AN IMPROVED RISK GRAPH APPROACH FOR DETERMINATION OF SAFETY INTEGRITY LEVELS (SILs)

A version of the paper appeared in *Process Safety Progress*, Vol. 26, No. 1, pps. 66 - 76.

by Paul Baybutt
Primatech Inc.
50 Northwoods Blvd.
Columbus, OH 43235

Abstract

Risk graphs are one of the techniques used to determine Safety Integrity Levels for the Safety Instrumented Functions that make up Safety Instrumented Systems for processes. The standard risk graph approach originated in a German standard published in 1994. The standard approach has a number of disadvantages which are delineated in this paper. An improved risk graph approach has been developed to overcome these disadvantages. The improved method is described and an example of its application is provided. The improved method preserves the simplicity of risk graph methods while providing a theoretical foundation that facilitates moving into more refined methods such as Layers of Protection Analysis (LOPA*) or Quantitative Risk Analysis (QRA), if needed. Furthermore, the improved risk graph method can be incorporated easily into Process Hazard Analysis (PHA).

Introduction

Process control systems can be considered to be either Basic Process Control Systems (BPCSs) or Safety Instrumented Systems (SISs)(1). BPCSs respond to input signals from a process and generate output signals to direct the process to operate as intended. SISs are systems or devices that take the process to a safe state when the process operates outside normal defined limits. They are of critical importance in helping to ensure the safety of processes. SISs are made up of one or more Safety Instrumented Functions (SIFs) that are actions taken by the SIS to bring the process to a safe state. Each SIF consists of a set of actions to protect against a single specific hazard.

Requirements for SISs are addressed in the international standard IEC 61508(2) and the process industry sector-specific version IEC 61511(3). The US equivalent of IEC 61511 is ANSI/ISA S84.00.01-2004(4). These standards are intended to help ensure that SISs achieve certain minimum performance levels to help ensure safety and environmental protection as well as provide economic benefits. They address all safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning.

A key performance criterion for a SIF is its Safety Integrity Level (SIL). This is a numerical target for the Probability of Failure on Demand (PFD) of a SIF that operates in demand mode, or the Frequency of Dangerous Failures (FDF) for a SIF that operates continuously. Four integrity levels are defined by the standards (SIL 1, SIL 2, SIL 3, SIL 4); the higher the SIL, the more available the safety function. The standards provide a framework for establishing SILs although they do not specify the SILs required for specific applications. They suggest the use of various methods to determine the PFD or the amount of risk reduction needed. These methods include Risk Graphs(3,5) and Layers of Protection Analysis (LOPA)(6,7). LOPA has achieved popularity in the US and Risk Graphs in Europe. The terms *classification* and *selection* are also used to mean the determination of appropriate SILs for SIFs. In contrast, SIL *verification* means the determination that specific SIFs achieve a particular SIL.

Risk Graphs

Risk graph approaches are based on methods described in the German publication DIN V 19250(5). They enable SILs to be determined using process risk factors or *parameters* for hazardous events. Usually, four parameters are employed (Table 2):

C - Consequence of the hazardous event

F - Frequency of presence in the hazardous zone and the potential exposure time, or Occupancy

P - Probability of avoiding the hazardous event

W - Probability of the unwanted occurrence

Parameter values are combined together in order to estimate the risk, R, of the hazardous event. The combination of C with F and P is intended to represent the *effective* consequence (see Figure 1). W is the frequency of the hazardous event taking place without SIFs in place but with other safeguards operating, or the *effective* frequency. Risk graphs combine the effective consequence with the effective frequency of the hazardous event to determine a SIL that will reduce the risk to a tolerable level (see Figure 1).

DIN V 19250 provides definitions of four levels of consequences, two exposure times, two probabilities of avoiding the hazardous event, and three probabilities of the unwanted occurrence. However, these definitions are highly subjective and can lead to inconsistent results and possibly conservatism that may result in SIL overestimation. Lack of consideration of dependent failures between sources of demand and SISs may over-estimate SIS effectiveness.

Current risk graph approaches suffer from these disadvantages:

- The parameters used do not facilitate discrimination between the risks of different scenarios. SILs differ by orders of magnitude. Risk graph parameters should be chosen to facilitate assignment into order-of-magnitude categories. The biggest discriminators are the frequency of the initiating cause and the probability of intermediate events, including safeguard failures. They vary by orders of magnitude. However, current risk graph approaches lump these into a single category (W). Occupancy (F) and the probability of avoiding hazards (P) are each treated as separate parameters. Typical ranges for these parameters do not provide much discrimination between scenarios. More quantitative methods, such as LOPA, often consider F to be in the range 0.1 - 1 when expressed as a probability of being in the lethal zone, and P to be in the range of 0.1 - 1 too. Furthermore, the probabilities of other enabling events/conditions (enablers) can be significant but they are not considered by current risk graph methods.

- Use of only two levels for some parameters forces a choice that, if the levels are not defined carefully, may be either too conservative or too optimistic. It can be difficult to choose between two levels and people are more likely to disagree since there is no middle ground. For example, the standard definitions of the two levels of the F parameter (frequency of presence in the hazardous zone and the potential exposure time) are:

  - F_1 - Rare to more frequent exposure in the hazardous zone
  - F_2 - Frequent to permanent exposure in the hazardous zone

  Similarly the standard definitions of the two levels of the P parameter (possibility of avoiding the hazardous event) are:

  - P_1 - Possible under certain conditions
  - P_2 - Almost impossible

  Such definitions tend to be viewed as occupying the extremes of the ranges of these parameters and do not allow for assignment of values in the middle of the range.

- Current risk graph schemes can be confusing. For example, the F parameter in the standard risk graph method actually combines two factors, the frequency of presence in the hazardous zone as well as the potential exposure time to arrive at occupancy. Similarly, the standard method calls for five factors to be considered when deciding on the level of the parameter P: 1) Operation of a process (supervised by skilled or unskilled persons, or unsupervised), 2) Rate of development of the hazardous event (suddenly, quickly, slowly), 3) Ease of recognition of danger (seen immediately, detected by technical means, detected without technical measures), 4) Avoidance of hazardous event (escape routes possible, not possible, or possible under certain conditions), 5) Actual safety experience (with an identical or similar process, if it exists). Ambiguity in parameter definitions and possible overlap in parameters may result in credit being taken twice for the same factor.

- Definitions of the parameters are misleading. F is actually a dimensionless quantity when the frequency of presence in the hazardous zone is combined in a ratio with the potential exposure time to determine the occupancy. W, the *probability* of the unwanted occurrence, is actually the *frequency* of the unwanted occurrence. Users of risk graph methods can be easily confused over the difference between probability and frequency and these definitions do not help.

- Emphasis on consequences can lead to the domination of over-safe solutions.

- Guidance on using the standard Risk Graph method suggests that "The interpretation and evaluation of each risk graph branch should be described and documented in clear and understandable terms to ensure consistency in the method of application" (Annex E, ANSI/ISA S84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3 (4)). However, such documentation actually does not provide any assurance that the method will indeed be applied consistently. Documentation of results of SIL determination in using risk graphs is addressed in Annex D, ANSI/ISA S84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3 (4). However, there are no requirements, standards, or guidelines for documenting the decisions and any assumptions that are made when determining SILs using risk graphs.

