ELSEVIER

Journal of Hazardous Materials 71 (2000) 449–465

Journal of Hazardous Materials

www.elsevier.nl/locate/jhazmat

Performance-based standards: safety instrumented functions and safety integrity levels

Paris Stavrianidis *, Kumar Bhimavarapu

Factory Mutual Research, 1151 Boston-Providence Turnpike, Norwood, MA 02062, USA

Abstract

This paper discusses two international performance-based standards, ANSI/ISA S84.01 and IEC d61508 and the requirements they place upon companies that rely on electrical, electronic and programmable electronic systems to perform safety functions. Performance-based regulations are also discussed and common safety elements between the standards and regulations are identified. Several risk analysis techniques that can be used to comply with the aforementioned requirements are discussed and a simple example is used to illustrate the use, advantages and disadvantages of the techniques. The evaluation of safety integrity level (SIL) of the Safety Instrumented System (SIS) in terms of the probability to fail to function is outside the scope of this paper.

Keywords: Process risk; Performance-based standards; ANSI/ISA S84.01; IEC d61508; Safety instrumented systems; Safety integrity levels; Risk analysis; Standard compliance

1. Introduction to performance-based safety standards

During the last two decades, great emphasis has been placed on improving management of technological risks in the process industry. Process Industry refers to those processes involved, but not limited to, the production, generation, manufacture, and/or treatment of oil, gas, wood, metals, food, plastics, petrochemicals, chemicals, steam, electric power, pharmaceuticals, and waste material(s). These efforts have resulted in the development of performance-based standards from the International Electrotechnical Commission (IEC) IEC d61508, the Instrument Society of America (ISA), ANSI/ISA

* Corresponding author. Tel.: +1-781-255-4983; fax: +1-781-255-4024; e-mail: paraskevas.stavrianidis@factory-mutual.com

0304-3894/00/$ - see front matter
PII: S0304-3894(99)00093-X

S84.01 [1,2], and national (USA) regulations from Occupational Safety and Health Agency (OSHA) and the Environmental Protection Agency (EPA) [3,4].

The standards have been developed to support companies that use Safety Instrumented Systems (SIS) to protect against hazardous events. A Safety Instrumented System is composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when predetermined conditions are violated. Other terms commonly used include Emergency Shutdown Systems, Safety Shutdown Systems, and Safety Interlock Systems. SIS is used in ANSI/ISA S84.01 to refer to E/E/PE SRSs, a term used in IEC 61508. For the remainder of this paper the term SIS will be used.

This paper briefly discusses several new and/or emerging performance-based standards and regulations that apply to the process industries. [1] It proposes an assessment scheme, for the risk associated with a process and the reliability of a safety system, consistent with the standards, in order to generate data and information to meet the requirements of the standards and regulations. An example is used to illustrate the use of the assessment scheme in compliance to the standards/regulations.

1.1. IEC d61508 standard

The IEC d61508 performance-based draft standard [1] has been developed as an umbrella standard that can be applied to any industrial process that uses electrical, electronic and programmable electronic components to comprise a SIS. The standard employs a safety life-cycle model to identify and provide guidance on the establishment of safety specifications for the required safety instrumented functions that will be implemented in an SIS and other system activities, such as design, installation, maintenance and de-commissioning, that impact the functional safety of a SIS.

The standard relies on performance-based metrics such as process risk and SIS probability to fail to function. Therefore, it can objectively and systematically be applied by industry, manufacturers of systems, system integrators, industry regulators and approval agencies. The performance metric for the safety instrumented functions and of the SIS is referred to as Safety Integrity Level (SIL) and is shown in Table 1. These SILs are given in terms of the probability of the SIS to fail to function, which can be translated to process risk reduction (i.e. reducing the likelihood of occurrence of hazardous events due to the presence of a new safety system without affecting the consequences) that can be achieved by employing the SIS.

1.2. ANSI / ISA S84.01 standard for the process industry

The Instrument Society of America (ISA) has independently developed ANSI/ISA S84.01 [2] to be a performance-based standard for the use of SIS in the process industry. It follows a similar life-cycle model as the IEC d61508 to identify the need for a SIS.

[1] These industries produce, generate, manufacture, and/or treat: oil, gas, plastics, petrochemicals, chemicals, wood, metals, pharmaceuticals and waste material.

Table 1
IEC d1508 safety integrity levels

Safety integrity level (SIL)	Probability to fail to function
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$

The objectives are to determine the safety functions and associated SILs that will be implemented in a SIS in order to achieve the desired safety target level. Detailed information on the requirements of the standard is given in Ref. [2].

The standard focuses on industrial applications of SISs and uses the safety integrity levels in Table 1, but clearly states that SIL 4 is not used in the process industries. Currently, the International Electrotechnical Commission (IEC) is working to convert the ANSI/ISA S84.01 standard to an IEC d61511 standard [5] for the process industry.

2. Performance-based regulations

Recently, performance-based regulations have been published in the United States that mandate some of the safety elements embedded in the aforementioned standards, such as hazard and risk analysis. Therefore, compliance to these regulations would, in part, support some of the compliance activities of the standards.

