TECHNICAL PAPER

UNWIN
Integrated Risk Management

1920 Northwest Blvd., Suite 201
Columbus, OH 43212-1197 USA
614.486.2245 irm@unwin-co.com

Presented at the
ISA Safety Symposium
April 24, 2008, Calgary, Alberta

Robert W. Johnson

Interfacing HAZOP Studies with SIL Determinations using Exponential Frequency and Severity Categories

Abstract

Orders of magnitude can greatly simplify the mathematics of risk calculations. This concept has found use in combining cause frequencies, protective layer probabilities, and consequence severities quickly and easily in team-based process hazard analyses. The ability to develop hazard scenarios and estimate each scenario's risk parameters at the same time allows review teams to specify safety integrity layer (SIL) requirements in the same fashion as a stand-alone layer of protection analysis study. The order-of-magnitude approach to documenting risk parameters during a PHA is explained and illustrated, and its extension to determining SILs to meet risk targets is shown.

Introduction

Risk calculations span vast ranges. Initiating event frequencies can range from daily occurrences to rare events with likelihoods in the tens of thousands of years. Impacts can range from a minor injury to multiple fatalities and many millions of dollars of losses. *Risk*, taken as the conventional combination of likelihood and severity of loss events, can extend over an even greater range when these factors and their wide spans are combined.

Orders of magnitude help us grasp vast ranges such as those used in risk calculations. The Richter scale conveys in simple numerical terms the amplitude of signals recorded by a seismograph. A magnitude 7 earthquake is likely to make international news, whereas a magnitude 4 earthquake may make only local news.

The pH scale used to measure acidity is an inverse logarithmic measure of the effective hydrogen ion (H^+) concentration in an aqueous solution. Knowing that the pH of cola is around 2.5 is much easier to express (and remember) than knowing that its hydrogen ion concentration is 0.003 gram-moles per liter. Not only are many things easier to express in logarithmic terms, the breadth of differences are easier to grasp. The difference in pH between cola (2.5) and household ammonia

(11.5) spans a hydrogen ion concentration range of nine orders of magnitude, or a factor of one billion. Likewise, it is easier to express that there are 11 orders of magnitude between a brisk snail's pace (3 mm/s) and the speed of light (300,000 km/s) than that the difference in their velocities is 100,000,000,000-fold.

Orders of magnitude are also useful in simplifying mathematics. Adding and subtracting exponents is much preferable to multiplying and dividing very large or very small numbers. This concept has found use in combining initiating cause frequencies, safeguard risk reduction factors and consequence severities quickly and easily in process hazard analyses (PHAs). The ability to concurrently develop hazard scenarios and estimate their risk parameters allows PHA review teams to specify safety integrity layer (SIL) requirements in the same manner as a stand-alone layer of protection analysis (LOPA) study. This order-of-magnitude approach to documenting risk parameters during a PHA is explained and illustrated, including its extension to determining SILs to meet risk targets.

Exponential Risk Calculations

Risk can be defined as the combination of the likelihood (expressed as a frequency) and severity (expressed as the total impact) of loss events.[1] This paper focuses on process industry loss events, with a *loss event* defined as the point in time in an abnormal situation when an irreversible physical event occurs that has the potential for loss and harm impacts. Examples include release of a hazardous material, ignition of flammable vapors or ignitable dust cloud, and overpressurization rupture of a tank or vessel.

For risk calculations, the frequency and severity of a loss event are generally combined by direct multiplication:

Scenario Frequency x ***Scenario Impact*** = ***Scenario Risk***

(loss events / year) x (impact / loss event) = (impact / year)

For example, if the scenario under consideration is a "hundred-year flood" that can affect an industrial facility and cause total monetary losses on the order of $10 million, the scenario risk is

(0.01 flood per year) x ($10,000,000 per flood) = $100,000 per year.

This $100,000 per year can be thought of as an annualized loss rate. Risk of process incidents can also be expressed in injuries or fatalities per year, or defined environmental impacts per year.