Improved Risk Graph Method

An improved risk graph method has been developed. It focuses on scenario risk, not consequences. It uses four parameters (Table 3):

I (Initiators) - Initiating cause frequency

E (Enablers) - Enabling events/conditions and other modifiers

S (Safeguards) - Safeguards failure probability

C (Consequences) - Consequences of the hazardous event or scenario

An example of the improved risk graph is shown in Figure 2. The following steps are followed for each hazard scenario analyzed.

Step 1: Assign parameter for the initiating cause (I parameter).

Six levels of initiating cause frequency are used, I1 through I6. Their assignment is based on the types of failure which are categorized as equipment failures, human failures, and external events (see Tables 4 - 6).

Step 2: Account for any enablers or conditional modifiers (E parameter)

Enablers do not directly cause the scenario but must be present or active for the scenario to proceed, for example, the process being in a particular mode or phase. Other examples include alarms disabled, safeties bypassed, preventive maintenance not performed, and extreme ambient conditions.

Conditional modifiers that are commonly considered are the probability that released flammable/explosive material will ignite, the probability that a person will be present to be exposed to a hazard, and the probability than an exposed individual will actually be injured.

Two levels are used for the E parameter:

E1 – one or more present

E2 – none considered

In order to be credited, enablers and modifiers must provide at least a 1 in 10 reduction factor for risk. A more conservative approach is not to take credit for any enablers and, if necessary, address them in LOPA or QRA.

A refinement of the method is possible in which greater amounts of risk reduction from enablers can be included by reducing the I parameter from its otherwise assigned value. For example, if a scenario is assigned to the I3 level and has one or more enablers that together are believed to reduce the risk by 0.01, the E parameter can be assigned as E1 and the I parameter level reduced to I2. Often, it is the initiating cause frequency that is adjusted by the probabilities of such enablers in LOPA so this refinement is consistent with LOPA methods.

Some enablers may act to increase the scenario frequency or event probabilities. They can be accounted for by suitable adjustments in the I and S parameter levels.

Step 3: Select risk matrix to use according to safeguards present (S parameter)

Three levels are used for safeguard failure probability:

S1 – one allowable Category 1 safeguard or two or more allowable Category 2 safeguards

S2 – one allowable Category 2 safeguard

S3 – no allowable safeguards

An example of allowable safeguards for the two categories are provided in Table 7. Category 1 safeguards have lower failure probabilities than Category 2 safeguards, i.e. they are less likely to fail when needed. Unallowable safeguards can be recorded but no credit should be taken for them in the risk graph analysis.

Users of this improved risk graph method should assign safeguards used in their processes to one of these categories. Suggested criteria that can be used to guide this assignment are:

- Allowable safeguards should be chosen so they will likely fail independently.

- Passive safeguards are usually assigned to Category 1. Active safeguards can be assigned to Category 1 but are usually assigned to Category 2.

- Category 1 safeguards should have a failure probability an order of magnitude less than Category 2 safeguards.

- Unallowable safeguards include training, procedures, experience, monitoring and surveillance, and controls provided by the BPCS, and any other safeguards for which a failure probability of less than or equal to 0.1 cannot be claimed. Risk graph methods are intended to be simple but conservative. Therefore, they do not try to account for all safeguards. While training and procedures are vital, they are actually weak safeguards since they rely on the actions of people and it is well established that human failure rates are generally higher than those for equipment. Even SIS standards restrict the amount of credit that can be taken for BPCS controls to no more than 0.1(4).

- Ideally, data on safeguard failure probabilities, preferably plant-specific, should be used to make these assignments. The theoretical foundation of the improved method described later in the paper provides the basis for doing so.

Step 4: Assign consequence (C parameter)

Separate schemes are used for each consequence type, e.g. personnel safety, environmental impact, business impact. Five levels are used for each consequence type to provide appropriate discrimination between the possibilities usually encountered in process plants (see Table 8).

Note that Tables 4 - 8 are intended as examples. In practice, more items are included. Ideally, companies should tailor the assignment of initiators and safeguards to levels based on failure data from their own operating experience and environment. If such data are not available or are not adequate, generic failure data from industry sources, for example, Reference 6, can be used. The basis for the assignments should be recorded as part of the Risk Graph documentation.

Step 5: Determine required risk reduction (SIL)

The risk graph defines required IEC 61508/61511/S84 SILs according to the various combinations of risk graph parameters for a hazard scenario. Scenarios that do not require risk reduction require no further analysis. For scenarios requiring risk reduction, the analysis can be refined using other methods such as LOPA and QRA, or the improved risk graph results can be accepted, for example, when only low SILs are needed.

Step 6. Document the Analysis

The integrity of SIL determination and its transparency are very important. Therefore, the decisions and any assumptions that go into each SIL determination should be documented. Documentation produces several benefits. Analysts are encouraged to carefully determine SILs since the basis of their determination is made clear for anyone to see. Technical reviewers and other interested parties are provided with the information needed to evaluate the validity of the analysis. Also, SIL determinations can be more readily updated when process changes are made.

Typically, the results of using the improved risk graph method are recorded in a PHA or PHA-type worksheet (see examples in the next section), rather than just recording the SIL required. While such documentation is not necessary for use of the improved method, it clarifies the analysis. The worksheet contains the values of the risk graph parameter levels for each scenario. In addition, these guidelines should be followed for documentation:

- Initiators:
    - Clearly identify initiating causes and specify, as appropriate, who, what, where, etc.
    - Identify the way failures occur and provide appropriate detail. For example, the *immediate* cause of a scenario may be that a pump fails off, but usually the *basic* causes for the pump failure should also be specified, e.g. loss of power, switched off by the operator, mechanical failure, etc.
    - Clearly identify equipment, controls, instrumentation, etc. using tag numbers, names, or other identifiers. The identifiers used must correspond with P&IDs, procedures, etc.
    - Word entries so their correspondence to the table of Initiator parameter levels is clear.

- Intermediate Events
    - Identify any important aspects of the scenario not captured by the initiating cause and consequence entries. For example, scenarios may involve events, besides the failure of safeguards, such as responses by the BPCS.
    - Include “how”, “where” and “what”, as appropriate.
    - The worksheet entry should end with a hazard realized, for example, fire, explosion, toxic release, reactivity incident, etc.

- Consequences
    - Ensure consequences are expressed in a form compatible with the definitions used for the Consequence parameters.
    - Word entries so their correspondence to the table of Consequence parameter levels is clear.
    - Provide sufficient detail to define the type of impact, e.g. employee health effects, public health effects, environmental impacts.
    - Usually, specify the worst-case consequence, i.e. the consequence without the benefit of any safeguards.
    - Address conditional modifiers, as required. For example, the probabilities that released flammable / explosive material will find an ignition source, people will be present to be exposed to hazards, and harm will occur if exposure takes place. These modifiers may be recorded in the Enablers column since they are a particular type of enabler.
    - Consider conditional modifiers carefully. During some modes of operation, such as startup, operators may always be present. Furthermore, during the development of a hazardous event more people may be present investigating the problem. Such issues must be considered when using modifiers.

- Safeguards
    - Identify controls that prevent or reduce the likelihood of scenario causes, detect scenario causes or consequences, or mitigate scenario consequences.
    - Specify “what”, and “where” if it is not obvious.
    - Clearly identify safeguards using tag numbers and names, or other identifiers.
    - Include only appropriate safeguards[6]. Consider:
        - Reliability - Will it work?
        - Adequacy - Is it enough?
        - Applicability - Does it really apply? Is it directly applicable?
        - Effective - Does it accomplish its purpose?
        - Functionality - Is it inactive, bypassed, disabled or removed?
    - Word entries so their correspondence to the table of Safeguard parameter levels is clear.