2.1. OSHA process safety management (PSM) rule

The OSHA PSM [3] rule lists a large number of specific chemicals plus all hydrocarbons and provides threshold values above which a company using, storing, or producing the chemicals must comply with the provisions of the law. The law is performance based rather than a prescriptive (specification based) standard, with no specific measurements which the company is mandated to meet. The specific provisions for compliance addressing process safety and risk related issues are: Process safety information (PSI), process hazard analysis (PHA), operating procedures, employee training, pre-startup reviews, mechanical integrity, hot work permits, management of change, incident investigations, emergency response and control, compliance safety audits, contractor oversight, employee participation and trade secrets.

2.2. EPA's Risk Management Plan Rule

EPA's Risk Management Plan (RMP) Rule [4] is designed to prevent accidental releases of regulated substances and other extremely hazardous substances into the air. Similar to OSHA's PSM, EPA's RMP rule is performance based, and has most of the same elements as OSHA's PSM Standard. However, the RMP rule sets minimum requirements for fixed installations in developing risk management programs using dispersion modeling to quantify the concentration of hazardous material downwind of a

release point. It is the responsibility of individual plants to design systems to address these minimum requirements in a way that prevents accidental releases of regulated substances.

Those facilities that present a higher risk to populations and the environment outside the plant boundaries must comply with more stringent requirements than those that present lower risks to off site receptors. The full risk management program required by the RMP rule is comprised of a compilation of 5 year accident history, hazard assessment, a management system, a prevention program and an emergency response program.

3. ''Integrated risk assessment'' program

The process safety management standards and regulations mentioned in the previous sections have some common elements. The ''integrated risk assessment'' [6] program, shown in Table 2, combines these elements into one program that allows practitioners to claim compliance to these standards using a range of techniques, from purely qualitative to well established quantitative methodologies for probabilistic and consequence modeling. It is the use of this program that makes compliance to the standards practical and cost-effective.

Table 2
Integrated risk program. Key: (+) requirement but not within scope of standard; (✓) requirement and within scope of standard

Safety and risk elements	ISA S84.01 IEC 1508	OSHA PSM	EPA RMP	Integrated risk
Compliance audits		✓	✓	✓
Contractor handling		✓	✓	✓
Emergency Management Plans, inside facility		✓	✓	✓
Emergency Management Plans, outside plant			✓	✓
Employee participation		✓	✓	✓
Hazard assessment	+	✓	✓	✓
Consequence assessment	+		✓	✓
Hotwork permits		✓	✓	✓
Incident investigation		✓	✓	✓
Management of change	✓	✓	✓	✓
Mechanical integrity	+	✓	✓	✓
Operating procedures	✓	✓	✓	✓
Pre-startup safety review	✓	✓	✓	✓
Process risk	+			✓
Safety Integrity Levels for SIS	✓			✓
Other risk reduction facilities	+			✓
Training		✓	✓	✓
Installation/maintenance	✓			✓
Decommissioning	✓			✓

4. Compliance to ANSI/ISA S84.01 and IEC d61508 standards

The overall objective of the standards is to identify the required safety instrumented functions, establish their SILs and implement them in an SIS in order to achieve the desired safety level for the process. The standards also mandate the development of a safety management plan, require documentation of safety activities that affect functional safety, and propose validation and verification activities throughout the safety life cycle. The following are the basic steps required in order to comply with the standards:

4.1. Identify the safety target level of the process

A fundamental requirement for the successful implementation of the standards is the concise and clear definition of a desired process safety target level. This level may be defined using national and international standards and regulations, corporate policies supported by good engineering practices with input from concerned parties such as the community, local jurisdiction and insurance companies. The safety target level is specific to a process and should not be generalized unless existing regulations, standards and/or corporate policies have safety target levels that apply across industries, processes and often applications.

4.2. Evaluate hazardous events that pose a risk higher than the safety target level

The standards mandate the performance of a hazard analysis and risk assessment in order to identify and quantify the risk associated with the process. There are several techniques that can be used to identify hazards such as Safety Reviews, Checklists, What If Analysis, HAZOP, Failure Mode and Effects Analysis, Cause-Consequence Analysis [7,8]. Process risk can be evaluated using techniques ranging from a purely qualitative approach to full quantitative risk assessment [1,2,7–11].

Once the hazardous events and the associated risk has been determined it is compared to the established safety target level. The hazardous events that pose a risk higher that the safety target level are identified along with opportunities to reduce risk below the safety target level.

4.3. Determine safety functions to be implemented in an SIS

For the hazardous events that pose a risk greater than the safety target, the standards require that safety systems of other technologies and external risk reduction facilities be employed prior to establishing the need for a safety instrumented function implemented in an SIS. After such risk reduction systems have been implemented, the hazardous events that remain with a risk greater than the safety target must be protected using safety instrumented functions implemented in an SIS.

