AIChE

Understanding Hazards, Consequences, LOPA, SILs, PFD, and RRFs as Related to Risk and Hazard Assessment

Roberto Fernández Blanco
DASIS Corp., Buenos Aires, Argentina; robertofblanco@gmail.com (for correspondence)

Published online 25 July 2014 in Wiley Online Library (wileyonlinelibrary.com). DOI 10.1002/prs.11700

This article is intended for any engineer, supervisor, or manager who does not specialize in process safety engineering. It presents the concept of layers of protection analysis, safety integrity level (SIL) and its relationship to probability of failure on demand (PFD) and the related risk reduction factors (RRFs). Novel SIL/PFD/RRF graphics are presented to help the reader understand the concepts involved. An example using a safety instrument function for a gas-fired boiler is also used to help the reader understand the concepts.

Keywords: risk assessment; hazards evaluation; safety engineering

INTRODUCTION

External safety engineers often arrive at a plant site expecting that terminology related to hazard and risk analyses are well known. For example, there are three "S" acronyms, SIL, SIS, and SIF that exist and the safety engineer may use all three in the same sentence. SIL is used for Safety Integrity Level and is associated with a Safety Instrumented Function (SIF). SIL is an integer with a value of "1," "2," "3," or "4." In low demand operations, a mode that occurs when the process demand frequency is less than once per year, these numbers are related to probability of failure on demand (PFD) and the risk reduction factor (RRF) [1]. The PFD is the likelihood that a system will fail to perform a specified function when it is needed. RRF is the reciprocal of the PFD. In high demand or continuous operations (an independent protection layer, IPL, is demanded more than twice its test frequency per year) [1], SILs are related to probability of dangerous failure per hour (PFH) [2]. More discussion follows in the examples and tables presented below. If SIL is implemented, it implies that a certain level of risk reduction will occur depending on the integer cited by the safety engineer or vendor.

At the highest level, SILs are related to the concept of independent layers of protection (IPLs) and the related Layer of Protection Analysis (LOPA) [3]. Often LOPA is applied after a process hazard analysis [4]. An initiating event is selected and a consequence is imagined. Then, a quantitative analysis is completed determining the frequency of the consequence based on layers of protection. Figure 1 presents the concept of layers of protection. Each layer has a RRF and a PFD (low demand) or PFH (high demand). Several of these layers depend upon process control. For example, the inside layer has a basic control system. It can be an instrumentation loop that controls a system deviation and prevents a major incident such as an explosion, fire, or release. An outstanding review of the general area of process control as applied to process safety is offered in Lee's [5]. Another layer of protection in Figure 1 is related to safety instrumented systems (SIS) and the related SIF. A SIS can be composed of several SIF's. However, a SIF is a singular safety control system with one sensor or more sensors, attached to a logic system that issues an output to a final element that should stop the dangerous conditions of the process [6]. Further, the SIF layer is the only layer that will have a numerical SIL attached to it as specified in industrial guidelines such as the International Electrotechnical Commission Standard 61511 [7]. For the chemical process industries, the concepts of SIL and SIS are discussed in a classic CCPS book *Guidelines for Safe Automation of Chemical Processes* [8]. Articles on SIS are offered by Summers *et al.* [9, 10] and Jin *et al.* [11].

In the article below, an example related to gas boiler safety is used to demonstrate the concepts. Additional PSP articles related to boiler safety have been offered by Cazabon and Erickson [12], Morrison *et al.* [13], and Lovejoy and Clark [14]. This article expands concepts presented in Ref. 15. A complete treatise is offered by the author as noted in Refs.16 (English) and 17 (Spanish).

PROCESS SAFETY MANAGEMENT

Thirty years ago, the science of process safety burst into day-to-day industrial activities like a hurricane. Primarily driven by OSHAs response to the 1984 Bhopal Incident [18], process safety management (PSM) became a regulatory requirement [19]. Along with it came the concepts such as SILs, which generated—among managers and department heads—the uneasy and disturbing sense that it was a "not an easily understood" concept. Rigorous prevention and protection measures are required to reduce—to below the levels deemed tolerable by the community—the risks derived from the hazards residing in industrial processes. The idea is to safeguard the health and physical integrity of individuals, the

This article was originally presented at the 3rd CCPS Latin American Conference on Process Safety held in Buenos Aires in August 2011. A Spanish version webinar was done in October 2008.