    - Either record only those safeguards credited, or capture all significant safeguards and flag those actually credited, for example, using a “Category” or “Credit” worksheet column (see examples in the next section).

- Enablers:
    - Record enablers in a separate worksheet column to make it clear that they have been considered in the analysis
    - Either record only those enablers credited, or capture all significant enablers and flag those actually credited, for example, using a “Category” or “Credit” worksheet column (see examples in the next section).

- Comments
    - Provide justification for any deviations from standard assignments for Initiators and Safeguards.
    - Explain the basis used for the level assignment of any Initiators or Safeguards that are credited but are not in the standard lists.
    - Justify the assignment of the level for the Enabler parameter.
    - Justify any extra credit taken for enablers, e.g. for time-at-risk factors.
    - Explain any adjustments to the I or S parameters to account for enablers.
    - Justify, as appropriate, the assignment of the level for the Consequence parameter.

    Alternatively, this information can be included with the individual entries in the appropriate worksheet columns.

Parameter levels have been defined so that as the level increases, the frequency, probability, or consequence increases. This was done for consistency with the standard risk graph approach, which does the same for its parameters, and because it meets typical expectations. However, this approach does introduce an inconsistency with IEC 61508/61511 SILs for which the PFD *decreases* as the SIL increases. If this convention causes any difficulties in using standard lookup tables, parameter levels can be redefined by reversing their order.

Examples for the Improved Risk Graph Method

Scenario 1

A low-pressure hazard scenario involves the exposure of operators to a toxic gas released from a stuck-open relief valve. The scenario Initiator parameter is assigned a level of I4 (stuck-open relief valve, see Table 4).

Operators are present less than 10% of the time (0.1 probability) so E1 is assigned for the Enablers parameter level. There are toxic gas detectors and alarms that alert the operators to the release. Together with human action they constitute an allowable Category 2 safeguard (see Table 7) resulting in the assignment of S2 for the Safeguards parameter level. The release could result in multiple fatalities so the Consequence parameter level is assigned as C5 (see Table 8).

The required risk reduction is determined by look-up in the risk matrix. For (I4, E1, S2, C5) a SIL 1 SIF or other safeguard is needed (see Figure 3). This analysis can be performed in a PHA worksheet. Figure 4 shows a PHA worksheet with a Comments column containing explanatory details on the risk graph analysis. Figure 5 shows the same worksheet with a Recommendations column. Both the Comments and Recommendations columns can be included in the same worksheet when printing on paper sufficiently wide.

Scenario 2

An operator charges the wrong catalyst to a reactor resulting in a runaway reaction causing a possible overpressure failure of the reactor vessel. The scenario Initiator parameter is assigned a level of I6 (failure to execute a routine procedure performed once or more per week, see Table 5). Several operators are always present in the reactor room so the Enablers parameter level for the presence of operators is assigned as E2, i.e. no credit can be taken. A reactor high pressure alarm alerts operators so they can take action. However, action must be taken immediately to be effective so no credit is taken for this safeguard (see Table 7). There is an automatic quench system and therefore S1 is assigned as the Safeguards parameter level (see Table 7). If the reactor fails, operators may be exposed to a blast wave. Therefore, the Consequence parameter level is assigned as C5.

The required risk reduction is determined by look-up in the risk matrix. For (I6, E2, S1, C5) a SIL 3 SIF or other safeguard is needed (see Figure 6). The analysis is shown in a PHA worksheet (Figure 7).

Theoretical Foundation of the Improved Risk Graph Method

The six levels of initiating cause frequency cover the frequency range of 1 to 1 x 10^{-5} per year: I1 – 1 x 10^{-5}, I2 – 1 x 10^{-4}, I3 – 1 x 10^{-3}, I4 – 1 x 10^{-2}, I5 – 1 x 10^{-1}, and I6 – 1.This covers the range of initiating cause frequencies that practitioners typically consider for process hazard scenarios and provides for maximum discrimination. Some practitioners have concerns about the ability of analysts to identify initiating cause frequencies in the range of 1 x 10^{-3} per year or lower, because those frequencies are difficult to envisage. However, the risk graph method described here removes that decision from the analysts. They must simply look up the level of the parameter in a table according to the type of initiating cause involved in the scenario. Frequencies are built into the table but they are not readily apparent to the analysts.

The assessment of enabler probabilities involves uncertainties and, therefore, users may wish to allow only an order-of-magnitude adjustment to ensure a conservative result. The two levels of the Enablers parameter provide for reductions in scenario risk as follows: E1 – 1 x 10^{-1}, E2 – 1 (i.e. none). In some cases enablers and conditional modifiers may have a greater impact, either individually, for example, when time-at-risk factors such as being in startup mode are considered, or in combination. In such cases, the refinement discussed above in the description of Step 2 can be used.

Processes usually contain many safeguards and they act to reduce the likelihood and possibly the consequences of hazard scenarios. The improved risk graph method allows credit to be taken for up to two allowable safeguards. This is a deliberately conservative approach since not all safeguards fail independently of each other. LOPA or QRA can be used to take more credit for existing safeguards. The three levels of the safeguards parameter provide for reductions in scenario risk as follows: S1 – 1 x 10^{-2}, S2 – 1 x 10^{-1}, S3 – 1 (i.e. none).

Five levels of consequences are used. The additional level over the usual four levels in the standard risk graph method provides for a category of “no adverse impacts”. The other four levels are similar to those used in the standard method.

The improved risk graph method described here can be tailored to meet individual user needs by modifying the number of levels of the parameters, the definitions of the levels, or the ordering of the parameters in the risk graph. Risk graphs are calibrated for tolerable risk by adjusting the SILs required within the risk matrix. The risk graph shown in Figure 2 has been calibrated for a tolerable fatality risk of 1 x 10^{-4} per year per scenario. Other calibrations are possible.

Conclusions

Conventional risk graphs are a simple but subjective and possibly unreliable way of determining SILs. The improved risk graph method is simpler to use and produces more objective results. Advantages of the improved method include:

- It employs the same theoretical foundation as LOPA and QRA.
- Four parameters are used as for the standard risk graph approach.
- Specific but simple criteria are provided to assist analysts in assigning parameter values. The criteria can be easily adjusted according to the needs and circumstances of the user.
- More than two levels are used for three out of the four parameters employed making it easier for analysts to make assignments of levels. The Enablers parameter has two levels but analysts choose between taking no credit or modest credit for enablers. They do not face a choice between the two extremes of a range. They also have the option of taking more credit, and thus effectively adding levels, by using a simple refinement of the method.

- Subjectivity in deciding on the levels of the parameters to assign for a hazard scenario is minimized thus helping to avoid disagreements among the analysts and producing more consistent results. Subjectivity may be present in the level definitions but that does not affect assignments by the analysts.
- The analysis can be incorporated easily into PHA worksheets but it avoids the need for numerical manipulations by PHA teams. Such manipulations are often viewed by team members as beyond the scope of PHA, and they cause frustration. Users are shielded from numerical frequencies, PFDs, and risk tolerance criteria.
- The flow of a hazard scenario is followed. This facilitates the analysis when it is performed as part of PHA.
- The method can be used to screen hazard scenarios for more detailed analysis using LOPA or QRA methods and it is structured to allow a seamless transition to LOPA and QRA.
- A sound theoretical foundation is used but the method avoids the need for analysts necessarily to understand the underlying theory.