4.4. Implement the safety functions in an SIS and evaluate its SIL

Each safety instrumented function is evaluated to establish its SIL. Furthermore, more than one safety instrumented function may be implemented in an SIS. The performance

of the SIS is evaluated in order to establish its SIL. There are several techniques that can be used to evaluate the probability of an SIS to fail to function [1,2,8,12].

It is important to note that if more than one safety instrumented function is implemented in an SIS, the common parts of the SIS (e.g. logic solver(s)) must conform to the highest SIL requirements. For example, if four safety instrumented functions are implemented in an SIS, each having a different SIL requirement ranging from SIL 2 to SIL 3, then the common parts of the SIS (those that cannot be shown to be independent) must have a SIL 3 requirement.

4.5. Install, test and commission SIS

The standards provide specific guidance on how to install, test and commission a new SIS application. It is clear that the burden is placed on the user company to make certain that the SIS is installed and commissioned according to an approved safety management plan and that procedures are in place to make certain that the SIS is continuously evaluated and maintained throughout its life cycle.

4.6. Verify installed SIS meets requirements

The new SIS has been selected, designed, tested and installed. Its reliability has been evaluated and perhaps certified by an independent third party, and installed. The process risk should be re-evaluated using the same techniques to determine if in fact the desired risk reduction has been achieved.

If the process risk is still below the process safety target level, then the new SIS has met its safety specifications and is in compliance with the standard(s). If however, the new process risk is not acceptable, then the process must be re-evaluated for further risk reduction opportunities. An iterative procedure is then followed until the process safety target level is achieved.

5. Risk analysis techniques

This section focuses on techniques that can be used to perform a hazard analysis and risk assessment of the industrial process. The risk associated with a process can be evaluated using qualitative or quantitative techniques published in [1,2,7–11]. These techniques rely on the expertise of plant personnel and other hazard and risk analysis specialists to identify potential accident scenarios and evaluate the likelihood, consequences and impact of such accidents.

5.1. Qualitative risk assessment techniques

In qualitative techniques, the risk concept of likelihood and consequences is used even though no explicit quantification is required. There are several examples of such

techniques published in literature [7,9]. These techniques rely on the expertise of plant personnel and other experts to identify potential accident scenarios and evaluate both the likelihood and consequences of an accident.

One such technique based on DIN 19250 [9] that can be applied to safeguard personnel and the environment is shown in Fig. 1. Similar risk graphs can be developed for damage to property. The risk graph identifies the required SIL of a safety function. In other words, it identifies the required risk reduction in order to achieve the desired safety target level. Therefore, the risk graph and the SILs depend on the safety target level that has been established for the process.

The proposed approach is to have a team of experts examine the process, identify each safety function that will be handled by an SIS and evaluate the SIL of each safety function using the risk graph shown in Fig. 1. The highest SIL is then allocated to the common elements of the new SIS that is needed to achieve a safety target level.

5.2. Semi-quantitative risk assessment approach

A semi-quantitative approach can be used to assess process risk [5–7]. Such a semi-quantitative approach allows for a traceable path of how the accident scenario develops, and comprises the following steps: (1) identify the accident scenarios; (2) identify the basic events that comprise each accident scenario, including the failure or success of safety systems; (3) assign a typical likelihood of occurrence for each event; (4) estimate the likelihood (approximate range of occurrence) of an accident scenario; (5) perform consequence analysis to understand the severity of the consequences of the accident scenario; (6) assign the rating for the severity of the consequences; and (7) evaluate the risk as a combination of the likelihood and the consequences.

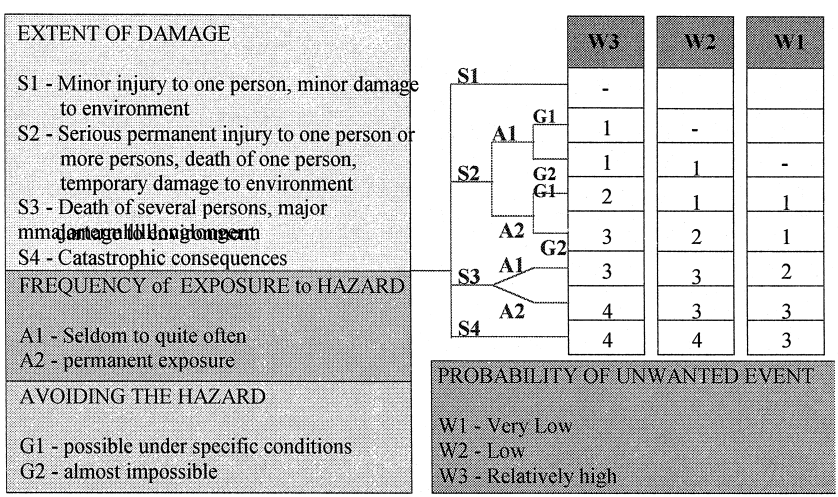

Fig. 1. Qualitative technique to assess risk.

