LOPA Articles

The following were the two definitive papers on the topic of Layer of Protection Analysis (LOPA). The CCPS textbook and our course notebook provide the most up-to-date explanation on LOPA, but these two articles are excellent starting points.

1997 CCPS Conference and Workshop Proceedings
Layer of Protection Analysis: A New PHA Tool After HAZOP, Before Fault Tree Analysis

American Institute of Chemical Engineers
3 Park Avenue
New York, New York 10016-5991

It is sincerely hoped that the information presented in this volume will lead to an even more impressive safety record for the entire industry; however, the American Institute of Chemical Engineers, its consultants, CCPS Subcommittee members, their employers, and their employers officers and directors disclaim making or giving any warranties or representations, express or implied, including with respect to fitness, intended purpose, use or merchantability and/or correctness or accuracy of the content of the information presented in this document. As between (1) American Institute of Chemical Engineers, its consultants, CCPS Subcommittee members, their employers, their employers officers and directors and (2) the user of this document, the user accepts any legal liability or responsibility whatsoever for the consequences of its use or misuse.

Layer of Protection Analysis: A New PHA Tool After Hazop, Before Fault Tree Analysis

Arthur M. (Art) Dowell, III Senior Technical Fellow, Hazard Analysis, Rohm and Haas Company, PO Box 1915, Deer Park, TX 77536-1915 E-Mail: chedowe@rohmhaas.com

(first published in "International Conference and Workshop on Risk Analysis in Process Safety", 1997, CCPS/AIChE)

ABSTRACT

How do you know how many safeguards are enough to prevent or mitigate a chemical process impact event? What integrity level should be chosen for a Safety Instrumented (interlock) System (SIS)?

Building on the CCPS (Center for Chemical Process Safety) Guidelines for Safe Automation of Chemical Processes, this paper describes a new PHA (Process Hazard Analysis) tool called Layer of Protection Analysis (LOPA). Starting with data developed in the HAZOP (HAZard and OPerability analysis), and suggested screening values, the methodology accounts for the risk reduction of each safeguard. The mitigated risk for an impact event can be compared with the corporation's criteria for unacceptable risk. Additional safeguards or independent protection layers can be added. The required integrity level for any SIS safeguards can be determined.

LOPA focuses the risk reduction efforts toward the impact events with the highest risks. It provides a rational basis to allocate risk reduction resources efficiently.

LOPA can be easily applied after the HAZOP, but before fault tree analysis.

Introduction

In the Safety Life Cycle outlined in ISA-S84.01-1996 (ISA, 1996), steps are included to determine if a SIS (Safety Instrumented System) is needed and to determine the target SIL (Safety Integrity Level) for the SIS. The SIL is defined by the PFD (Probability of Failure on Demand) of the SIS (1). S84.01 gives guidance on building an SIS to meet a desired SIL; Green and Dowell (1995) outline how to set standard SIS designs.

How does one determine what SIL is appropriate for a particular process? Companies and individuals have struggled with qualitative ways to make this determination. It was frequently inconsistent and was often very upsetting. For example:

Portions of this paper will be published in ISA Tech/97 and the journal of Loss Prevention. Used by gracious permission.

ENGINEER: "Why is this existing interlock SIL 2?"

RISK ANALYST: "I don't know off the top of my head. What does the documentation say?"

ENGINEER: "It was set in a safety review. And you were there!"

RISK ANALYST: "Beats me! It doesn't look like it should be SIL 2 when I look at it now."

Undesired events and their causes are identified in a Process Hazard Analysis, such as HAZOP or What-If For an undesired event, several methods are in use in the process industries to determine the required SIL.

1. The modified HAZOP (HAZard and OPerability analysis) method in CCPS (1993) and in the informative annex of S84.01 really depends on the team comparing the consequence and frequency of the impact event with similar events in their experience, and then choosing an SIL. If the event being analyzed is worse or more frequent, then they would choose a higher SIL. It is very much in the experience and judgment of the team. Thus, the SIL chosen may depend more on whether a team member knows of an actual impact event like the one being analyzed, and it may depend less on the estimated frequency of the event.

2. The safety layer matrix listed in CCPS (1993) and in the informative annex of S84.01 (p49) uses categories of frequency, severity, and effectiveness of the protection layers. The categories are described in general terms and some calibration would be needed to get consistent results. The matrix was originally developed using quantitative calculations tied to some numeric level of unacceptable risk (Green, 1993).