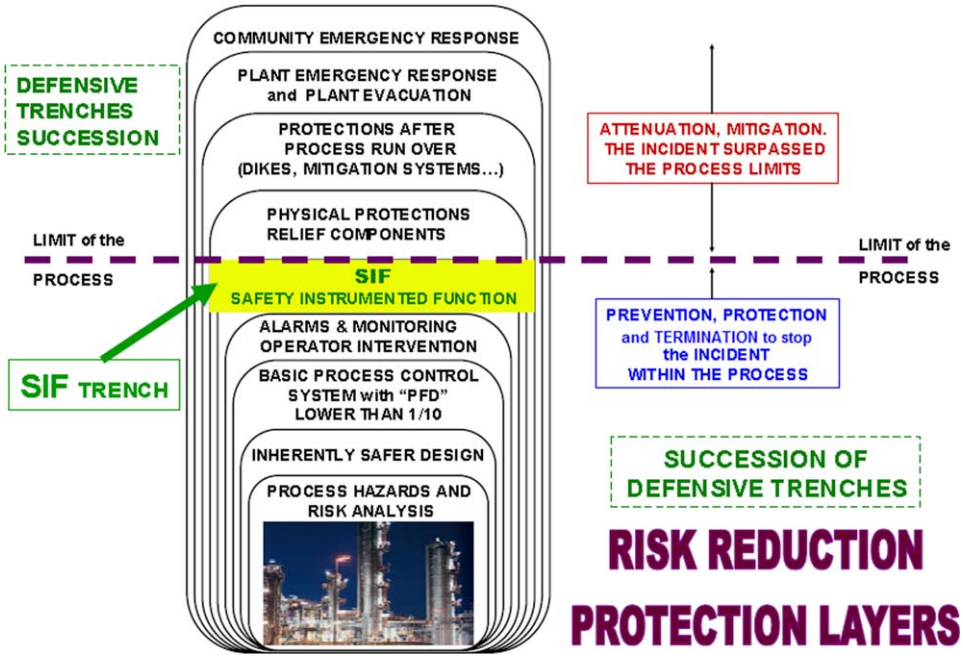

Figure 1. Risk reduction protection layers.

environment, production assets, and the continuity of plant operations.

KEY CONCEPTS

a. A process is deemed risky when it contains hazards with a damaging or destructive potential (e.g., a flammable or toxic material). The situation equivalent to keeping a fierce tiger in a cage that protects us from its attacks and consequent harm.
b. An initiating event is an occurrence that releases the tiger (by opening its cage door) and thus generates an incident that exposes us to the tiger's damaging potential. This condition, that is, exposure to the tiger's damaging potential (the hazard), is a danger. Hence the phrase "a hazard is a source of danger" (Figure 2).
c. The possibility of the tiger escaping from its cage is measured in terms of the frequency of an initiating event (an unlatched door opening), IEFi times the product of the PFD of the independent safety layers (in this example, the probability that an installed latch actually opens based on observation of the dropping of many branches on the latch).
The general mathematical relationship is provided as follows [1]:

$$f_i^C = \mathrm{IEF}_i \times \mathrm{PFD}_{i1} \times \mathrm{PFD}_{i2} \times \ldots \times \mathrm{PFD}_{ij} \quad (1)$$

Where:
f_i^C = frequency of the consequence occurring for scenario *i*.
IEF_i = frequency of the initiating event for the scenario *i*. Units are per time. Must be below 1 event/time unit.
PFD_{ij} = probability of failure on demand of independent protection layer *j* for scenario *i*.

For Eq. 1 to give correct results, an overall reduction in frequency of a consequence, f_i^C, the initial event frequency must be below 1 event per unit time used in the analysis. The time unit, or period, can be any convenient time units, for example, seconds, minutes, hours, days, months, or years. The typical default is per year for low demand processes (PFD), and per hour (PFH) for high demand and continuous processes. The example below will use months. PFD is the number of "failed" attempts divided by the total number attempts when the "demand" is called for. Ideally, the testing should be across several "periods" and an average failure rate per period used.
d. Once an initiating event has occurred, generating an incident, it can develop and escalate until it reaches an undesirable outcome (the tiger jumps out!), thus causing damaging and destructive consequences of various degrees of intensity, severity or magnitude. Consequences can be expressed in terms of number of fatalities, dollars lost in sales, or the total cost involved in the incident to recover.
e. The risk may be reduced by diminishing the potential damaging capacity of the hazard. That is, by reducing its level of consequences, and/or decreasing the frequency that an incident releasing its destructive force will start and spread. For example, the tiger in the cage could have a ball and chain attached to his paw that slows him down from biting Pedro.
f. If the incident has indeed arisen, the necessary action is to terminate it as soon as practicable, to prevent its development, escalation, expansion, and outcome.
g. "Risk", R, is defined in several ways. A recent CCPS definition cited that risk is "A measure of potential economic loss, human injury, or environmental impact in terms of the frequency of the loss or injury occurring and the magnitude of the loss or injury if it occurs" [1].
I will quantitatively represent the Risk (**R**) as the product of the frequency (**F**) times the Consequence (**C**) in an *XYZ* axes coordinate graph, as $\mathbf{R} = \mathbf{F} \times \mathbf{C}$, using arrows to indicate the magnitude of every value (Figure 3).
h. For the above graph to be meaningful, a reference criterion or benchmark (Tolerable Risk Level) should be established so that the risk can be assessed as high, low,

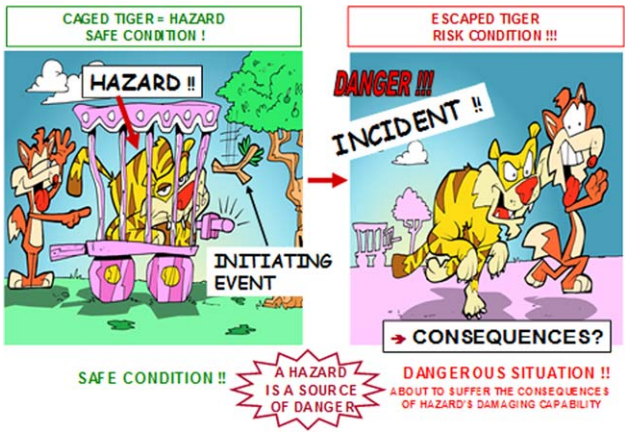

Figure 2. Concept of a hazard as opposed to an incident.