Table 3
Criteria for probability of occurrence of hazardous events

Type of events	Likelihood	
	Frequency/year	Qualitative ranking
Events like multiple instrument or valve failures, multiple human errors or spontaneous failures of process vessels.	$<10^{-4}$	Very low
Events including combinations of instrument failures and human errors or full bore failures of small process lines or fittings.	10^{-4}–10^{-3}	Low
Events like dual instrument, valve failures, or major releases in loading/unloading areas.	10^{-3}–10^{-2}	Moderate
Events like process leaks, single instrument, valve failures or human errors that result in small releases of hazardous materials.	$>10^{-2}$	High

Typical guidance on how to estimate the likelihood of accidents to occur is provided in Table 3. Table 4 shows one way of converting the severity of the consequences into ratings for a relative assessment. Similar tables for likelihood and severity of consequences can be developed based on plant specific expertise and experience.

A risk matrix can be used for the evaluation of risk by combining the likelihood and the consequences. Such a risk matrix, shown in Fig. 2 [5,7], can be used with qualitative or semi-quantitative approaches. The matrix can and should vary with different applications. The three-dimensional matrix shown in Fig. 2 accounts explicitly for the presence of independent protection layers (IPLs) [7] using safety systems of other technologies such as pressure relief valves and rupture disks. Therefore, the likelihood of a hazardous event is estimated without accounting for the contribution of IPLs.

5.3. Quantitative risk analysis techniques

The quantification of the risks associated with a process is accomplished through a Quantitative Risk Analysis (QRA) [7,8,10,11] that identifies and quantifies the risks associated with potential process accidents. The results (i.e. process risk or safety level)

Table 4
Criteria for severity of consequences of hazardous events

Severity	Nature of consequences
High	Large scale damage of equipment. Shutdown of a process for a long time. Catastrophic consequence to personnel and the environment.
Moderate	Damage to equipment. Short shutdown of the process. Serious damage to personnel and the environment.
Low	Minor damage to equipment. No shutdown of the process. Temporary injury to personnel and damage to the environment.
Very low	No damage to equipment. Minor injury and environmental damage.

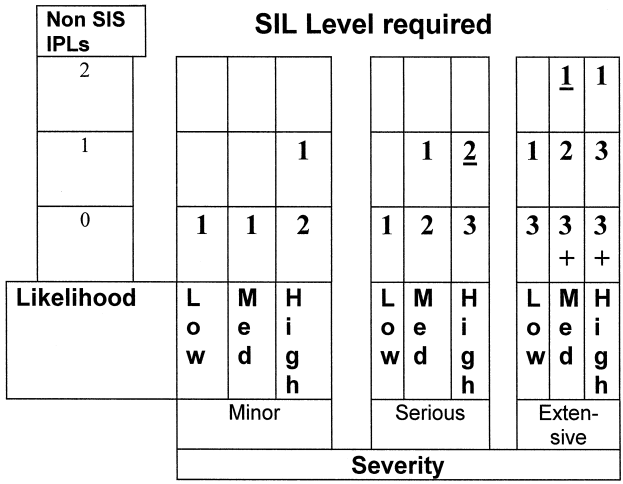

Fig. 2. Three-dimensional risk matrix.

can be used to identify safety functions and their associated SIL in order to reduce the process risk to an acceptable level.

The significant outcomes of interest are:

- A better and more detailed understanding of risks associated with the process.
- The process risk profile.
- The contribution of existing safety systems to the overall process risk reduction.
- The identification of each safety function needed to reduce process risk.
- A comparison of current process safety with the process safety target level.

5.4. Comparison of techniques

The use of the qualitative technique may be difficult because: (a) it relies heavily on the expert opinion of team members to assess the critical parameters that may produce inconsistent results; (b) it is difficult to document all thought processes that have led to the stated outcome; (c) it does not facilitate the use of a monitoring and management of change system for life-cycle management; and (d) it may be difficult to use for complex processes. The benefits of this approach are its simplicity, timeliness and the limited resources required for its execution making it a useful screening tool to identify areas of safety concern. The disadvantage is that because it is so dependent on the expertise of the practitioners, consistency may be a problem.

A semi-quantitative approach is generally used to identify and assess process risk where the emphasis is more on relative assessment rather than absolute assessment. The semi-quantitative technique does provide a more systematic approach to assess risk than qualitative methods. It also relies on the ability of the team to assign values to the risk parameters based on judgment. It does have all the benefits of the quantitative approach without presenting the same level of challenge in documentation and life-cycle activities management.

The quantitative technique is resource intensive but does provide benefits that are not provided in the other two approaches. The technique relies on the expertise of a team to identify hazards, provides an explicit method to handle existing safety systems of other technologies, uses a framework to document all activities that have lead to the stated outcome and provides a system for life-cycle management. The one significant disadvantage is the lack of credible data that is process specific.

A proposed approach to assess the risk associated with a new process in order to determine the safety functions that will be incorporated into an SIS and comply with the standards follows:

- Use the qualitative or semi-quantitative technique as a screening tool to reduce initial cost by identifying complicated and significant, accident scenarios in terms of risk that require further analysis.
- Use the quantitative technique to assess process risk and clearly document the procedure and results.

