hazards the assessment is highly qualitative. However, when the potential impacts get high enough, more quantitative methods come into play. For significant hazards, a quantitative value is established for the consequences of the hazards, and the probability of that hazard occurring is identified.

The financial impact can be described in a variety of terms. Commercial impacts typically have a direct financial value identified. Other consequences relating to personnel injury or fatalities, environmental impacts, community impacts, company reputation impacts or the right to conduct business are usually expressed in terms of unacceptable consequences (e.g. one or more fatalities, loss of permits to operate, etc.). Effectively, these impacts can all be reduced to a cost of some form. In any operation, there are some numbers of significant consequences which have some number of initiating causes, and each cause has some number of safeguards or protective functions. This leads to two probabilities existing. One probability is that of the consequence occurring without consideration of the mitigating effects of safeguards and protective safety functions. The other is the probability of the consequence occurring with safeguards and protective safety functions in place. Fortunately, the major events being considered are not frequent, but the probabilities of the event occurring are fairly inaccurate. Most techniques are considered to only be accurate to orders of magnitude. However, this does not prevent the analysis from being meaningful. A typical site may have 50 to 100 potential serious consequence scenarios, and a large world-wide corporation may have 100 or more sites. This can lead to the conclusion that a company may have a 100% probability of one or more serious consequence events occurring somewhere in the company each year, unless very effective prevention and mitigation measures are in place. Unfortunately, no one can predict where or when an event will occur, so the measures must occur across the board.

2.5 An Example

An insurance company performs careful economic analysis of the potential costs to pay out on a risk versus the income from premiums before it decides to insure a risk. Similarly, the installation, operation and maintenance of Protective Safety Systems should be subjected to the same analysis. Ideally, the costs of installing, operating and maintaining Process Safety Systems should provide a net return to the business. However, there are other considerations, particularly when clearly unacceptable consequences are involved. In this case, there is still usually an acceptable net cost to the business.

When a quality process hazard analysis is performed, there is a basis for the business evaluation established. When a realistic economic analysis of a typical Process Safety System is performed, it is usually the case that the Process Safety System is a good investment. Consider the following case:

2.5.1 Scenario Description

A process hazard scenario has been identified with a total business impact to a corporation of $100,000,000 when all impacts are considered, including commercial impact, personnel death or injury, economic impact, reputation and right to conduct business.

A detailed review of potential initiating causes has been conducted. The probability of the full consequences of the event occurring, if safeguards and protective functions are not included, is once in every 100 years. Inclusion of safeguards and protective functions reduces the probability of the full consequences of the event occurring to once in every 10,000 years.

The design of a SIS that performs the protective functions has been identified as costing $2,000,000, including field devices, engineering, installation and initial procedures and training. The service life of the SIS is expected to be 20 years.

Costs of operation and maintenance of the SIS and its protective functions are determined to be:

2.5.2 Operations

Cost Area	Basis	Cost/Year
Operation Training	20 operators – 8 hours training per year @ $80 per hour	$12,800
Record Keeping – Demands, Faults, Bypasses	100 hours per year @ $80 per hour	$8,000
Testing Support	2 operators – 3 days per year @ $80 per hour	$3,840
Operations Costs		$24,640

2.5.3 Maintenance

Cost Area	Basis	Cost/Year
Maintenance Training	4 technicians – 8 hours training per year @ $80 per hour	$2,560
Testing	4 technicians – 3 days per year @ $80 per hour	$7,680
Routine Maintenance, Parts		$5,000
Records, Testing, Routine Maintenance	2 technicians – 3 days per year @ $80 per hour	$3,840
Maintenance Costs		$19,080

2.5.4 Supervision, Engineering

Cost Area	Basis	Cost/Year
Training Support	40 hours per year @$150 per hour	$6,000
Performance Assessment	40 hours per year @$150 per hour	$6,000
Technical Support	20 hours per year @$150 per hour	$3,000
Miscellaneous Support	20 hours per year @$150 per hour	$3,000
Supervision & Engineering Costs		$18,000

Total Operation and Maintenance Supervision and Engineering Costs = $61,720 per year

Cost of Event without Protective Functions = $100,000,000 x 0.01/year x 20 years = $20,000,000

Cost of Event with Protective Functions = $100,000,000 x 0.0001/year x 20 years = $200,000

Potential Benefit of Protective Functions = $20,000,000 - $200,000 = $19,800,000

Cost of Protective Functions = $2,000,000 + 20 x $64,720 = $3,294,400

Potential Net Benefit of Protective Functions = 19,800,000 - $3,294,400 = $16,505,600

The simplified analysis above (costs and benefits have not been adjusted for time in the example) shows that statistically the value of the SIS is approximately $16,500,000. However, this is a statistical assessment and doesn't truly apply to a single SIS. If the SIS prevents the consequences of the event, its true value will be much higher when accounting for costs of equipment damage, personnel causalities or any other costs due to the occurrence of the event. Due to the 2005 Texas City refinery explosion, BP has paid out more than $2 billion in fines and lawsuits.1 The 2013 West Texas fertilizer plant explosion led to the death of 15 people and wounded another 226, costing the West Fertilizer Co. approximately $123 million in damages and fines.2 An effective way to get a handle on the true value is to apply the consequences and frequencies for the events identified in the hazard analysis as a basis for determining potential avoided losses and comparing them to the costs of installing and maintaining protective functions.

Process hazard analyses and protective systems analyses are statistical. Across a number of systems, the statistics say that having effective SISs and protective functions pay for themselves several times over. In the real world, you may install 100 SISs and only have a few of them actually have to prevent a major consequence. However, those SISs will pay for all others several times over; when the avoided costs of the consequences are recognized.

Statistical assessments can be frustrating in that no single output is guaranteed. However, just as at the craps table, roll the dice enough and you will get snake eyes when you don't need it. In the process world, companies are rolling virtual dice every day. Proper specification, installation and operation and maintenance greatly reduce the chances of rolling snake eyes.

1 Sam Hananel. "BP Texas City Refinery: Company To Pay Additional $13 Million For 2005 Explosion." Huffington Post. Web. 12 Jul. 2012. http://www.huffingtonpost.com/2012/07/12/bp-texas-city-refinery-fines_n_1668173.html. 2 Matthew Pierre. "Final Report Texas Fertilizer Plant Explosion." Web. 2014. https://stonybrook.digication.com/matthew_pierre/Final_Report_Texas_Fertilizer_Plant_Explosion.

2.6 Risks of Poor Safety Lifecycle Management

When an insurance company decides to insure an industrial risk, they often define many conditions around design requirements, operation capability, equipment inspection and testing which affect overall risk. If the insured does not comply with the requirements of the insurance policy, the insured may have the insurance withdrawn, or find that the expected loss payment is not made due to non-compliance with requirements. The design and operation of Protective Safety Systems are the same. If a company has purchased insurance on an operation, it is very likely that a condition of that insurance includes compliance with specific industry standards, such as IEC 61511. If a company is self-insured, the risk conditions still exist. If a SIS is not properly designed and maintained, the cost/benefit assessment (such as the example above) becomes invalid. The result is that the company bears all of the consequence risk with none of the benefits of the investment.

2.7 Conclusions

The entire economic benefit of installing effective protective systems, including SISs, is derived from the avoided cost of the identified hazards and the consequences of those hazards. These systems also require that rigorous design, operations and maintenance be followed if the investments involved can be expected to pay out.

As demonstrated in the example presented, the potential liability avoidance to a business for investing in protective functions and its maintenance are exceedingly high, perhaps one of the best Return on Investment (ROI) decisions a business can make.

Author: Rick Stanley, Aurora, CO