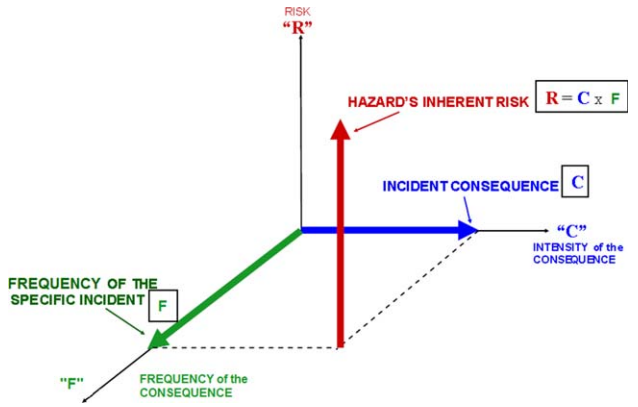

Figure 3. Risk graph of a specific hazard.

medium and primarily as "acceptable/tolerable" or as "unacceptable/intolerable." We will represent this reference Tolerable Risk as a level which cannot be exceeded by the risk arrow for the risk to be acceptable (Figure 4).

i. The analysis or assessment of the different risk levels will be performed by drawing a matrix on the base level (levels C–F) which may be subdivided into any number of rows and columns as long as these can be distinguished (Figure 5) from each other qualitatively (subjectively) or quantitatively (objectively).
j. The risk of the specific hazard under consideration can be reduced by means of an "inherently safer" redesign of the process (see Inherently Safer Chemical Processes, CCPS [20]), which reduces the intensity of the consequences and/or the likelihood or frequency that the incident will evolve and escalate.
k. If, after the process has been rendered "inherently safer", the hazard remains higher than the Tolerable Risk and we want—additionally—to stop and terminate it within the limits of the process, we will have to reduce the likelihood or frequency of the incident being initiated and escalating. This will require setting up a number of successive defensive trenches (such as those that guard a fortress from an enemy attack), which are known as layers of protection [3].
l. As the "attack to the community" (incident) is initiated, arises, and escalates from the "source" of the process (the release of the tiger), the trenches or defensive layers are set up serially from such source outward, as shown in the Figure 1.

EXAMPLE OF APPLICATION

Let us analyze a specific defensive trench, namely, the layer of protection consisting of a Safety Instrumented Function (SIF) implemented for the protection of a furnace, boiler, or home water heater, in the event of a flameout in the burner. An article with a broader overview of LOPA applied to a steam boiler is offered by Morrison *et al.* [13]. In our example, the flameout incident will cause the furnace or boiler to begin to fill up with an explosive mix of flammable material (natural gas, for instance) and air, a type of incident that must be terminated very quickly. Thus, a protective SIF consisting of three serially lined-up and linked components is installed: a flame detector linked to a safety controller linked in turn to a shut-off valve to hermetically close and block the gas flow (Figure 6).

Whenever the burner flames out (initiating event), the flame detector sends a "flame out" signal to the processor. This processor sends out a demand to the safety controller, which, in turn, sends a demand to the shut-off valve instructing it to shut off the inflow of gas into the burner. If upon any of these successive "demands for protection" one of the links should malfunction and fail to perform its intended role, the valve will not shut off, there will be no protection, the gas will keep feeding the firebox, and the incident will escalate until it reaches a catastrophic outcome (explosion).

This highlights the importance of ensuring the integrity level of the equipment that makes up the SIF protective loop, as measured in terms of its risk reduction factor (RRF = 250) and that the PFD = 1/RRF = 1/250 or 0.004. In our figure, we have considered a RRF = 250 (a fictitious value used solely for illustration purposes), meaning that—on average—out of every 250 times the flame burns out (and the process demands protection) the SIF function will properly fulfill its protective action on each such occasion except one (1 in 250). This particular result was established after several months of running demands and determining the average number of failures per month.

Figure 7 is an elementary way of representing probability. I use several references to die and gambling spinning wheels in the narrative that follows.

To sum up, the process has per se an inherent flameout likelihood, and, in addition (as will be seen later), there is the failure demand probability that the SIF protective loop may fail. If both circumstances occur, it will not be possible to stop and terminate the incident, which will escalate until it reaches a catastrophic outcome.

HAZARD, INCIDENT, AND SIF

Each hazard residing in a process, as well as the potential incident it is capable of generating, is proper to and inherent in the nature of the process itself. For the same reason, the average frequency with which the specific incident is initiated is also an inherent characteristic specific to the process itself and the manner in which it is operated. It may be helpful to view the process as a series of resident hazards where one is "activated" by an initiating event, which gives place to a specific incident that will develop, escalate, and spread—depending on its inherent potential—until it reaches its outcome, provoking consequences of various degrees of intensity or severity. The inclusion of a SIF protective function will not alter the nature of the process or of its hazards, nor the frequency of occurrence of the incident involved. The

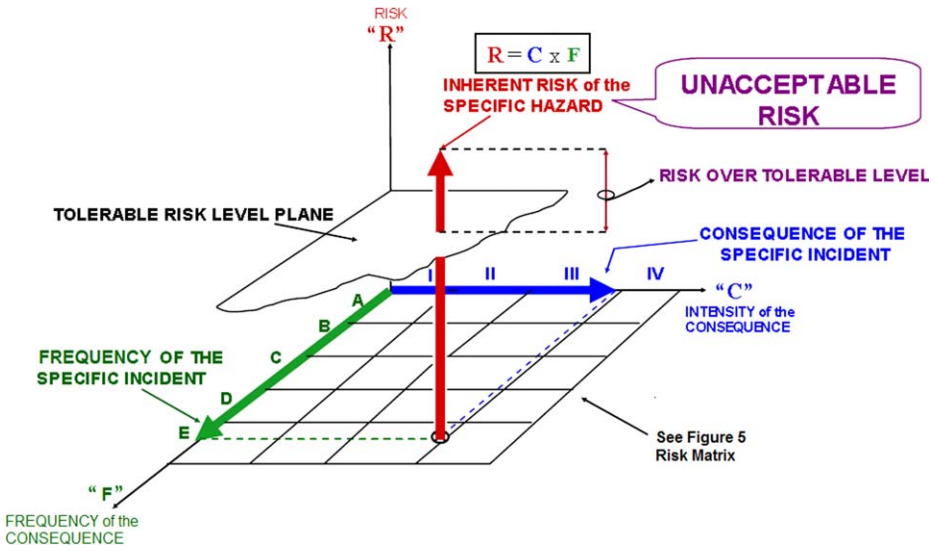

Figure 4. Risk graph with a tolerable risk level plane.