The same order-of-magnitude calculations can be performed by adding exponents rather than multiplying the frequency and impact factors, which tend to be either very large or very small numbers (Johnson, 1998). For the hundred-year flood example, if the 0.01 flood per year ($= 10^{-2}$/year) frequency is represented by a frequency magnitude of **-2** and the $10,000,000 per flood ($= \$10^{7}$/flood) impact is represented by the impact magnitude of 7, then a risk magnitude of **5** corresponding to the risk of $\$10^{5}$/year can be easily calculated.

[1] See Appendix for a glossary of terms used in this paper.

$$(10^{-2}/\text{year}) \times (\$10^{7}/\text{flood}) = \$10^{5}/\text{year}$$

$$\mathbf{-2 + 7 = 5}$$

Severity Magnitudes

For the severity side of the risk equation, Table 1 illustrates one example of a loss event severity scale arranged with roughly an order of magnitude severity increase from one column to the next.

.Table 1. Example of EHS impact categories and magnitudes used in hazard evaluations (CCPS 2008)

	Impact magnitude				
Impact category	**1**	**2**	**3**	**4**	**5**
On-site (worker) health effects	Recordable injury	Lost-time injury	Multiple or severe injuries	Permanent health effects	Fatalities
Off-site (public) effects	Odor; exposure below limits	Exposure above limits	Injury	Hospitalization or multiple injuries	Severe injuries or permanent effects
Environmental impacts	Reportable release	Localized and short-term effects	Intermediate effects	Widespread or long-term effects	Widespread and long-term effects
Accountability; attention/ concern / response	Plant	Division; regulators	Corporate; neighborhood	Local/state	State/national

Another example of a loss event severity scale using order-of-magnitude categories is the Process Safety Incident Severity scale in CCPS (2007) as it pertains to fire or explosion process safety incidents (including overpressure):

Severity Level **4**: Incident resulting in $25,000 to $100,000 of direct costs

Severity Level **3**: Incident resulting in $100,000 to $1MM of direct costs

Severity Level **2**: Incident resulting in $1MM to $10MM of direct costs

Severity Level **1**: Incident resulting in > $10MM of direct costs

In this scale, the severity level number cannot be used directly as the surrogate for the impact magnitude.

Likelihood Magnitudes

For incidents in the process industries, the likelihood side of the risk equation is expressed as the frequency of occurrence of a specific loss event such as a fire, explosion or hazardous material release. For rare events, this can also be understood as the probability per year of operation that the loss event will occur. A frequency magnitude scale is shown in Table 2 that expresses order-of-magnitude steps with their corresponding exponents highlighted in bold.

Table 2. Example order-of-magnitude initiating cause frequency scale (CCPS 2008)

Magnitude 10^{x}/yr	Equivalent cause likelihood	Comparison with experience
0	Once a year	Unpredictable as to when it will occur, but within realm of most employees' experience
-1	1 in 10 (10% likelihood) per yr of operation	Outside of some employees' experience; within realm of process' experience
-2	1 in 100 (1% likelihood) per yr of operation	Outside of almost all employees' experience; within realm of plant-wide experience
-3	1 in 1,000 per yr of operation	Outside of almost all process experience; may be within realm of company-wide experience
-4	1 in 10,000 per yr of operation	Outside of most companies' experience; within realm of industry-wide experience
-5	1 in 100,000 per yr of operation	May be outside the realm of industry-wide experience, except for common types of facilities and operations

This scale is not all-inclusive; frequencies can also be higher (e.g., ten times a year) or lower (e.g., once in a million years). However, this scale covers the range of frequencies that is used most often to express the likelihood of significant loss events for a given process operation.

Safety Integrity Levels

Hazard analysis methodologies such as Hazard and Operability Studies and Fault Tree Analyses can be used to break down the likelihood of loss events into more manageable and easily estimated components. The two basic components are the initiating cause frequency and the safeguards risk reduction factor:

Scenario Frequency x *Scenario Impact* = *Scenario Risk*

(loss events/year) x (impact/loss event) = (impact/year)

[Initiating Cause Frequency / ***Safeguards Risk Reduction Factor]*** x *Scenario Impact* = *Scenario Risk*

[(initiating events/year) / (dimensionless factor)] x (impact/loss event) = (impact/year)

The *initiating cause* is the operational error, mechanical failure, or external event or agency that is the first event in an incident sequence, marking the transition from a normal to an abnormal situation.