3. The consequences-only method (mentioned in S84.01) evaluates only the severity of the unmitigated consequence. If the severity is above a specified threshold, a specified SIL would be required. This method does not account for frequency of initiating causes; it assumes all causes are "likely". It is recognized that this method may give a higher required SIL than other methods. The perceived trade-off is reduced analysis time. On other hand, for events whose causes have a high frequency, this method could give a lower SIL.

4. The fault tree analysis (FTA) method LISA, 1996) quantitatively estimates the frequency of the undesired event for a given process configuration. If the frequency is too high, an SIS of a certain SIL is added to the design and incorporated into the FTA. The SIL can be increased until the frequency is low enough in the judgment of the team. FTA requires significant resources.

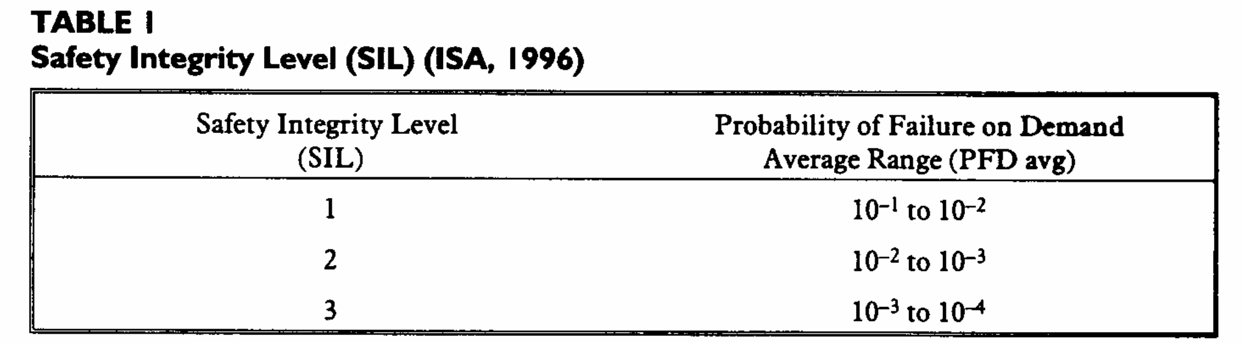


TABLE 1
Safety Integrity Level (SIL) (ISA, 1996)

Safety Integrity Level (SIL)	Probability of Failure on Demand Average Range (PFD avg)
1	10^{-1} to 10^{-2}
2	10^{-2} to 10^{-3}
3	10^{-3} to 10^{-4}

5. This paper describes a new method, Layer of Protection Analysis.

What Analysis Is Really Needed?

Each method to determine SIL attempts to deal with the following issues, either explicitly or implicitly:

- the severity of each consequence-fires, injuries, fatalities, environmental damage, property damage, business interruption, etc.
- the likelihood, or frequency, of each initiating cause of the undesired event-challenge occurs x times per year.
- the capability of non-SIS layers of protection-no layer of protection is perfect; for example, a pressure relief valve may fail to open I out of 100 times it is challenged.
- the frequency of the mitigated event compared to a target frequency – if the frequency of the mitigated event is low enough, the risk is viewed as tolerable. The more severe the consequences, the lower the target frequency.

Non-SIS Layer of Protection – Any Independent Protection Layer that prevents the impact event. Includes:

- **Relief Valves, Rupture Disks**
- **Evacuation Procedures**
- **Process Design (e.g., vessel maximum allowable working pressure is greater than the maximum pressure generated by the initiating cause.)**
- **Basic Process Control System (when control loop or logic can prevent the impact event)**
- **Operator Response to Alarms**

Inconsistency in determining SIL often comes from a lack of clarity for the frequency of the initiating cause and the target mitigated event frequency for which the risk is viewed as tolerable. These issues may be handled implicitly with individual team members having a different perception of the frequencies and the risk level that is tolerable. Some methods listed in the introduction do not deal with the causes explicitly, some do not deal with the frequencies of causes explicitly, and some do not deal with the target frequency for a risk level that is tolerable. Yet each team member is doing some sort of intuitive, internal analysis that asks:

- How bad is it?
- How often could it be caused?
- How effective will the layers of protection be?
- Is the mitigated event frequency intolerable or not?