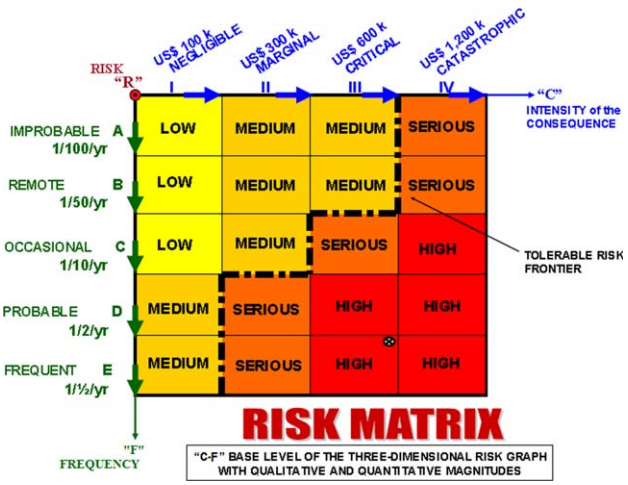

Figure 5. Risk matrix.

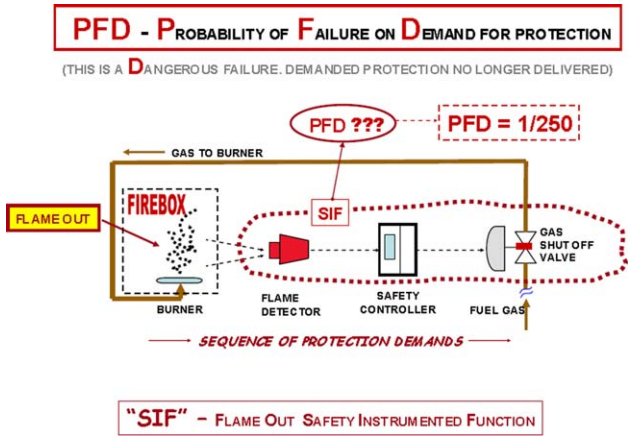

Figure 6. Flameout safety instrumented function for a firebox.

SIF function merely detects the hazard "activated," condition that generate the incident and then executes an immediate stop and termination action.

However, the SIF loop is not an entirely perfect arrangement. Its terminative action can fail, thus allowing the incident to escalate until it reaches its outcome and to cause its damaging and destructive consequences. This makes it all the more important to install a SIF loop with the appropriate levels of reliability and integrity, in line with the harmful potential of the hazard and the level of risk posed by the specific incident. Reliability means the proper execution of the actions for which the SIF was installed, and integrity refers to its resistance, strength, and toughness not to falter in performing its protective action, but rather to execute it in due manner and time.

Let us examine a single-burner boiler more carefully (Figure 8).

In Figure 8, several initiating events can occur: burner flame out, feed water loss, or implosion of the superheating zone. The protective system for burner flame out includes two flame scanners.

First, we should find out the event frequency of a flameout in the burner. Statistical records (fictitious values for purposes of this explanation) confirm that in this type of boiler the flame tends to be out (on average), 1 time every 6 months. The incident frequency is 1/6 month^{-1} or 0.167 month^{-1}. Note that the incident frequency is less than one and thus, Eq. 1 can be used.

Another view point on flameout frequency statistic can be consider that if a plant has six equal boilers, each month, one of these boilers will flame out. For purposes of this industrial analysis, let us assume that a company has only one boiler. Thus, the 1/6/month unwanted flameout rate of the burner is represented by a six-sided die bearing a bomb symbol (Figure 7) on its #1 side. This means that we should roll the die once a month and that, whenever the die falls with the bomb "head up," this means that the burner has flamed out and given rise to the initiating event. If this

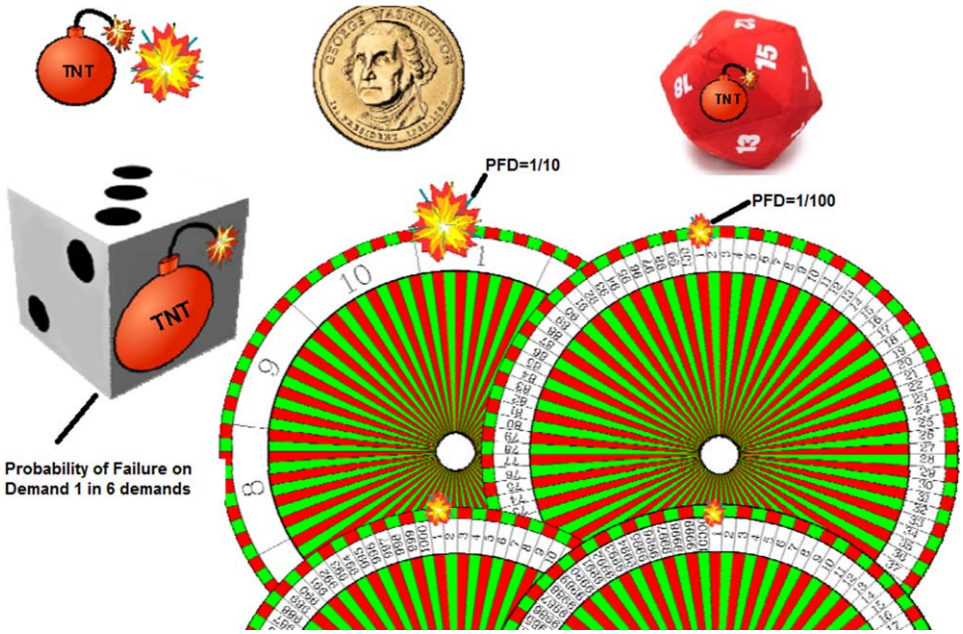

Figure 7. Conventional ways to demonstrate probability of failure.