Safeguards are devices, systems and actions that would likely interrupt the chain of events following an initiating cause or that would mitigate loss event impacts. Examples include operator response to an alarm, safety instrumented systems, emergency relief systems, and post-release mitigation systems. If no safeguards are employed, then the overall scenario frequency is equal to the initiating cause frequency.

The above risk equation, adding and subtracting magnitudes instead of multiplying and dividing the factors, can be expressed as:

Initiating Cause Magnitude - Safeguards Risk Reduction Magnitude
+ Scenario Impact Magnitude = Scenario Risk Magnitude

Using the previous example, if the facility that can be affected by a "hundred-year flood" is protected by a barrier that has a risk reduction factor of 100 or 10^2 (safeguard risk reduction magnitude of **2**), the overall scenario risk magnitude for the scenario of a $\$10^7$ flood loss impact is reduced from **5** to **3** (= -2 - 2 + 7). The risk reduction factor of 100 means that out of 100 flood events, only one would result in the major loss, thus giving an overall scenario frequency of 10^{-4} loss events/year or one chance in 10,000 per year that the $\$10^7$ loss would be realized.

The effectiveness of a safety instrumented system in bringing an abnormal operation to a safe state is expressed in terms of safety integrity levels (SILs), as expressed in Table 3 for demand mode of operation. Since SILs are defined in order-of-magnitude categories, these categories are compatible with the initiating cause frequency and impact severity magnitudes already defined. Industry has commonly used the SIL to be equivalent to the risk reduction magnitude by conservatively using the lower bound of the target risk reduction range.

Table 3. Safety Integrity Levels: Probability of failure on demand (ANSI/ISA, 2004)

Demand mode of operation		
Safety Integrity Level	Target average probability of failure on demand	Target risk reduction
SIL 3	≥ 0.0001 to < 0.001	> 1000 to ≤ 10,000
SIL 2	≥ 0.001 to < 0.01	> 100 to ≤ 1000
SIL 1	≥ 0.01 to < 0.1	> 10 to ≤ 100

SIL Determinations in Process Hazard Analyses

Considering SIL values to be risk reduction magnitudes allows SIL values to be specified at the same time scenario-based hazard evaluation procedures are used to evaluate the adequacy of existing safeguards. If the SIL is already specified for a given safety instrumented function, the SIL can be used directly as the safeguard risk reduction magnitude.

Table 4 is an excerpt from a Hazard and Operability (HAZOP) Study, with columns added for documenting initiating cause frequency, loss event impact and scenario risk magnitudes. The four example scenarios in this Table will be used to illustrate how SIL levels can be determined by analyzing HAZOP scenarios on an order-of-magnitude basis.

Table 4. Example HAZOP Study table with frequency, impact, safeguard and risk magnitudes (adapted from CCPS 2008, Table 15.7)

Deviation	Initiating Cause	Fre-- quency	Consequences	Impact	Safeguards	Scenario Risk
No Flow – ethylene	FCV-1 fails closed or commanded to close	**-1**	Unreacted chlorine to furnace; possible failure of furnace tubes from chlorine contact damage; hot chlorine vapor release from furnace	4	[1] Alarm, shutdown on PT-1 low pressure [2] Detection of loss of ethylene flow by 2/h reactor sampling before furnace tube(s) fail	0
			Unreacted chlorine through furnace and incinerator to plant scrubber; eventual chlorine breakthrough; chlorine release from scrubber stack	3	[1] Alarm, shutdown on PT-1 low pressure [1] Detection of loss of ethylene flow by 2/h reactor sampling before chlorine release [0] Scrubber breakthrough alarm (not an additional independent layer of protection)	0
No Flow – ethylene	PCV-1 fails closed or commanded to close	**-1**	Unreacted chlorine to furnace; possible failure of furnace tubes from chlorine contact damage; hot chlorine vapor release from furnace	4	[2] Detection of loss of ethylene flow by 2/h reactor sampling before furnace tube(s) fail	+1
			Unreacted chlorine through furnace and incinerator to plant scrubber; eventual chlorine breakthrough; chlorine release from scrubber stack	3	[1] Detection of loss of ethylene flow by 2/h reactor sampling before chlorine release [1] Scrubber breakthrough alarm	0

In this example, the numbers in square brackets in the Safeguards column correspond to the risk reduction magnitudes assigned to each independent preventive safeguard. For example, the first safeguard of "Alarm, shutdown on PT-1 low pressure" has a risk reduction magnitude of **1**, indicating that if ethylene flow is lost, there is a 10-fold ($10^{\mathbf{1}}$) risk reduction factor (i.e., on the order of nine times out of ten) that loss of pressure will be detected, the operator will be alerted, and the system will be brought to a safe state before the consequences of concern are realized.