Some companies have published guidelines for the risk the process imposes on the community (Renshaw, 1990), industrial neighbors, and employees. These guidelines can be used to establish criteria for the SIL evaluation as shown later in this paper.

On the other hand, many companies have not published guidelines for the risk the process imposes on the community, industrial neighbors, and employees. However, for various process configurations, decisions are still made to apply further risk reduction via design change or additional IPLs, or not to apply additional risk reduction (i.e., risk is tolerable). This information can be converted to targets for use in determining SIL. The target could take the form of the number of IPLs and the SIL value required for a given consequence severity and challenge frequency.

What is needed is a way to determine the required SIL rationally and consistently among individuals, teams, projects, and companies.

Layer of Protection Analysis (LOPA)

LOPA is built on concepts from chapter 7 of CCPS (1993). This paper is based on more than five years' use of the technique.

LOPA uses a multi-disciplined team, like a HAZOP team. Knowledgeable representatives are needed from:

- Operations-operator, foreman

- Management

Process Engineering Control Engineering Instrument/Electrical (craftsman, foreman, or engineer) Risk Analysis (hazard evaluation specialist)

At least one person must be skilled in the LOPA methodology. One of the team members should be skilled as a meeting/team facilitator.

A HAZOP (or other hazard identification procedure) is done first. HAZOP tables usually list Deviations, Causes, Consequences, Safeguards, and Recommendations. The HAZOP table may also include estimates of the Frequency for each Cause and Severity for each Consequence. With these estimates a risk matrix can be used to estimate Risk for a Cause-Consequence pair (Fryman, 1996). Figure 1 shows the HAZOP information and the LOPA information in graphical form. The solid lines show the sequence of the HAZOP or LOPA development. The dotted lines show how HAZOP information is transferred to the LOPA. A sample LOPA table is shown in Figure 2.

Impact Event Classification

Each Impact Event from the Hazard Identification is classified for Severity Level and Maximum Target Likelihood for the impact event using 2. The Impact Event, Severity Level, and Maximum Target Likelihood are written into column I of the Layer of Protection Analysis form, Figure 2.