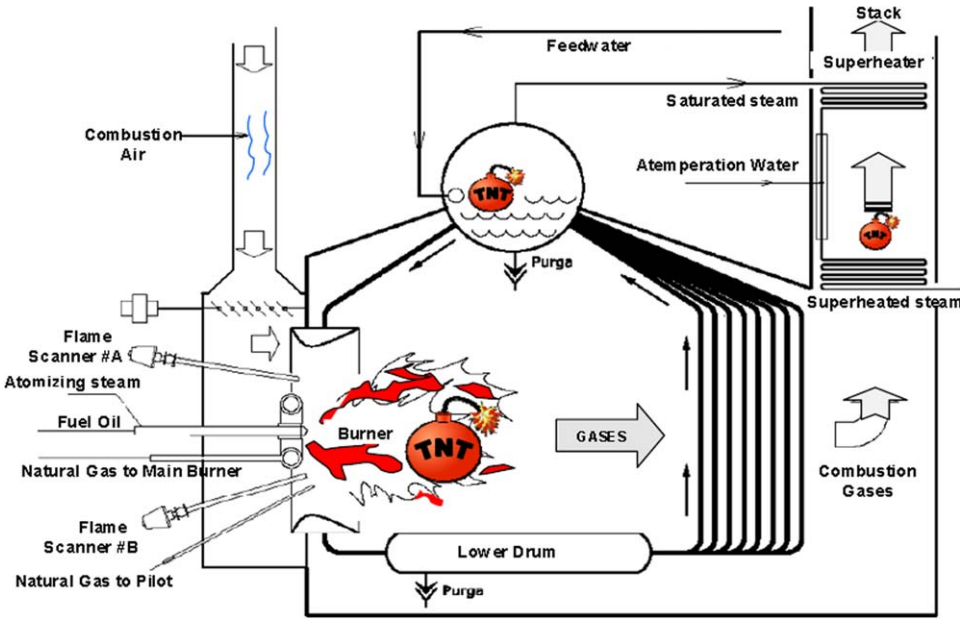

Figure 8. Example of a boiler and various hazards in place.

six-sided die is rolled once a month, the average probability (considering long periods) for the bomb to land head up will be once every six times the die is rolled, that is, once every six months, equal to 1 unwanted flameout every 6 months.

Thus, the boiler suffers a flameout every 6 months it will have two flameouts per year, that is, two incidents per year that will tend to lead to the explosion and destruction of "two" boilers per year, with—additionally—potential serious injuries to the plant personnel. Clearly, running the risk of destroying two boilers per year, plus the associated injuries to the personnel and the disruptive effects on the continuity of the plant's operations, is wholly unacceptable.

The Key Question is, then, What is the Tolerable Risk Level?

The answer should be provided by someone in charge, namely, the plant's operating manager; the company; the government through a law, executive decree, or regulation; the technical agencies having jurisdiction over these issues; risk insurance companies, or professional references such as

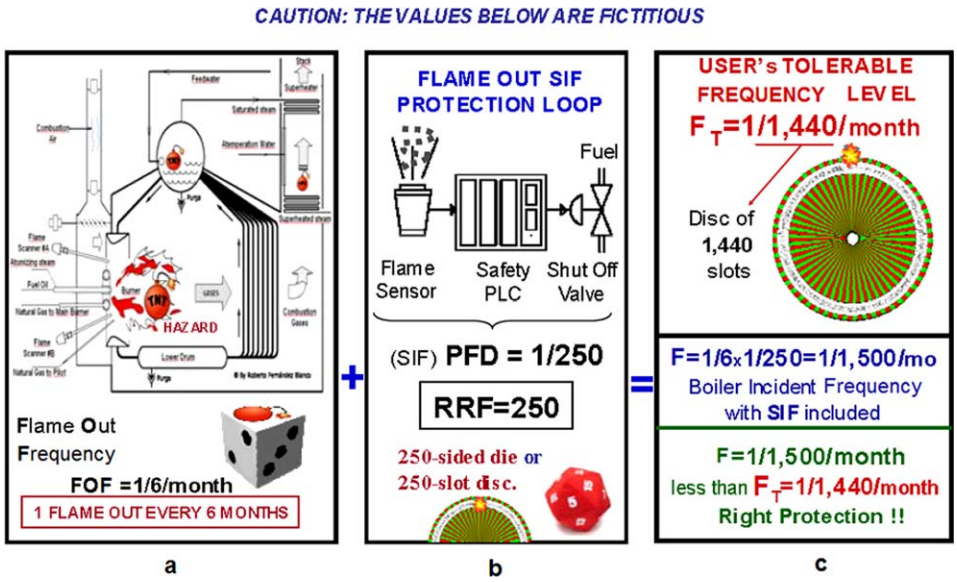

Figure 9. Risk probability reduction through a protective SIL.