If, however, a user company has developed a significant experience base with the operation of a particular process, the hazards and hazardous events of interest are probably well known, and therefore a qualitative or semi-quantitative method can be used to identify the safety functions that should be implemented in an SIS. The success of any risk assessment technique will depend on the expertise of the analysis team and their experience with the process under study.

6. Application example

A quantitative risk analysis technique is used on a simple example to illustrate a methodology for compliance with the aforementioned requirements.

6.1. Process

Consider a process comprised of a pressurized vessel containing volatile flammable liquid with associated instrumentation (see Fig. 3). Control of the process is handled

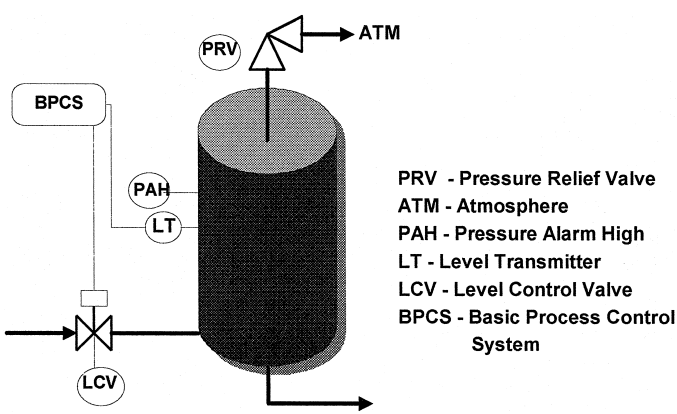

Fig. 3. Pressurized vessel with existing safety systems.

through a Basic Process Control System (BPCS) that monitors the signal from the level transmitter and controls the operation of the valve. The engineered systems [2] available are:(a) an independent pressure transmitter to initiate a high pressure alarm and alert the operator to take appropriate action to stop inflow of material; and (b) in case the operator fails to respond, a pressure relief valve to release material to the environment and thus reduce the vessel pressure and prevent its failure.

6.2. Process safety target levels

For the illustrative example, assume that the safety target level for the vessel is: no release to the atmosphere with a probability of occurrence greater than 10^{-4} *in one year.*

6.3. Hazard analysis

For the illustrative example, a HAZOP was performed for the process. The results of the HAZOP study identified that an overpressure condition could result in a release of the flammable material to the environment. This is an initiating event that could propagate into an accident scenario depending on the response of the available engineered systems. If a complete HAZOP was conducted for the process, other initiating events that could lead to a release to the environment may include leaks from process equipment, full bore rupture of piping, and external events such as a fire. For this illustrative example, the overpressure condition will be examined.

6.4. Risk assessment

For the illustrative example, one initiating event — overpressurization — was identified through the HAZOP study to have the potential to release material to the environment. It should be noted that the approach used in this section is a combination of a quantitative assessment of the likelihood of the hazardous event to occur and a qualitative evaluation of the consequences. This approach is used to illustrate the systematic procedure that should be followed to identify hazardous events and safety instrumented functions.

The next step is to identify factors that may contribute to the development of the initiating event. In Fig. 4, a simple fault tree is shown that identifies some events that contribute to the development of an overpressure condition in the vessel. The top event, vessel overpressurization, is caused due to the failure of the basic process control system (BPCS), or an external fire. The fault tree is shown to highlight the impact of the failure of the BPCS on the process. The BPCS does not perform any safety functions. Its failure, however, contributes to the increase in demand for the SIS to operate. Therefore, a reliable BPCS would create a smaller demand on the SIS to operate. The fault tree can

[2] Engineered systems refers to all systems available to respond to a process demand including other automatic protection layers and operator(s).

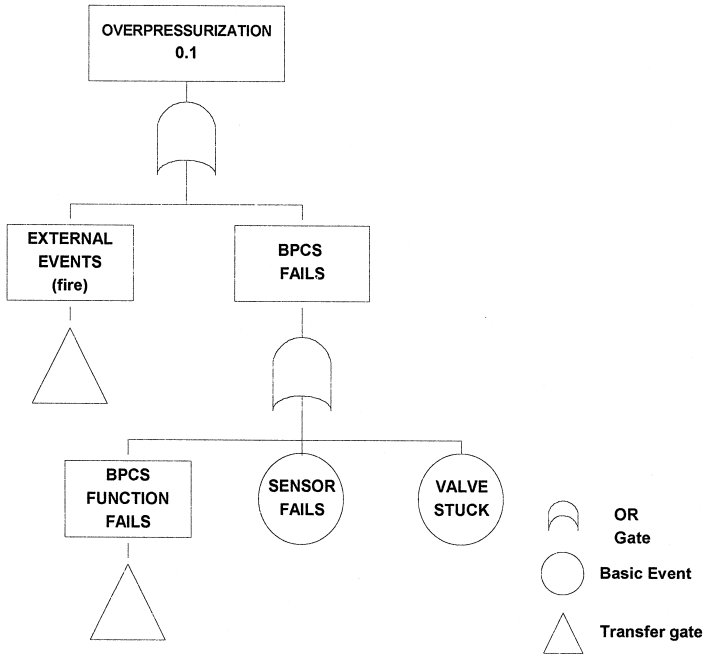

Fig. 4. Fault tree for overpressure of the vessel.

be quantified using minimal cut-set theory [13]. For this example, the likelihood of the overpressure condition is assumed to be in the order of 10^{-1} in one year.