Note

The figures used to illustrate the incorporation of risk graphs into PHA are screen captures from PHAWorks®, Primatech's PHA software package. PHAWorks® templates for both the standard and improved risk graphs methods are available at no cost to PHAWorks® licensees from Primatech at software@primatech.com.

References

1. W. M. Goble and H. Cheddie, Safety Instrumented Systems Verification, ISA, 2005.

2. IEC 61508, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, 1998.

3. IEC 61511, Functional Safety - Safety Instrumented Systems for the Process Industry Sector, 2003.

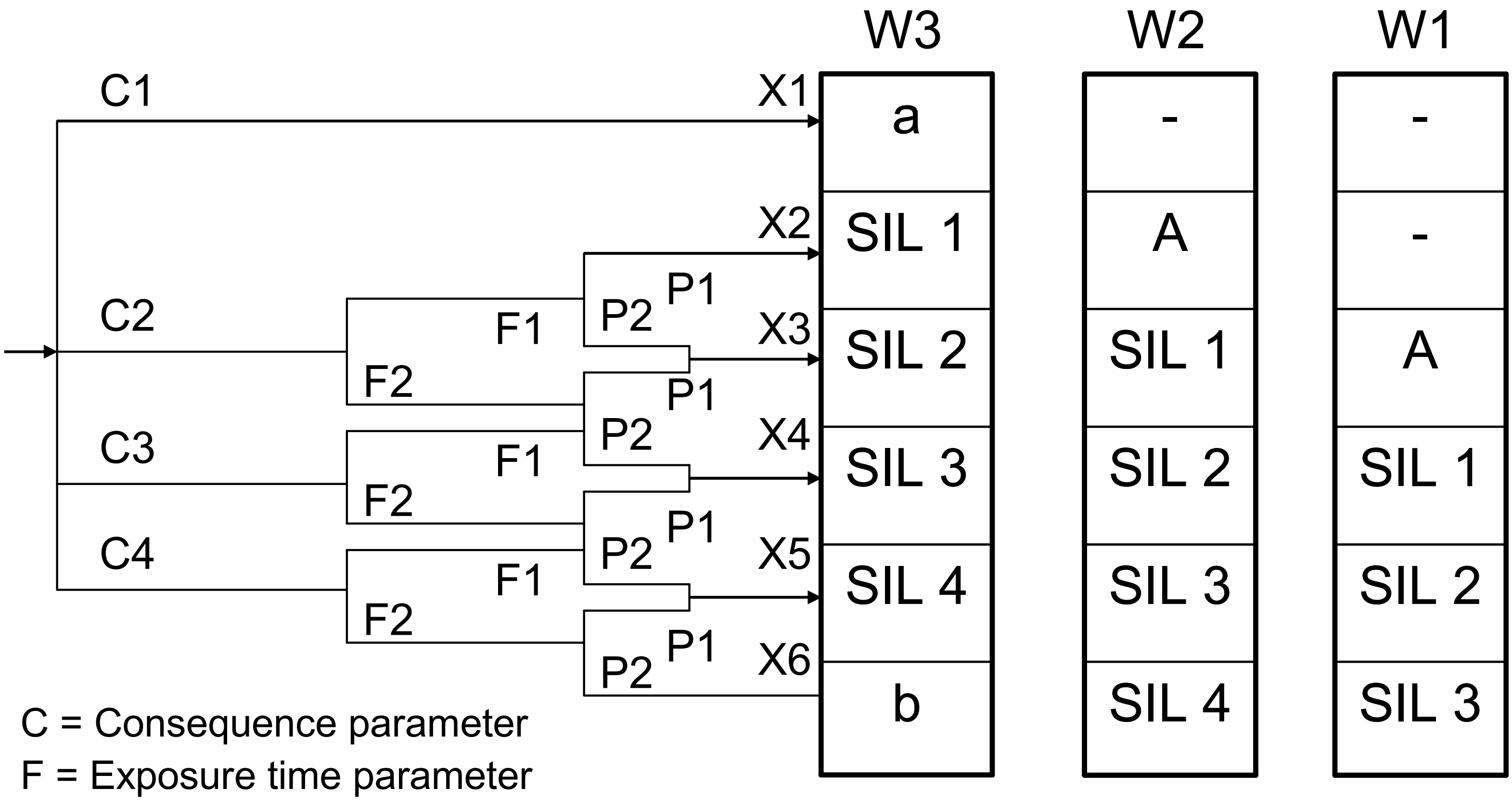
4. ANSI/ISA S84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector.

5. DIN V 19250, 1994, Control Technology: Fundamental Safety Aspects to be Considered for Measurement and Control Equipment.

6. Layer of Protection Analysis, Simplified Process Risk Assessment, AIChE/CCPS, New York, NY, 2001.

7. E. Marzal and E. Scharpf, Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis, ISA, 2002.

Figure 1. Example of Risk Graph Modeled on IEC 61511.



	W3	W2	W1
X1	a	-	-
X2	SIL 1	A	-
X3	SIL 2	SIL 1	A
X4	SIL 3	SIL 2	SIL 1
X5	SIL 4	SIL 3	SIL 2
X6	b	SIL 4	SIL 3

C = Consequence parameter

F = Exposure time parameter

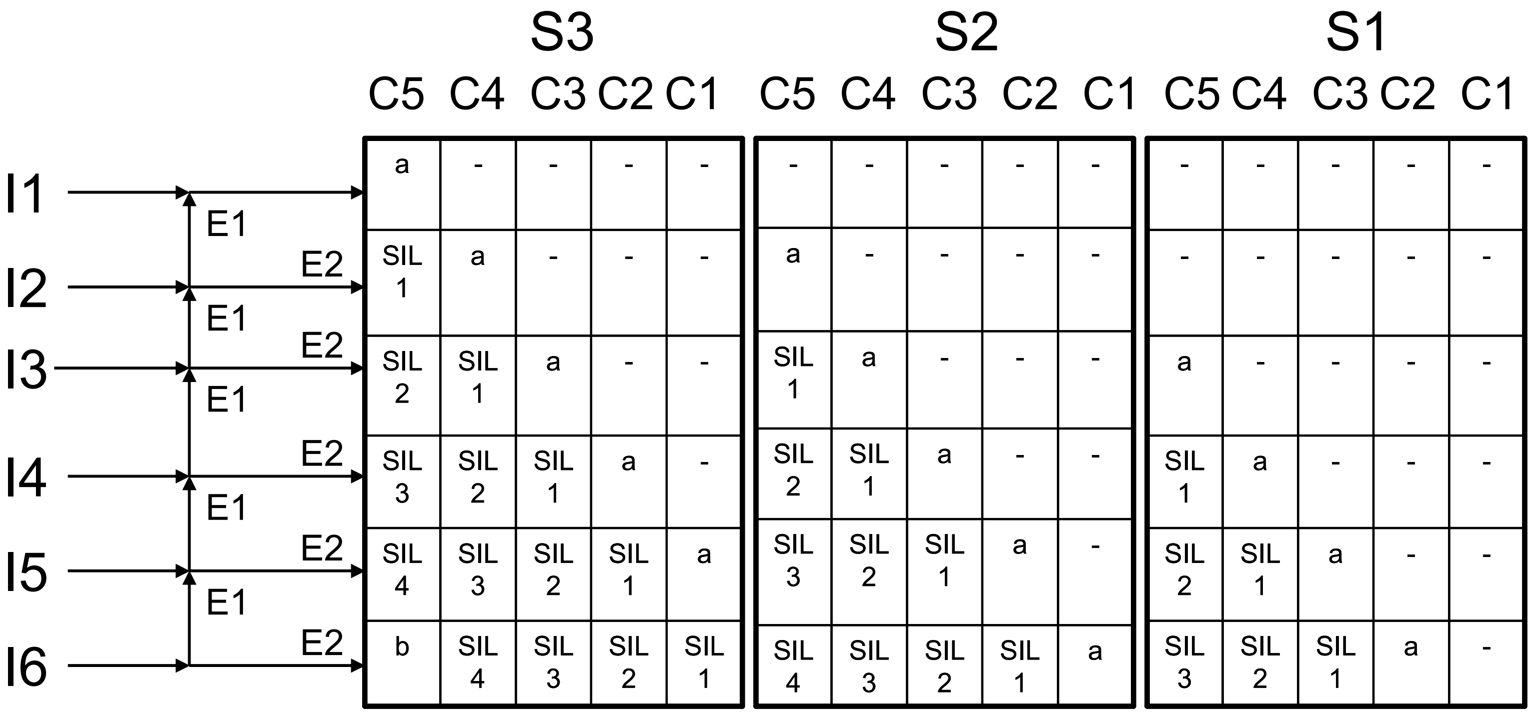
P = Probability of avoiding the hazardous event