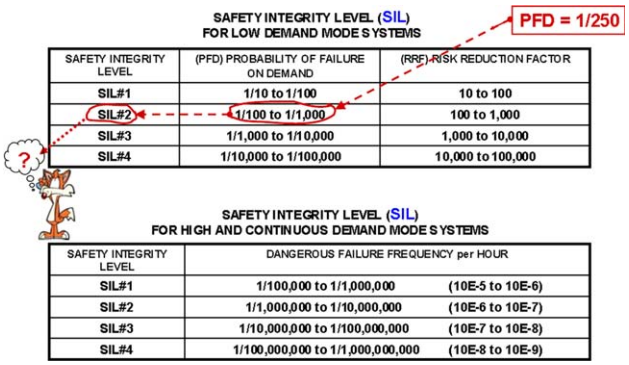

Figure 10. Conventional SIL category table.

those offered by the AIChE Center for Chemical Process Safety (CCPS) [21, 22].

By way of example, let us assume that the company imposes a maximum tolerable frequency for serious destruction by a flameout to be 1 time every 120 years or 1 time in 1,440 months, that is, an average frequency of one boiler — out of 1,440— experiencing a catastrophic flameout each month.

Based on the above two values, the initiating frequency of flameout (1/6/month) in the boiler and the maximum tolerable frequency for destruction of the boiler (1/1,440/month), we can calculate the integrity (strength not to falter in performing its protective action) of the SIF function that should be added to the boiler in order to avoid the flameout-related incident and thus reduce from 1/6/month to 1/1,440/month (or less), the possibility that such incident will develop and escalate until it reaches its destructive outcome (explosion in the firebox).

To achieve this flameout protection, an SIF function with an Integrity of RRF = 250 will work. This SIF with RRF = 250 (PFD = 1/250 or a single probable failure for every 250 protection requests) can be represented by a 250-slot gambling wheel with only one "yellow" slot and all the rest of the slots white. Now, two things have to happen to reach the destructive outcome. The six-sided die has to come up with the "bomb" appearing face up (Figure 9a). The 250-slot gambling wheel has to stop on the single yellow spot (see base of Figure 9b). This combination reduces the frequency of a destructive outcome by 1/1,500/month which is less than the 1/1,440/month required by the company's management (Figure 9).

A key conclusion to be drawn from this analysis is the significant and determinant role played by the Failure-on-Demand Probability Wheel that represents the Integrity of the SIF function.

- The number of slots in the Failure-on-Demand Probability Wheel provided by the SIF protective function represents the RRF.
- A wheel having fewer slots than the required RRF, the required protection level cannot be achieved.
- The proper, or higher, level of protection can only be achieved with a SIF function represented by a Probability Wheel with a number of slots equal to or higher than the required 250 (i.e., an equal or higher RRF).

Comparison with SIL

Once the necessary risk reduction has been calculated by determining the RRF or the required PFD for the SIF protection, conventional SIL tables (Figure 10) can be used determine the SIL for this application. For this example, the SIL falls in the level "2." Note that there are two tables in Figure 10. The first table is for low safety system demand mode. The PFDs ranges are on an annual basis. The second table is for high safety system demand operations. The PFH's are presented as Dangerous Failure Frequencies per hour basis. The RRFs remain the same and match with the SIL number. Identical SIL numbers in each table means the specification in terms of a SIF.

But beyond the systematic use of such tables, as dictated by standard practices, the concept, essence, and content of the SIL remain unexplained. To address this challenge, in 2005, I chose to discontinue the use of those conventional

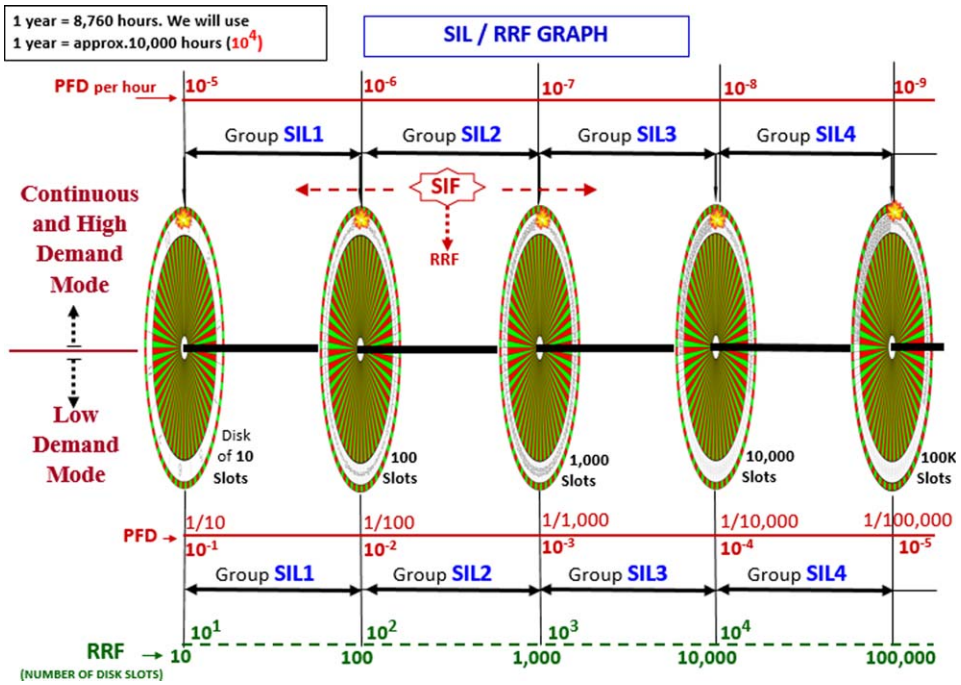

Figure 11. SIF's RRF selection in the SIL/RRF Graph.