As long as multiple preventive safeguards (layers of protection) are truly independent, the risk reduction magnitudes associated with each safeguard can be added. For the first scenario, the risk reduction of factor of **1** for "Alarm, shutdown on PT-1 low pressure" added to the risk reduction factor of **2** for "Detection of loss of ethylene flow by 2/h reactor sampling before furnace tube(s) fail" gives a total risk reduction factor of 3.

In the example of Table 4, a single risk magnitude number is used. This scenario risk magnitude is easily calculated as the initiating cause frequency magnitude reduced by the sum of the safeguard risk reduction factors and added to the impact magnitude.

The scenario risk magnitude can be compared to a facility's tolerable risk criteria to determine whether the corresponding risk criterion is met for each scenario. Alternatively, a risk matrix can be used to express the tolerable risk boundary, with the overall scenario frequency on one axis and the scenario impact on the other axis.

If the facility's tolerable risk criterion for the example of Table 4 is that any scenario risk magnitude greater than **0** must be reduced, then only one of the four scenarios in Table 4 would require further risk reduction. The difference between the risk magnitude for this one scenario of **+1** and the

tolerable risk criterion of **0** is one order of magnitude. Hence, an additional independent safeguard with a risk reduction factor of **1** would satisfy this requirement. If the new safeguard was a safety instrumented system (SIS), SIL 1 would be indicated by this analysis as the SIL to be specified for the new safety instrumented system if this were the only safety instrumented function for the new SIS. Note that the scenario risk criterion could also be met by reducing the initiating cause frequency or the consequence impact, or adding another kind of independent safeguard other than a SIS.

If the facility's tolerable risk criterion for the example of Table 4 is that any scenario risk magnitude greater than **-2** must be reduced, then all four scenarios in Table 4 would require further risk reduction. The difference between the risk magnitude for this one scenario of **+1** and the tolerable risk criterion of **-2** is three orders of magnitude, thus requiring a SIL 3 system to be specified or other combinations of instrumented and non-instrumented frequency and/or severity reduction measures to be implemented that would add up to at least three orders of magnitude.

References

Johnson, R.W., 1998. "Risk Management by Risk Magnitudes," *Chemical Health and Safety 5*(5), September/ October, 9-13.

CCPS, 2008. Center for Chemical Process Safety, *Guidelines for Hazard Evaluation Procedures, Third Edition*, New York: American Institute of Chemical Engineers.

CCPS, 2007. Center for Chemical Process Safety, "Process Safety Leading and Lagging Metrics," American Institute of Chemical Engineers, December 20. Available from www.aiche.org/ccps.

ANSI/ISA-S84.00.01-2004 Part 1 (IEC 61511-1 Mod), "Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1," Table 3.

Appendix

For consistency with industry usage, the following definitions extracted from the Glossary of CCPS (2008) were employed and apply to the terms used in this paper.

Cause**:* In the context of hazard evaluation procedures, an ***initiating cause.

***Consequence**:* Result of a specific event. In the context of qualitative hazard evaluation procedures, the *consequences* are the effects following from the initiating cause, with the consequence description taken through to the loss event and sometimes to the loss event impacts. In the context of quantitative risk analyses, the *consequence* refers to the physical effects of the loss event usually involving a fire, explosion, or release of toxic or corrosive material.

***Deviation**:* A process condition outside of established design limits, safe operating limits, or standard operating procedures.

***Event**:* An occurrence involving the process caused by equipment performance or human action or by an occurrence external to the process.