W = Probability of the failure/occurrence (without SIS in place)

X = Frequency/probability-adjusted consequence

-	No safety requirement
a	No special safety requirements
b	A single SIF is not sufficient

Figure 2. Improved Risk Graph.



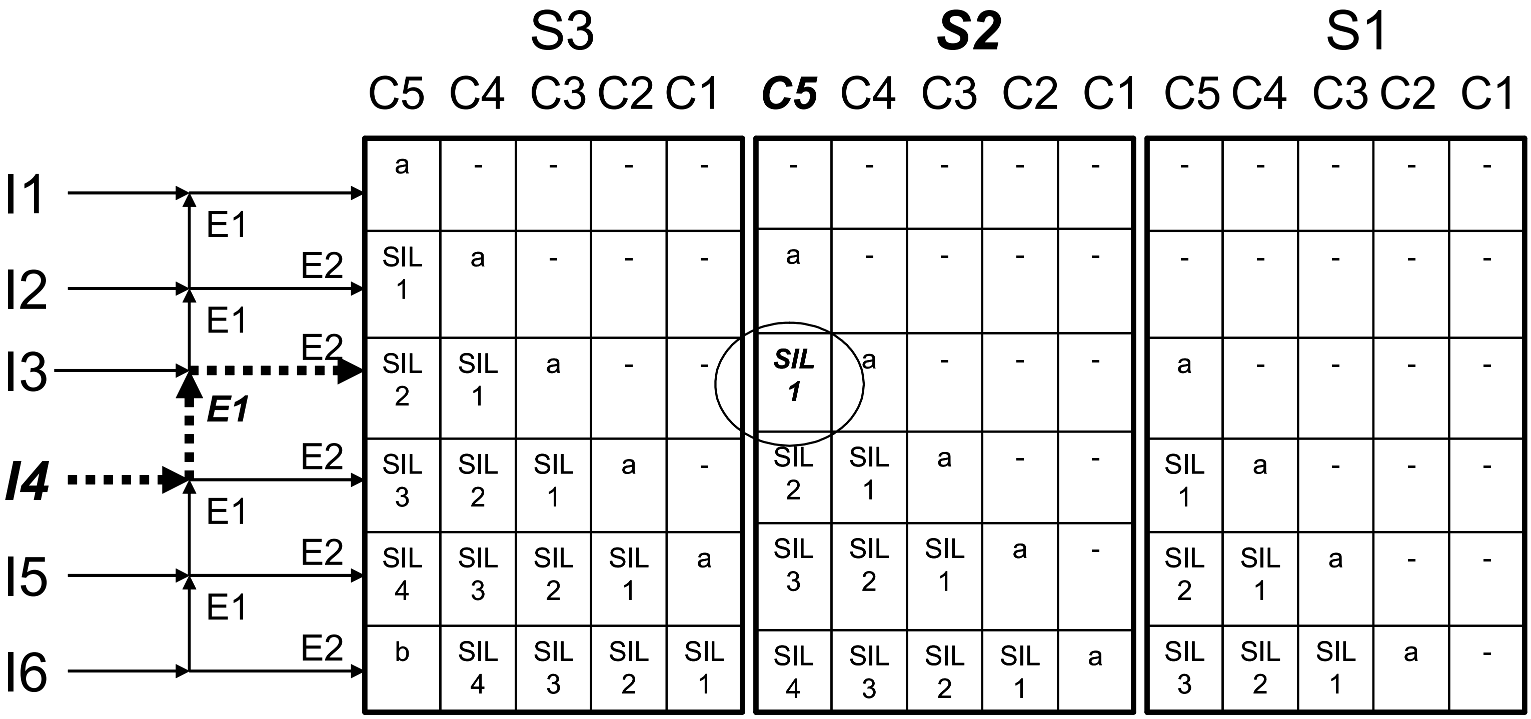
	S3					S2					S1				
	C5	C4	C3	C2	C1	C5	C4	C3	C2	C1	C5	C4	C3	C2	C1
I1	a	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I2	SIL 1	a	-	-	-	a	-	-	-	-	-	-	-	-	-
I3	SIL 2	SIL 1	a	-	-	SIL 1	a	-	-	-	a	-	-	-	-
I4	SIL 3	SIL 2	SIL 1	a	-	SIL 2	SIL 1	a	-	-	SIL 1	a	-	-	-
I5	SIL 4	SIL 3	SIL 2	SIL 1	a	SIL 3	SIL 2	SIL 1	a	-	SIL 2	SIL 1	a	-	-
I6	b	SIL 4	SIL 3	SIL 2	SIL 1	SIL 4	SIL 3	SIL 2	SIL 1	a	SIL 3	SIL 2	SIL 1	a	-

I = Initiators (see Table 4 - 6)
E = Enablers (see Step 2)
S = Safeguards (see Table 7)
C = Consequences (see Table 8)

Note: E1 branches upwards and over; E2 branches horizontally.