Once the probability of occurrence of the initiating event has been established, the success or failure of the safety systems to respond to the abnormal condition is modeled using event tree analysis [11,13]. The reliability data for the performance of the safety systems can be taken from actuarial data, published databases or predicted using reliability modeling techniques. For this example, the reliability data were assumed and should not be considered as representing published and/or predicted system performance. Fig. 5 shows the potential release scenarios that could be developed given an overpressure condition. The results of the accident modeling are: (a) the probability of each accident sequence to occur; [3] and (b) the consequences in terms of release of flammable material. In Fig. 5, five accident scenarios are identified, each with a probability of occurrence and a consequence in terms of potential releases. Accident scenario 1, no release, is the designed condition of the process. The remainder scenarios range from a probability of occurrence in the order of 9×10^{-3} for release of material from the relief valve to about 1×10^{-3} for failure of the vessel.

[3] Each event in Fig. 5 is assumed to be independent. Furthermore, the probability data shown is approximate; therefore, the sum of the probabilities of all accidents approaches the probability of the initiating event (0.1).

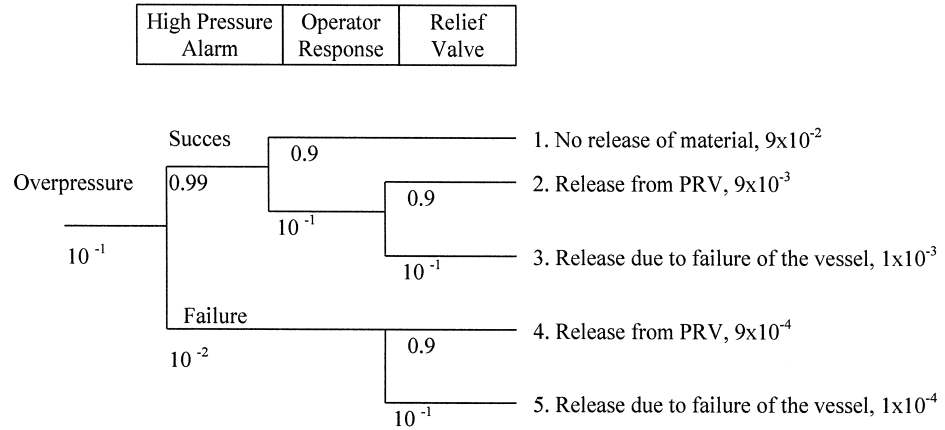

Fig. 5. Accident scenarios with existing safety systems.

6.5. Events that do not meet the safety target level

As was stated earlier, plant specific guidelines establish the safety target level as: no release of material to the environment with a probability of occurrence greater than 10^{-4} in one year. Given the accident probability of occurrence and consequence data in Fig. 5, risk reduction is necessary in order for accidents 2, 3 and 4 to be below the safety target level.

6.6. Risk reduction using other protection layers

Both standards require that safety systems of other technologies be employed prior to establishing the need for a safety function implemented in an SIS. To illustrate the procedure, assume that an additional pressure relief valve with a higher set point is introduced to augment the existing safety systems. Fig. 6 shows the process with the new safety systems. Event tree analysis is employed to develop all the potential accident scenarios. From Fig. 6, it can be seen that seven release accidents may occur, given the same overpressure condition.

Examination of the probability of occurrence of the modeled hazardous events shows that the safety target level for the vessel has not been met because accident scenarios 2, 3 and 5 are still above the safety target level. At this point the feasibility of using external risk reduction facilities should be evaluated. Given that the safety target is to minimize the risk due to a release of material to the environment, it will be assumed that external risk reduction facilities such as a dike or transfer of the released material to a holding tank is not a feasible alternative risk reduction scheme. Therefore, since no other non-SIS protection can meet the safety target level, a safety function implemented in an SIS is required to protect against an overpressure and the release of the flammable material.