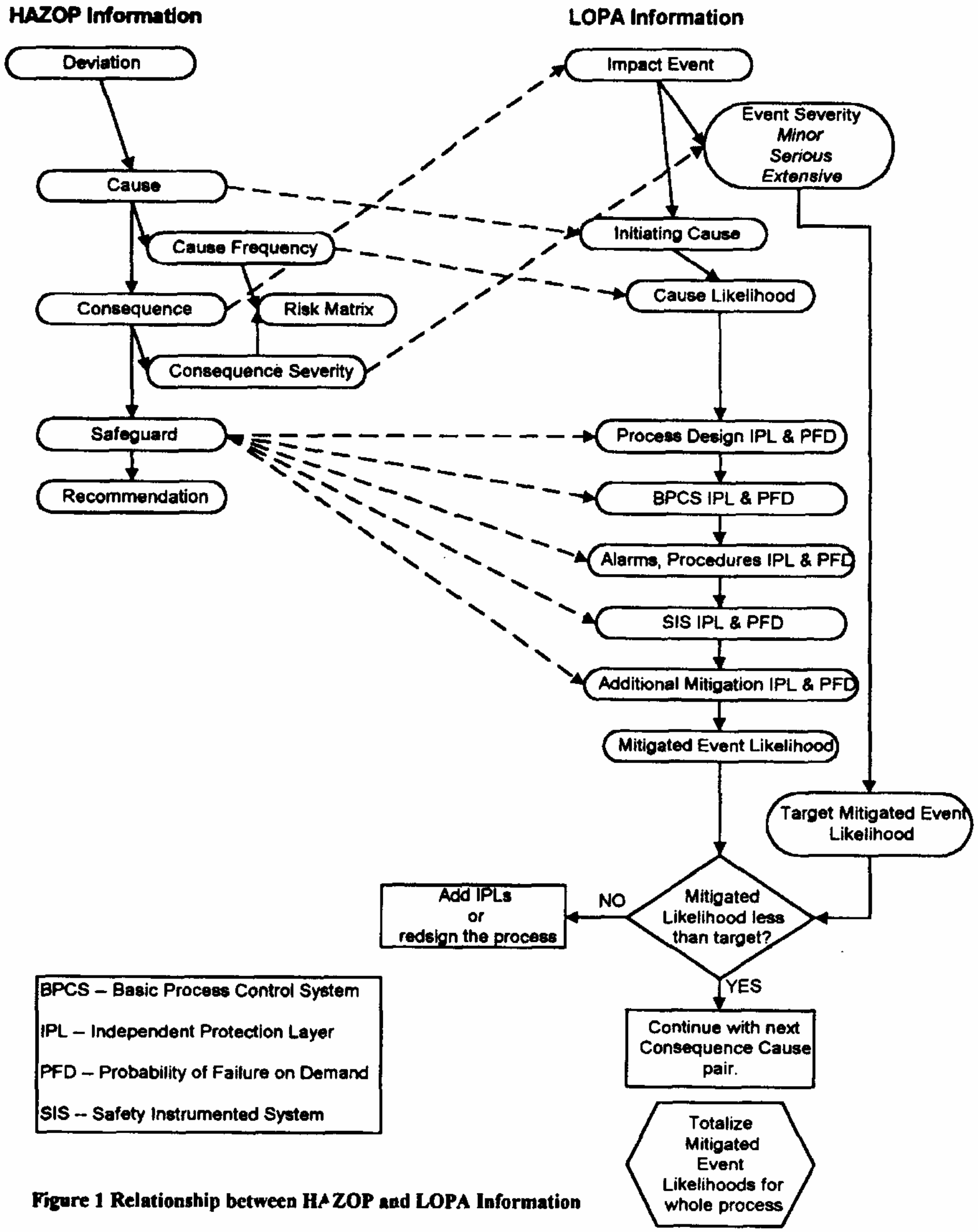

HAZOP Information
LOPA Information
Deviation
Cause
Cause Frequency
Consequence
Risk Matrix
Consequence Severity
Safeguard
Recommendation
Impact Event
Event Severity
Minor
Serious
Extensive
Initiating Cause
Cause Likelihood
Process Design IPL & PFD
BPCS IPL & PFD
Alarms, Procedures IPL & PFD
SIS IPL & PFD
Additional Mitigation IPL & PFD
Mitigated Event Likelihood
Target Mitigated Event Likelihood
Mitigated Likelihood less than target?
NO
Add IPLs or redesign the process
YES
Continue with next Consequence Cause pair.
Totalize Mitigated Event Likelihoods for whole process
BPCS – Basic Process Control System
IPL – Independent Protection Layer
PFD – Probability of Failure on Demand
SIS – Safety Instrumented System

Figure 1 Relationship between HAZOP and LOPA Information

Figure 2 Layer of Protection Analysis

Interlock Number ____________ Asset Number ____________ Drawing Number ______________

____________ Company Plant: ____________

Process: ____________ Sample — Work in Progress

Page 14 of 14

Meeting Dates: ________

#	1	2	3	4	5	6	7	8	9	10
	Impact Event & Severity	Initiating Cause	Challenge Likelihood	Independent Protection Layers				Additional Mitigation: Pressure Relief Fire Protection System	IPLs	Mitigated Event Likelihood
			/yr	Process Design	BPCS (DCS)	Alarms, Procedures	SIS (PLC, relays)	Restricted Access Etc.,		/yr
1.	Catastrophic rupture of distillation column with shrapnel, toxic release E Maximum Target Likelihood = 1E-8 /yr	Loss of cooling tower water to condenser, once every 10 years	1E-1	Column, condenser, reboiler, and piping maximum allowable working pressures are greater than maximum possible pressure from steam reboiler 1E-2	Logic in DCS trips steam flow valve and steam RCV on high pressure or high temperature. No credit since not independent of SIS.	High column pressure and temperature alarms can alert operator to shut off the steam to the reboiler (manual valve). 1E-1	Logic in PLC trips steam flow valve and steam RCV on high pressure or high temperature (dual sensors separate from DCS). (SIL 3) 1E-3	Pressure relief valve opens on high pressure. 1E-2	3	1E-9
2.	Toxic release from distillation column relief valve S Maximum Target Likelihood = 1E-6 /yr	Loss of cooling tower water to condenser, once every 10 years	1E-1		Logic in DCS trips steam flow valve and steam RCV on high pressure or high temperature. No credit since not independent of SIS.	High column pressure and temperature alarms can alert operator to shut off the steam to the reboiler. (manual valve). 1E-1	Logic in PLC trips steam flow valve and steam RCV on high pressure or high temperature (dual sensors separate from DCS). (SIL 3) 1E-3		2	1E-5 (Additional Prevention / Mitigation needed)
3.										
4.										