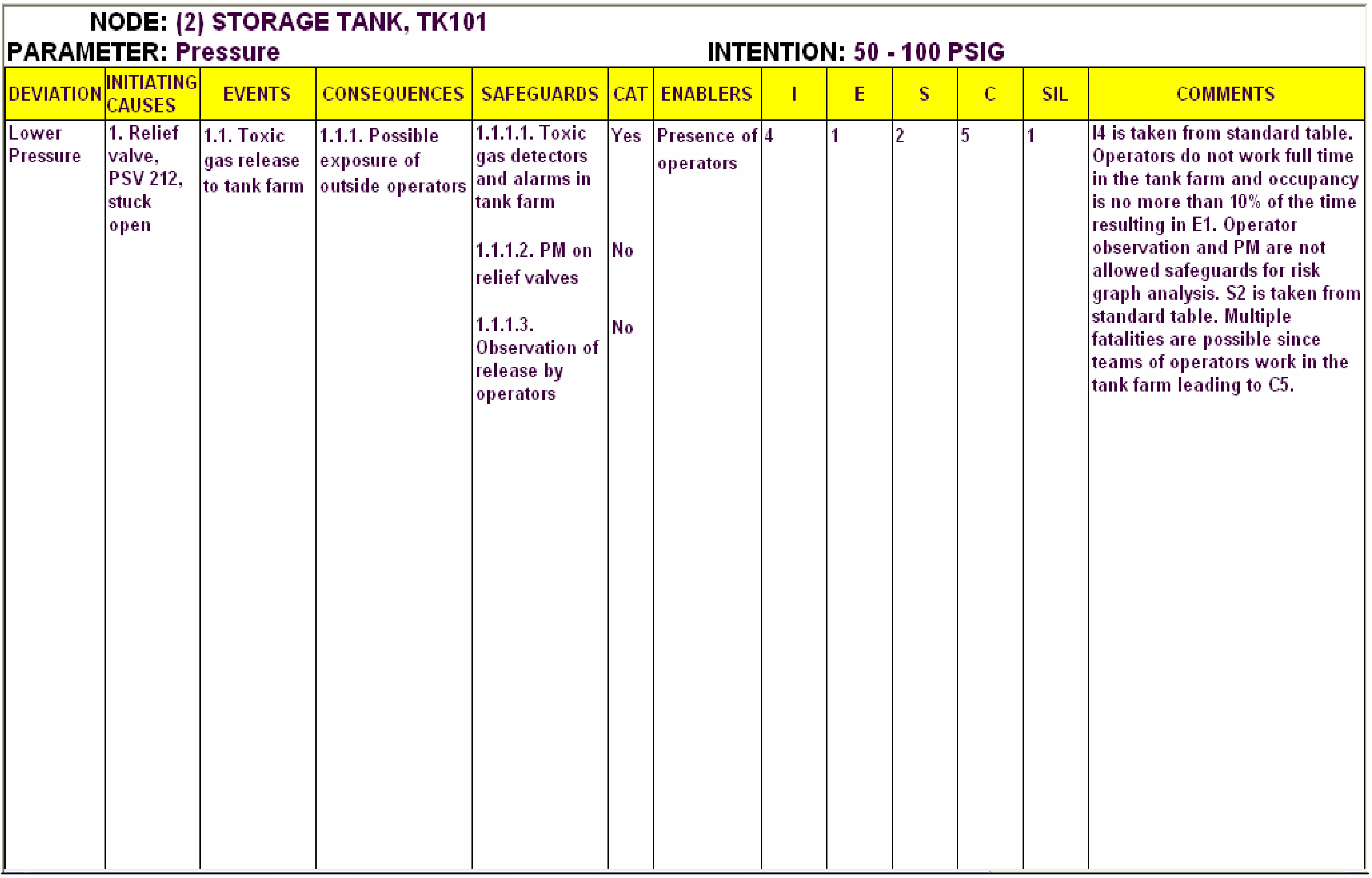
-	No safety requirement
a	No special safety requirements
b	A single SIF is not sufficient

Figure 3. Improved Risk Graph With Example 1 SIL Determination



S3					***S2***					S1				
C5	C4	C3	C2	C1	***C5***	C4	C3	C2	C1	C5	C4	C3	C2	C1
a	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SIL 1	a	-	-	-	a	-	-	-	-	-	-	-	-	-
SIL 2	SIL 1	a	-	-	***SIL 1***	a	-	-	-	a	-	-	-	-
SIL 3	SIL 2	SIL 1	a	-	SIL 2	SIL 1	a	-	-	SIL 1	a	-	-	-
SIL 4	SIL 3	SIL 2	SIL 1	a	SIL 3	SIL 2	SIL 1	a	-	SIL 2	SIL 1	a	-	-
b	SIL 4	SIL 3	SIL 2	SIL 1	SIL 4	SIL 3	SIL 2	SIL 1	a	SIL 3	SIL 2	SIL 1	a	-

Figure 4. Example 1 PHA Worksheet Containing Improved Risk Graph Analysis With Explanatory Details.