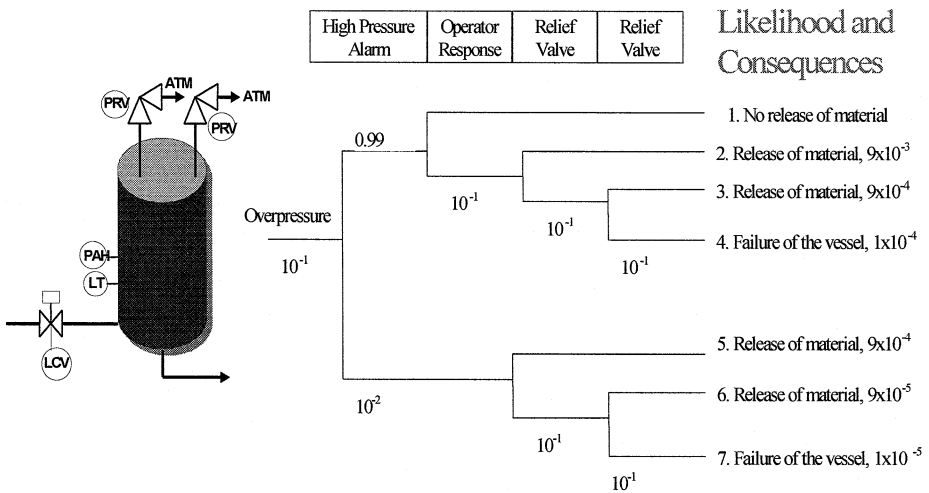

Fig. 6. Accident scenarios with redundant pressure relief valve.

6.7. Risk reduction using an SIS safety function

The safety target cannot be achieved using safety systems of other technologies or external risk reduction facilities. Therefore, a new SIL 2 safety function implemented in an SIS is required to meet the safety target level. The safety function must reduce the probability of occurrence of the second accident scenario, in Fig. 6, from 9×10^{-3} in a year to or below the established safety target of less than 10^{-4} in one year. This requires a SIL 2 safety function (Probability to Fail to Function 10^{-3} to 10^{-2}, see Table 1). The new safety function is shown in Fig. 7. It is not necessary at this point to perform a

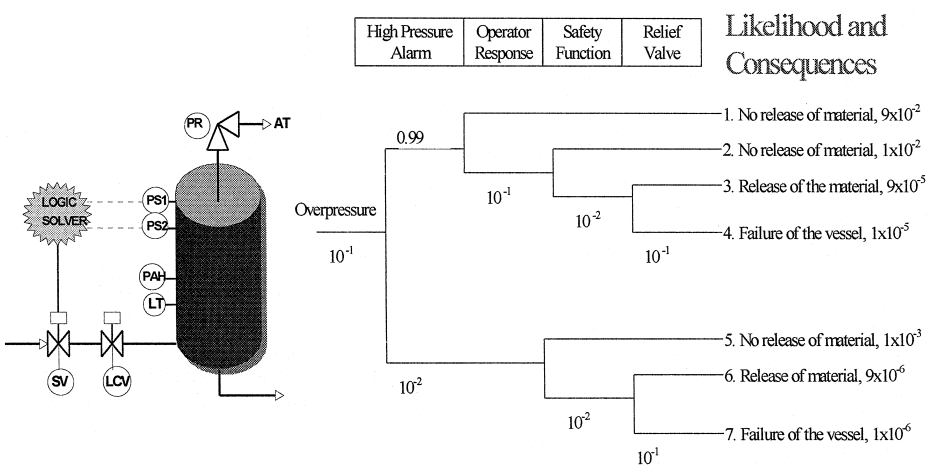

Fig. 7. Accident scenarios with SIL 2 SIS safety function.

detail design on the safety function. However, a general concept of the new safety function should be available. For example, the new safety function can use dual, safety dedicated, pressure sensors in a loo2 configuration sending signals to a logic solver. The output of the logic solver controls one additional shutdown valve. [4]

The new SIL 2 safety function is used to minimize the likelihood of a release from the pressurized vessel due to an overpressure. Fig. 7 presents the new safety layer and provides all the potential accident scenarios. As can be seen from this figure, the probability to have a release from this vessel can be reduced to 10^{-4} or lower and the safety target level can be met provided the safety function can be evaluated to be consistent with SIL 2 requirements.

6.8. Define safety function specification requirements

As was mentioned earlier, there are additional initiating events that may occur and cause the release of material from the pressure vessel. These have to be examined using the aforementioned procedure. Using the same technique, event trees representing accident scenarios for the chemical process for additional initiating events can be developed to identify all the safety functions required to protect the process and evaluate the SIL of each safety function. For the illustrative example, assume that three additional safety functions have been identified ranging from a SIL 1 to SIL 2 requirement. All four safety functions will be implemented into an SIS.

The new SIS must then be designed according to the requirements for the highest SIL determined from the analysis of the safety functions. What this clearly implies is that the common elements of the SIS, such as the logic solver, must meet the SIL 2 requirements. However, SIS elements that can be shown to be independent, such as sensors, can be designed to meet the specific safety function SIL requirements.

7. Integrate safety functions in an SIS

The specifications for the new SIL 2 SIS have been defined through the hazard and risk analysis. The SIS must handle four safety functions that safeguard against a release of material to the environment. A new SIS can be designed in terms of sensor configuration (i.e. redundancy, voting, etc.), logic solver(s) requirements and valve configuration. [5] One such example of an SIS is shown in Fig. 8. The SIS shown includes the safety function against overpressure (safety dedicated dual pressure transmitters in a redundant loo2 configuration sending signals to a logic solver that controls one shutdown valve), and three additional safety functions to protect against other initiating events. The common elements of the SIS, logic solver, are assumed to meet the SIL 2

[4] loo2 means that either one of the pressure sensors can send a signal to shutdown the process.