Notes: Severity Levels: E - extensive; S - Serious; M - Minor

1E-8 equals $1x10^{-8}$

Likelihood value(s) are events per year, other numerical values are probabilities of failure on demand.

Participants: XXXX

BPCS is Basic Process Control System, PLC is Programmable Logic Controller, IPLs is Independent Protection Layers.

file: C:\MY DOCUMENTS\AMD WORK\R&H\CCPS_ATL\CCPS97C.DOC

Date Printed: May 26, 1997

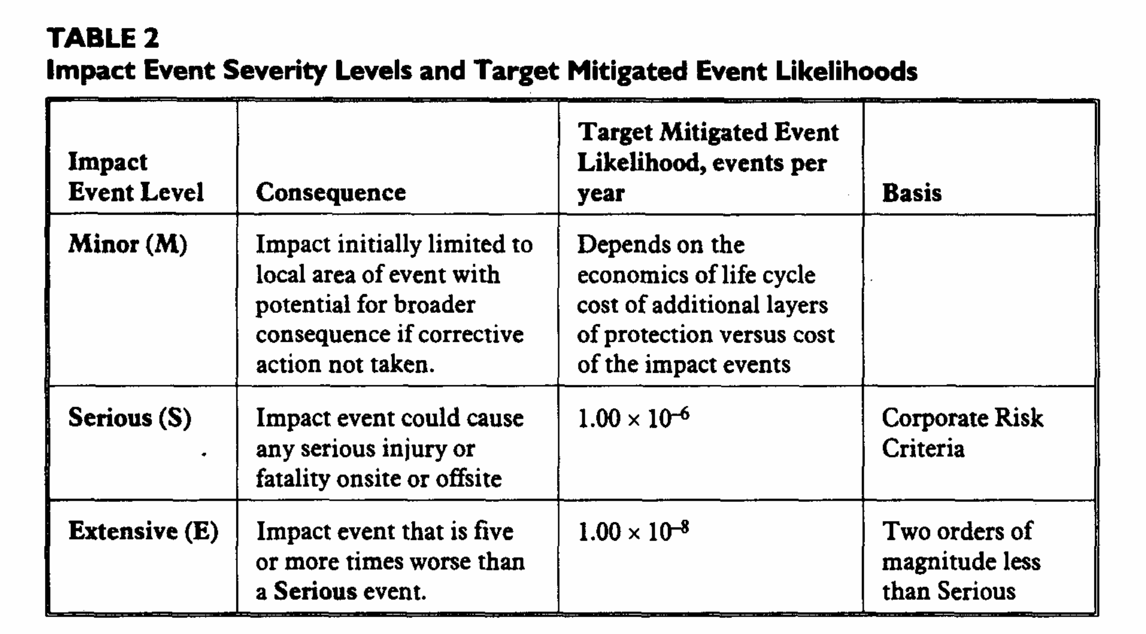


TABLE 2
Impact Event Severity Levels and Target Mitigated Event Likelihoods

Impact Event Level	Consequence	Target Mitigated Event Likelihood, events per year	Basis
Minor (M)	Impact initially limited to local area of event with potential for broader consequence if corrective action not taken.	Depends on the economics of life cycle cost of additional layers of protection versus cost of the impact events	
Serious (S)	Impact event could cause any serious injury or fatality onsite or offsite	1.00×10^{-6}	Corporate Risk Criteria
Extensive (E)	Impact event that is five or more times worse than a Serious event.	1.00×10^{-8}	Two orders of magnitude less than Serious

Initiating Cause

For each Impact Event, the team lists all the Initiating Causes in column 2 of Figure 2. Note that a HAZOP Consequence may be listed in several sections of the HAZOP. It's important to gather all the Causes. The remaining calculations are carried out for each Initiating Cause for each Impact Event.

Initiating Cause Likelihood

For each Initiating Cause, the team fills in the Challenge (Initiating Cause) Likelihood in column 3, Figure 2, with units of events per year. Typical Initiating Cause Likelihoods are shown in 3. The team uses its experience to estimate the Initiating Cause Likelihood. The Initiating Cause Likelihood is also called the frequency of the challenge.