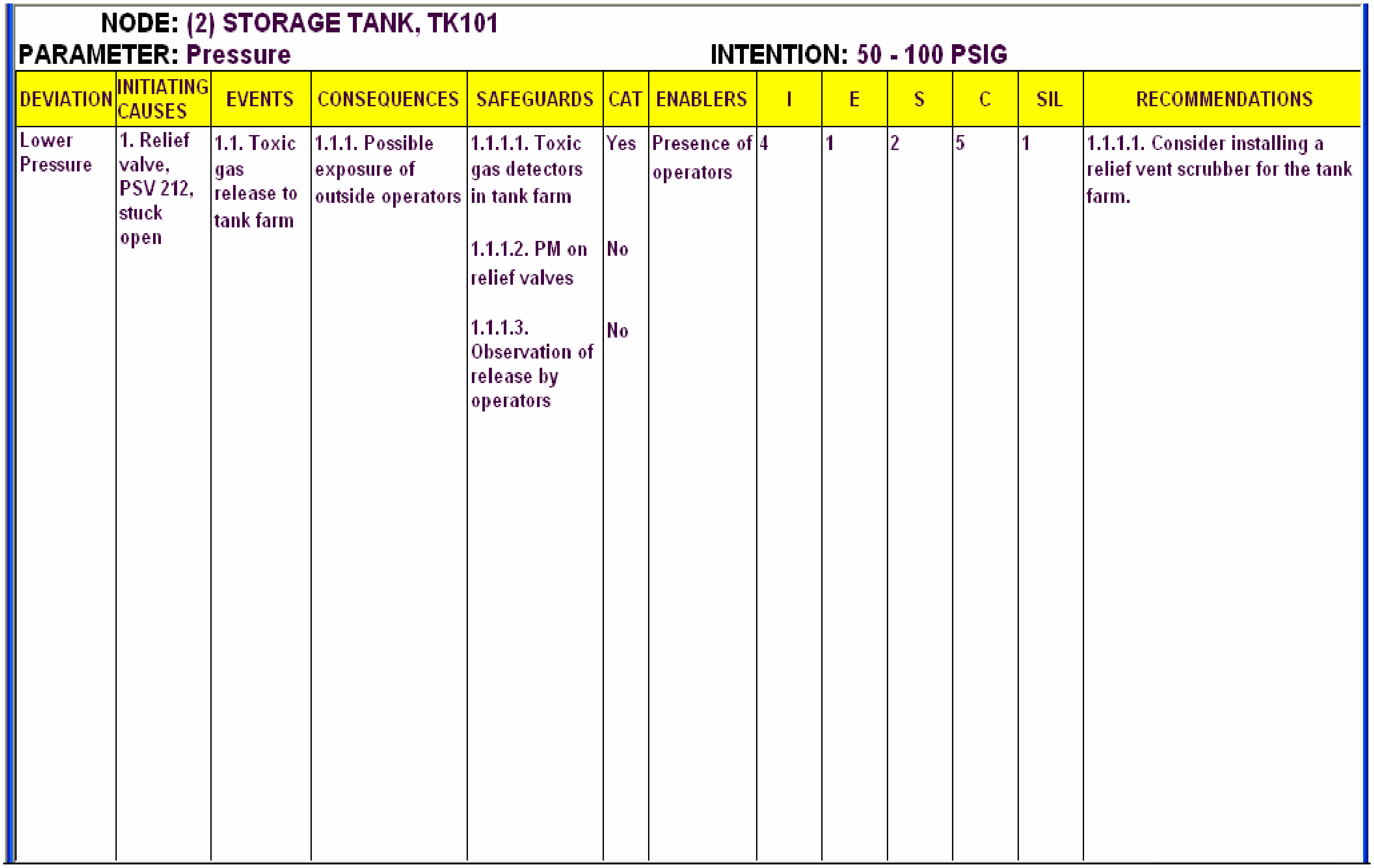


NODE: (2) STORAGE TANK, TK101

PARAMETER: Pressure INTENTION: 50 - 100 PSIG

DEVIATION	INITIATING CAUSES	EVENTS	CONSEQUENCES	SAFEGUARDS	CAT	ENABLERS	I	E	S	C	SIL	COMMENTS
Lower Pressure	1. Relief valve, PSV 212, stuck open	1.1. Toxic gas release to tank farm	1.1.1. Possible exposure of outside operators	1.1.1.1. Toxic gas detectors and alarms in tank farm	Yes	Presence of operators	4	1	2	5	1	I4 is taken from standard table. Operators do not work full time in the tank farm and occupancy is no more than 10% of the time resulting in E1. Operator observation and PM are not allowed safeguards for risk graph analysis. S2 is taken from standard table. Multiple fatalities are possible since teams of operators work in the tank farm leading to C5.
				1.1.1.2. PM on relief valves	No							
				1.1.1.3. Observation of release by operators	No							

Figure 5. Example 1 PHA Worksheet Containing Improved Risk Graph Analysis With Recommendations.