***Frequency**:* Number of occurrences of an event per unit time (e.g., 1 event in 1000 yr = 1×10^{-3} events/yr).

***Hazard**:* A physical or chemical condition that has the potential for causing harm to people, property, or the environment.

Hazard and Operability (HAZOP) Study: A scenario-based hazard evaluation procedure in which a team uses a series of guide words to identify possible deviations from the intended design or operation of a process, then examines the potential consequences of the deviations and the adequacy of existing safeguards.

Hazard evaluation: Identification of individual hazards of a system, determination of the mechanisms by which they could give rise to undesired events, and evaluation of the consequences of these events on health (including public health), environment, and property. Uses qualitative techniques to pinpoint weaknesses in the design and operation of facilities that could lead to incidents.

Impact: A measure of the ultimate loss and harm of a loss event. *Impact* may be expressed in terms of numbers of injuries and/or fatalities, extent of environmental damage, and/or magnitude of losses such as property damage, material loss, lost production, market share loss, and recovery costs.

Incident: An unplanned event or sequence of events that either resulted in or had the potential to result in adverse impacts.

Incident sequence: A series of events composed of an initiating cause and intermediate events leading to an undesirable outcome.

Initiating cause: In the context of hazard evaluation procedures, the operational error, mechanical failure, or external event or agency that is the first event in an incident sequence and marks the transition from a normal situation to an abnormal situation. Synonymous with ***initiating event***.

Layer of protection: A physical entity supported by a management system that is capable of preventing an initiating cause from propagating to a specific loss event or impact.

Layer of Protection Analysis (LOPA): An approach that analyzes one incident scenario (cause-consequence pair) at a time, using predefined values for the initiating cause frequency, independent protection layer failure probabilities, and consequence severity, in order to compare an order-of-magnitude scenario risk estimate to tolerable risk goals for determining where additional risk reduction or more detailed analysis is needed. Scenarios are identified elsewhere, typically using a scenario-based hazard evaluation procedure such as a HAZOP Study.

Likelihood: A measure of the expected probability or frequency of occurrence of an event.

Loss event: Point of time in an abnormal situation when an irreversible physical event occurs that has the potential for loss and harm impacts. Examples include release of a hazardous material, ignition of flammable vapors or ignitable dust cloud, and overpressurization rupture of a tank or vessel. An incident might involve more than one loss event, such as a flammable liquid spill (first loss event) followed by ignition of a flash fire and pool fire (second loss event) that heats up an adjacent vessel and its contents to the point of rupture (third loss event). Generally synonymous with ***hazardous event***.

Mitigate: Reduce the impact of a loss event.

Mitigative safeguard: A safeguard that is designed to reduce loss event impact.

Preventive safeguard: A safeguard that forestalls the occurrence of a particular loss event, given that an initiating cause has occurred; i.e., a safeguard that intervenes between an initiating cause and a loss event in an incident sequence. (Note that *containment and control measures* are also preventive in the sense of preventing initiating causes from occurring; however, the term *preventive safeguard* in the context of hazard evaluation procedures is used with the specific meaning given here.)

Risk: The combination of the expected frequency (events/year) and severity (effects/event) of a single incident or a group of incidents.

Safeguard: Any device, system, or action that would likely interrupt the chain of events following an initiating cause or that would mitigate loss event impacts. See ***Preventive safeguard***; ***Mitigative safeguard***.

Scenario: An unplanned event or incident sequence that results in a loss event and its associated impacts, including the success or failure of safeguards involved in the incident sequence.

About the Author

Robert W. (Bob) Johnson earned B.S. and M.S. degrees in chemical engineering from Purdue University. He has been a process safety specialist since 1978, and is now president of the Unwin Company process risk management consultancy. He previously held senior positions with Hercules, Du Pont, and Battelle.

Mr. Johnson has authored AIChE Center for Chemical Process Safety (CCPS) books and has lectured on Hazard and Operability Studies and other process safety topics for the AIChE/ASME continuing education program and at universities in Ohio. He is a member of the CCPS Safety and Chemical Engineering Education (SACHE) Committee and the national Reactivity Management Roundtable, and is 2008 chair of the AIChE Safety & Health Division. He may be contacted at (614) 486-2245, rjohnson@unwin-co.com.