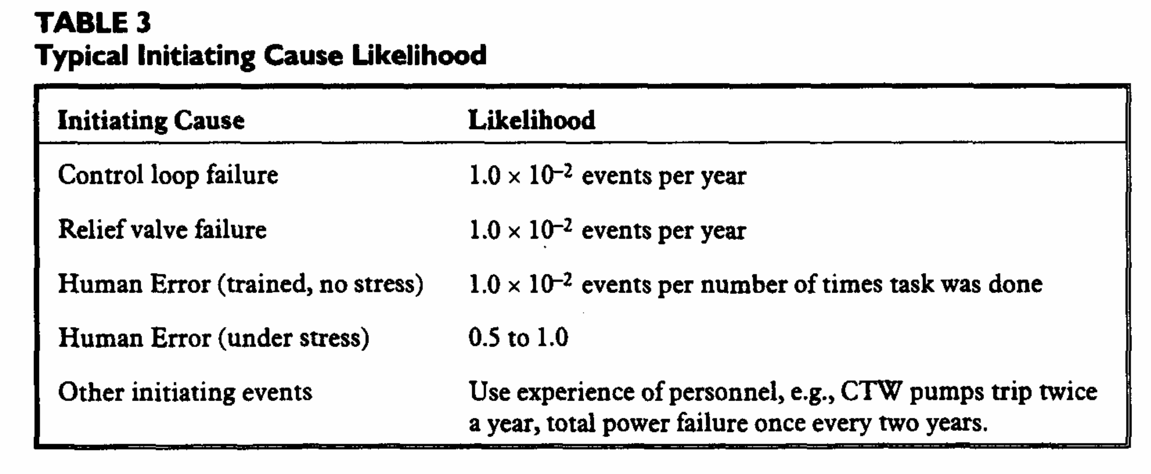


TABLE 3
Typical Initiating Cause Likelihood

Initiating Cause	Likelihood
Control loop failure	1.0×10^{-2} events per year
Relief valve failure	1.0×10^{-2} events per year
Human Error (trained, no stress)	1.0×10^{-2} events per number of times task was done
Human Error (under stress)	0.5 to 1.0
Other initiating events	Use experience of personnel, e.g., CTW pumps trip twice a year, total power failure once every two years.

Rules for IPLs

1. Each protection layer counted must be truly independent of the other protection layers. That is, there must be no failure that can deactivate two or more protection layers.

2. The frequency reduction for an IPL is two orders of magnitude, i.e., 10^{-2} PFD (that is, the availability is 99%).

- Exception: Risk reduction for Operator Response to Alarms is one order of magnitude, i.e., 10^{-1}.
- If an IPL is believed to be more reliable (lower value for PFD), a Quantitative method should be used to confirm the PFD. (For example, if the team desires to improve the unavailability of risk reduction logic in the BPCS (Basic Process Control System) by adding additional sensors or final elements, the impact event should be reviewed by a quantitative method such as fault tree.)

3. The IPL is specifically designed to prevent or mitigate the consequences of a potentially hazardous event.

4. The IPL must be dependable; it can be counted on to do what it was intended to do.

5. The IPL will be designed so it can be audited and a system to audit and maintain it will be provided.

6. If the initiating event is caused by a failure in the Basic Process Control System (BPCS), the BPCS cannot be counted as an IPL.

7. Alarms that are annunciated on the BPCS are not independent of the BPCS; if the BPCS is counted as an IPL, then such alarms cannot be counted as an IPL.

8. A control loop (PID loop) in the BPCS whose normal action would compensate for the initiating event can be considered as an IPL. For example, an initiating cause for high reactor pressure could be failure of a local upstream pressure regulator; the normal action of the reactor pressure controller would be to close the inlet PV, thus providing protection against the impact event.

Independent Protection Layers and Probability of Failure on Demand

The team lists all the Independent Protection Layers that could prevent the Initiating Cause from reaching the Impact Event. The IPLs may be different for different Initiating Causes (columns 4-7, Figure 2). The team determines which protection layers are independent.

The team assigns a PFD (Probability of Failure on Demand) to each Independent Protection Layer, typical values are shown in 4.