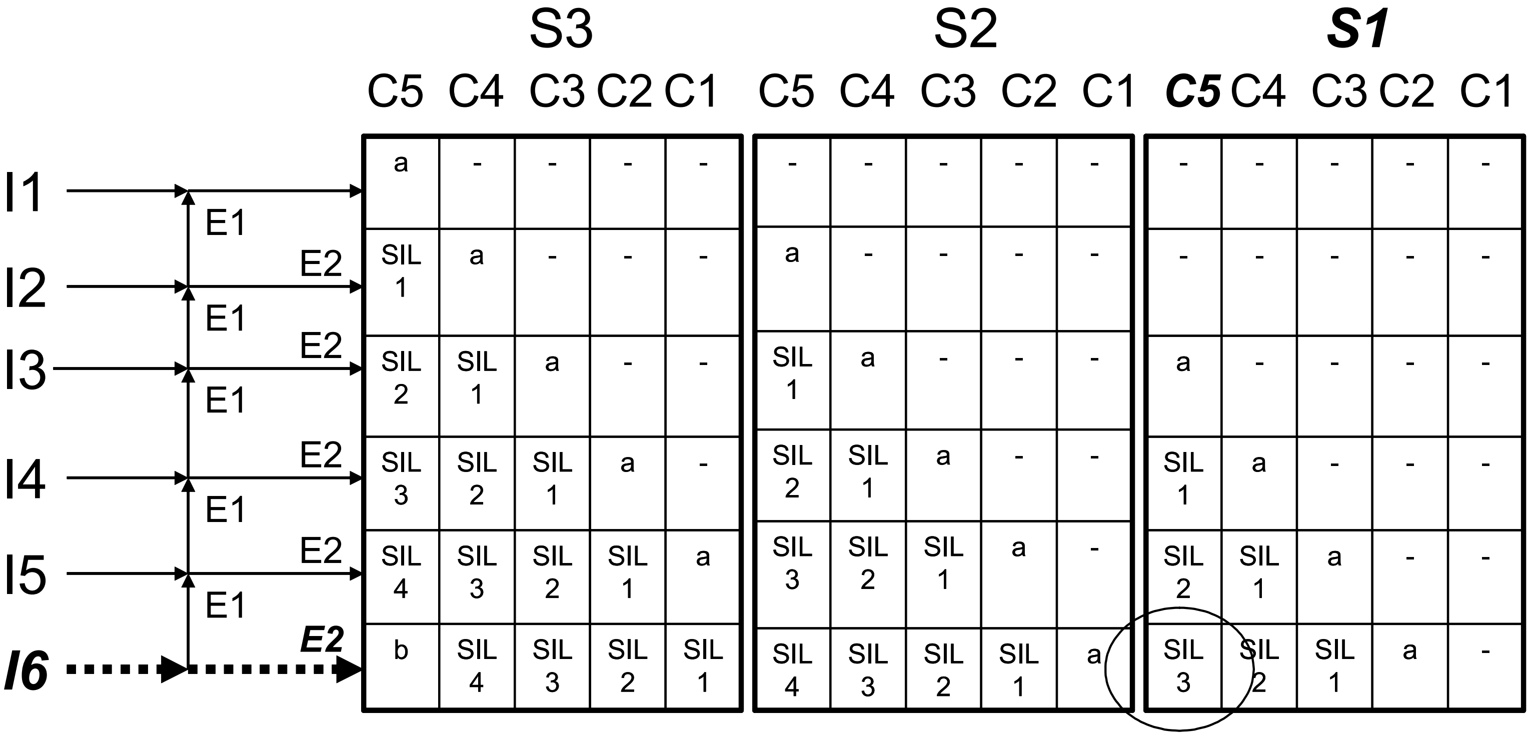
NODE: (2) STORAGE TANK, TK101

PARAMETER: Pressure

INTENTION: 50 - 100 PSIG

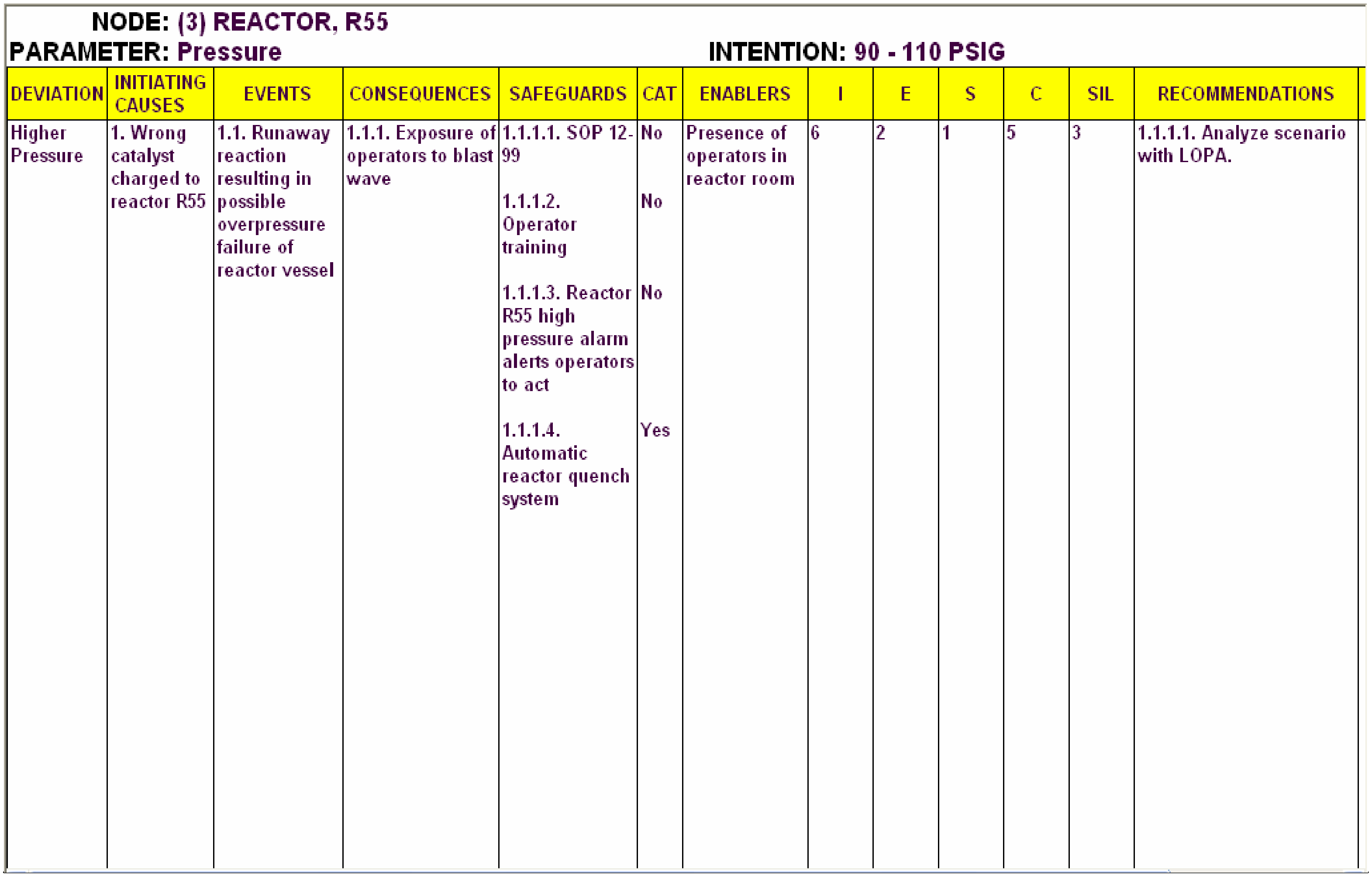
DEVIATION	INITIATING CAUSES	EVENTS	CONSEQUENCES	SAFEGUARDS	CAT	ENABLERS	I	E	S	C	SIL	RECOMMENDATIONS
Lower Pressure	1. Relief valve, PSV 212, stuck open	1.1. Toxic gas release to tank farm	1.1.1. Possible exposure of outside operators	1.1.1.1. Toxic gas detectors in tank farm	Yes	Presence of operators	4	1	2	5	1	1.1.1.1. Consider installing a relief vent scrubber for the tank farm.
				1.1.1.2. PM on relief valves	No							
				1.1.1.3. Observation of release by operators	No							

Figure 6. Improved Risk Graph With Example 2 SIL Determination



	S3					S2					***S1***				
	C5	C4	C3	C2	C1	C5	C4	C3	C2	C1	***C5***	C4	C3	C2	C1
I1	a	-	-	-	-	-	-	-	-	-	-	-	-	-	-
I2	SIL 1	a	-	-	-	a	-	-	-	-	-	-	-	-	-
I3	SIL 2	SIL 1	a	-	-	SIL 1	a	-	-	-	a	-	-	-	-
I4	SIL 3	SIL 2	SIL 1	a	-	SIL 2	SIL 1	a	-	-	SIL 1	a	-	-	-
I5	SIL 4	SIL 3	SIL 2	SIL 1	a	SIL 3	SIL 2	SIL 1	a	-	SIL 2	SIL 1	a	-	-
I6	b	SIL 4	SIL 3	SIL 2	SIL 1	SIL 4	SIL 3	SIL 2	SIL 1	a	SIL 3	SIL 2	SIL 1	a	-

Figure 7. Example 2 PHA Worksheet Containing Improved Risk Graph Analysis With Recommendations.



NODE: (3) REACTOR, R55

PARAMETER: Pressure INTENTION: 90 - 110 PSIG

DEVIATION	INITIATING CAUSES	EVENTS	CONSEQUENCES	SAFEGUARDS	CAT	ENABLERS	I	E	S	C	SIL	RECOMMENDATIONS
Higher Pressure	1. Wrong catalyst charged to reactor R55	1.1. Runaway reaction resulting in possible overpressure failure of reactor vessel	1.1.1. Exposure of operators to blast wave	1.1.1.1. SOP 12-99	No	Presence of operators in reactor room	6	2	1	5	3	1.1.1.1. Analyze scenario with LOPA.
				1.1.1.2. Operator training	No							
				1.1.1.3. Reactor R55 high pressure alarm alerts operators to act	No							
				1.1.1.4. Automatic reactor quench system	Yes							

Table 1. Key Terms

BPCS -	Basic Process Control System	
FDF	-	Frequency of Dangerous Failures
LOPA	-	Layers of Protection Analysis
PFD	-	Probability of Failure on Demand
PHA	-	Process Hazard Analysis
QRA	-	Quantitative Risk Analysis
SIF	-	Safety Instrumented Function
SIL	-	Safety Integrity Level
SIS	-	Safety Instrumented System

Table 2. Standard Risk Graph Parameters

C - Consequence of the hazardous event

F - Frequency of presence in the hazardous zone and the potential exposure time, or Occupancy

P - Probability of avoiding the hazardous event

W - Probability of the unwanted occurrence

Table 3. Improved Risk Graph Parameters

I (Initiators) - Initiating cause frequency

E (Enablers) - Enabling events/conditions and other modifiers

S (Safeguards) - Safeguard failure probability

C (Consequences) - Consequences of the hazardous event or scenario

Table 4. Example of Initiating Cause Levels for Equipment Failures.

Equipment Type	Level
Atmospheric tank failure	I2
Piping breach	I2
Piping leak	I3
Pressure vessel failure	I1
Pump seal failure	I5
Regulator failure	I6
Safety valve opens spuriously	I4
Unloading / loading hose failure	I6

Table 5. Example of Initiating Cause Levels for Human Failures.

Human Failure	Level
Failure to execute a routine procedure performed*:	
Once per year	I4
Once or more per month	I5
Once or more per week	I6
Failure to follow a safe work practice performed*:	
Once per year	I3
Once or more per month	I4
Once or more per week	I5

* Assuming trained, unstressed, and not fatigued.

Table 6. Example of Initiating Cause Levels for External Events

.

External Event	Level
Cooling water failure	I6
External fire (small)	I5
External fire (large)	I4
Lightning strike	I3
Third-party intervention (external impact by backhoe, vehicle, etc.)	I4

Table 7. Example of Allowable Safeguards.

Category 1	Category 2
Automated dump or quench system	Flame / detonation arrestors
Blast wall / bunker	Human response to BPCS indication or alarm within 40 minutes
Dike	Relief valve
Fireproofing	Rupture disk

Table 8. Example of Consequence Parameter Definitions.

Category	Definition		
	Personnel Safety	Environmental Impact	Business Impact
C1	No adverse impact	No adverse impact	No adverse impact
C2	Lost-time	Release to water or land resulting in a temporary impact which is self-correcting	< 1 week shutdown
C3	Severe injuries	Release to water or land requiring remediation that can be performed quickly at reasonable cost	1 week to 1 month shutdown
C4	Single fatality	Release to water or land requiring remediation that takes an extended time period and significant cost	1 - 6 month shutdown
C5	Multiple fatalities	Release to water or land that results in significant long-lasting impacts that cannot be remediated	> 6 month shutdown