[5] The example does not imply that only safety functions protecting the pressure vessel can be implemented in one SIS. The same SIS can also implement safety functions safeguarding other processes provided the same analysis is employed to identify the specification requirements of the safety functions.

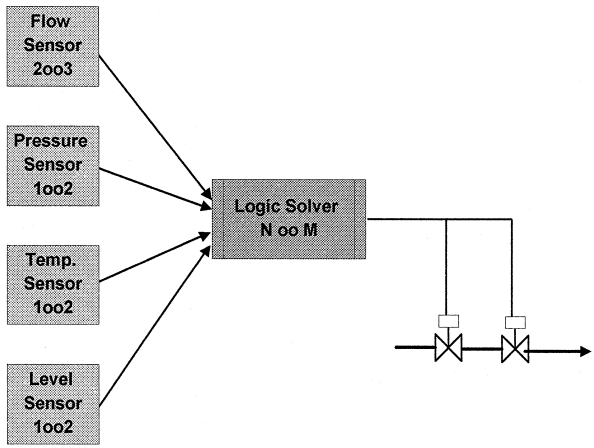

Fig. 8. Schematic of proposed SIS.

requirements supported either by reliability data taken from the manufacturer of the logic solver or through a reliability evaluation. Two shutdown valves in series are employed to place the process in a safe state.

At this point the proposed SIS configuration must comply with the requirements of the standards and meet the SIL that was identified through the risk analysis. It is beyond the scope of this paper to discuss techniques that may be used to evaluate the SIL of the proposed SIS.

8. Conclusions

Two performance-based safety standards (ANSI/ISA S84.01 IEC d61508) have been discussed. Compliance to the standard requires a hazards and risk analysis to establish the safety requirements for safety instrumented functions in terms of safety integrity levels. The identified safety functions were conceptually integrated into an SIS.

Several techniques to perform process risk analysis were discussed and their advantages and disadvantages identified. The benefits of each technique, in terms of initial cost, flexibility and life-cycle cost were discussed. A proposed approach to assess the risk associated with a new process in order to determine the safety functions that will be incorporated into an SIS and comply with the standards follows was illustrated through a simple example.

The success of any risk assessment technique will depend on the expertise of the analysis team and their experience with the process under investigation. If a user company has developed a significant experience base with the operation of a particular process, the hazards and hazardous events of interest are probably well known, and therefore a qualitative or semi-quantitative method can be used to identify the safety functions that should be implemented in an SIS.

Compliance to the standards and use of the aforementioned methodology provides several benefits to the user companies in the process industries such as:

- Compliance to one international standard such as the IEC d61508 which reduces operating costs for global companies.
- Achievement of a recognized level of process safety.
- Informed decisions when choosing a safety product for a specific application.
- Potential for improved operations and profitability by:
  - fewer losses
  - fewer process interruptions and therefore start-ups and shut downs
  - high process utilization and productivity

References

[1] IEC d61508; Functional Safety of Electric/Electronic/Programmable Electronic Systems, International Electrotechnical Commission, Draft Report, 1997.
[2] ISA S84.01; Application of Safety Instrumented Systems for the Process Industry, Instrument Society of America Standard, 1996.
[3] OSHA 29 CFR Part 1910; Process Safety management of Highly Hazardous Chemicals; Explosives and Blasting Agents; Final Rule, Occupational Safety and Health Administration, Washington, DC, 1992.
[4] EPA 40 CFR Part 68; Risk Management Programs for Chemical Accidental Release Prevention; Proposed Rule, Environmental Protection Agency, Washington, DC, 1995.
[5] IEC d61511; Functional Safety: Safety Instrumented Systems for the Process Industry, International Electrotechnical Commission, Draft Report, 1997.
[6] K. Bhimavarapu, L. Moore, P. Stavrianidis, Performance-based Safety Standards: An Integrated Risk Assessment Program, Presented at ISA Tech 97, Instrument Society of America, Anaheim, CA, 1997.
[7] CCPS — Guidelines for Safe Automation of Chemical Processes, Center for Chemical Process Safety of the American Institute of Chemical Engineers, NY, 1993.
[8] N.J. McCormick, Reliability and Risk Analysis, Academic Press, San Diego, CA, 1981.
[9] DIN V VDE 19250 — Fundamental Safety Aspects to be Considered for Measurement and Control Equipment, Germany, 1990.
[10] S. Contini, Benchmark Exercise on Major Hazard Analysis, Commission of European Communities, 1992.
[11] N. Siu, Risk Assessment for Dynamic Systems: An Overview, Reliability Engineering and System Safety, Vol. 43, 1996.
[12] ISA draft TR84.01: Application of Safety Instrumented Systems for the Process Industry, Instrument Society of America Standard, 1998.
[13] E.J. Henley, H. Kumamoto, Probabilistic Risk Assessment, IEEE Press, New York, 1992.