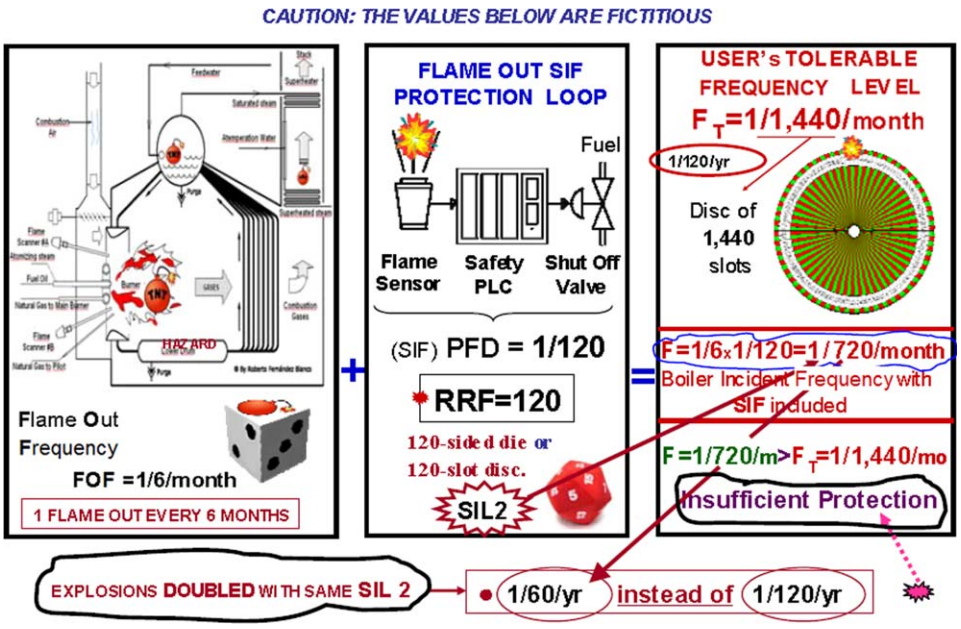

Figure 12. Insufficient protection even though a SIL 2 was purchased as specified.

tables and to replace them with a new SIL/RRF graph (Figure 11), whose construction unveils the mystery of SIL as related to PFD, PFH, and RRF.

In designing this new graphic, I simply used what is necessary for the process, that is, the RRF represented by a Probability Disk, similar to a roulette wheel, with the number of slots equal to the necessary RRF number.

Looking at Figure 11 one can imagine a little cart rolling on imaginary rails, in which the SIF function (metaphorically) "travels" in search of the Probability Wheel that represents the RRF required by the process-specific hazard in order to reduce below the Tolerable Level—as set by the company—the resulting probability that the incident will escalate until it reaches its outcome.

The novel SIL/RRF graphic provides several benefits:

1. Makes it clear that each SIL Level represents a "group or set" of "Probability Disks" or RRFs.

2. Includes in a single graph what previously required two conventional Tables: the bottom half shows the SIL/RRF for processes in the Low Demand Operation Mode, while the upper half includes those for the High or Continuous Demand Operation Mode.
3. Indicates whether or not the SIF loop that effectively provides the required Risk Reduction is being introduced.

EXAMPLES OF MISUNDERSTANDING

Case #1

This example illustrates the protection introduced in the boiler as explained above. The analysis has confirmed that the RRF = 250 required for the SIF belongs to SIL2 (Figure 11). Based on this input (SIL2), a Safety Requirement Specification (SRS) is drafted (pursuant to the conventional procedure) to acquire a SIL2 protection function. With this SRS, the procurement department will purchase a SIL2 SIF loop provided by any of the well-established international manufacturers of SIF functions. When the function has been installed in the process and the commissioning to start up the plant is underway, a validation procedure is carried out to confirm that the installed SIF is actually SIL2. However, as at the time of purchase of the SIF, the required RRF had not been specified (250-slot probability disk), upon completion of such validation procedure the installed SIF is found to have a specific SIL2 Integrity in line with a RRF = 120 (120-slot probability disk). The result of this difference is evidenced in Figure 12.

The SIL/RRF Graph confirms that the SIF with a RRF = 120 probability disk belongs to the SIL2 group as requested. The boiler figure shows that, with that SIL2-level SIF and RRF = 120, the probability that the incident may escalate until it reaches a catastrophic outcome will be an Overall PFD of 1/6/month × 1/120 = 1/720/month, that is, twice as high as the Tolerable Risk as set by the company (1/720/month = 2/1,440/month is double the Tolerable Risk of 1/1,440/month).

The most important benefit this new SIL/RRF Graph provides is that it renders "self-evident" and obvious that setting a SIL value is not enough to define the SIF needed to adequately protect the process.

What the process needs is to reduce the risk of the specific hazard to below the acceptable value set by the company. To achieve this, the proper RRF should be accurately determined (or else a somewhat higher RRF should be selected, with a wheel containing a larger number of slots).

Case #2:

Even with a targeted RRF, good practice suggests rounding up the specification to address uncertainty. If a required RRF for a process was 999, then one might consider that an SIL Level 2 safety instrumented instrument will work. There are two reasons this may not work. One SIL Level 2 instrument RRF ranges from 100 to 1,000, and odds are very low that the instrument purchased has an RRF of 1,000. Second, there is a degree of uncertainty throughout the process. The required RRF should then be rounded up, to an adequate RRF that will introduce a proper margin of safety added, moving in this particular case the SIL to become Level 3. Finally, when the required RRF is close to an upper boundary one should return to the process to see if any changes can be made to reduce the RRF. There are significant incremental instrument costs and complexities as one moves from a SIL 1 SIF through to a SIL 3 SIF.

CONCLUSIONS

This article provides a clearer understanding of the SIL concept, as it demonstrates that each SIL level actually groups several successive probability disks (or RRFs). It also clearly shows that the essential purpose of PSM is to run the process (in a sustainable manner) with the proper risk reduction**,** that is, with an appropriate RRF.

Naturally, the RRF risk reduction capability should be preserved through a rigorous preventive maintenance effort to keep the equipment in an "as new" operating condition in order to prevent the RRF from gradually degrading over time with an ensuing increase of the risk level over and above the tolerable level allowed. This is as important as checking and maintaining—with the same degree of dedication, care, precision, and perfection—the condition of the brakes in a car used daily. The probability of failure will continue to grow (degrade) if no proper and timely check-ups, "as new" maintenance and required testing are carried out, all of which should be carefully specified and scheduled before start-up and rigorously and continuously complied with as long as the car is in use.

Hence the recommendation, repeatedly made by this author to managers and department heads, is to buy a conventional six-sided die, slap a bomb sticker on its face numbered "1," keep it permanently on their office desk and roll it every day when they arrive at the plant. The author has indeed found that those who have received a "bomb-die" as a gift have become more aware of the problem and changed their habits as to the degree of attention and care they devote to ensuring a sustained maintenance effort to take all the Protection Layer components back to an "as new" condition. As the passive element of any culture entails habits, customs and usage, this simple game generated a positive cultural growth dynamics in PSM, the key objective of the CCPS's mission.

ACKNOWLEDGMENT

I express my gratitude to Ronald J. Willey, Ph,D.,PE, for his assistance in the preparation of this article.

LITERATURE CITED

1. Center for Chemical Process Safety (CCPS), Guidelines for Initiating Events and Independent Protection Layers, Wiley, New York, 2014.
2. International Electrotechnical Commission, International Standard IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, Geneva, Switzerland, 2010.
3. AIChE, Layer of Protection Analysis: Simplified Process Risk Assessment, Center for Chemical Process Safety, Wiley, New York, New York, 2001.
4. A.M. Dowell, Layer of Protection Analysis: A New PHA Tool, after HAZOP, before Fault Tree Analysis, American Institute of Chemical Engineers, New York, Atlanta, GA, 1997.
5. S. Mannan, Lees' Loss Prevention in the Process Industries, Volumes 1-3 - Chapts 8,9,&13 Hazard Identification, Hazard Assessment and Control System Design, 4th Edition, Elsevier, 2012.
6. B. Mostia, The Safety Instrumented Function an S-Word Worth Knowing, Control, 2003, Available at **http://www.controlglobal.com/articles/2003/255/**, Accessed on July 3, 2014.
7. International Standard IEC 61511-1 Functional Safety – Safety Instrumented Systems for the Process Industry Sector, IEC, Geneva, Switzerland, 2003.
8. Center for Chemical Process Safety (CCPS), Guidelines for Safe Automation of Chemical Processes, Wiley, New York, 1993.

9. A. Summers, Safe automation through process engineering, Chem Eng Prog 12 (2008), 41–47.
10. A.E. Summers and W.H. Hearn, Risk criteria, protection layers, and conditional modifiers, Process Saf Prog 31 (2012), 139–144.
11. H. Jin, M.A. Lundteigen, and M. Rausand, Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation, Reliab Eng Syst Saf 96 (2011), 365–373.
12. M.D. Cazabon and K. Erickson, An oven explosion: Lessons learned on PSM applications, Process Saf Prog 29 (2010), 87–93.
13. D.T. Morrison, M. Fecke, and J. Ramirez, Using layer of protection analysis to understand necessary safeguards for steam boiler operation, Process Saf Prog 31 (2012), 248–254.
14. G.R. Lovejoy and I.M. Clark, Furnace safety systems. A state-of-the-art review of current practice for safe and reliable control of industrial boilers, Plant Oper Prog 2 (1983), 13–21.
15. M. Charlwood, S. Turner, and N. Worsell, A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines, Research Report 216, Health & Safety Executive, 2004, Available at **http://www.hse.gov.uk/research/rrpdf/rr216.pdf**, Accessed on July 4, 2014.
16. R.F. Blanco, SIL or RRF that is the Question, 2011, Available at **http://www.dasiscorp.com/pdf/SN-516-11-English-SIL-or-RRF-for-CCPS.pdf**, Accessed on June 12, 2014.
17. R.F. Blanco, SIL or RRF that is the Question, 2011, Available at **http://www.dasiscorp.com/pdf/SN-516-11-Articulo-SIL-or-RRF-para-CCPS.pdf**, Accessed on June 12, 2014.
18. M. Heylin, et al., "Bhopal - The Continuing Story," Chemical and Engineering News 63(6), (1985), 14–40, DOI: 10.1021/cen-v063n006.p014.
19. OSHA, Process Safety Management of Highly Hazardous Chemicals, Final rule first published in 24 Feb 1992, Available at **https://www.osha.gov/SLTC/processsafetymanagement**, Accessed June 12, 2014.
20. Inherently Safer Chemical Processes: A Life Cycle Approach, 2nd Edition, Center for Chemical Process Safety, Wiley, New York, NY, 2009.
21. Center for Chemical Process Safety (CCPS), Guidelines for Developing Quantitative Safety Risk Criteria, Wiley, New York, 2009.
22. Center for Chemical Process Safety (CCPS), Guidelines for Risk Based Process Safety, Wiley, New York, 2007.