The IPLs and their PFDs are written in columns 4-7 of Figure 2.

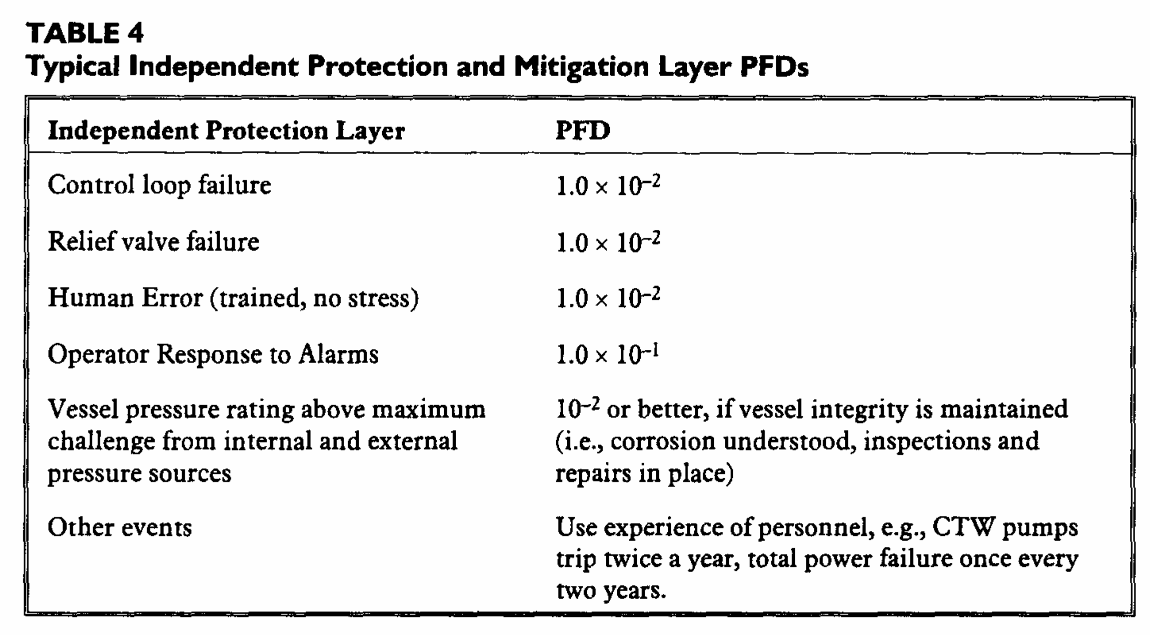


TABLE 4
Typical Independent Protection and Mitigation Layer PFDs

Independent Protection Layer	PFD
Control loop failure	1.0×10^{-2}
Relief valve failure	1.0×10^{-2}
Human Error (trained, no stress)	1.0×10^{-2}
Operator Response to Alarms	1.0×10^{-1}
Vessel pressure rating above maximum challenge from internal and external pressure sources	10^{-2} or better, if vessel integrity is maintained (i.e., corrosion understood, inspections and repairs in place)
Other events	Use experience of personnel, e.g., CTW pumps trip twice a year, total power failure once every two years.

Additional Mitigation

The team lists Additional Mitigation layers and assigns a PFD to each layer. A mitigation layer reduces the severity of the impact, but may not prevent all aspects of the event. Examples of mitigation layers include: relief valves, rupture disks, overflows to safe location, sensors to detect a release and an evacuation procedure, sensors and automatic deluge system. Again, each layer must be independent. The Additional Mitigation layers and their PFDs are written in column 8, Figure 2.

The team should be sure to understand the severity of the consequence of the mitigated event. An unmitigated event might be vessel rupture with toxic release. It could be mitigated to toxic release from a relief valve. If the severity of release from the relief valve is serious or extensive, it should be entered into the LOPA as another impact event.

Mitigated Event Likelihood

The team calculates the Mitigated Event Likelihood by multiplying the Initiating Cause Likelihood (column 3, Figure 2) by the PFDs of the IPLs (columns 5-8) and enters the number in column 10. The Intermediate Event Likelihood has units of events per year. The Intermediate Event Likelihood is compared with the Target Mitigated Event Likelihoods shown in 2.

If the Mitigated Event Likelihood is less than the Target Mitigated Event Likelihood, there are probably enough IPLs to meet the Corporate Risk Criteria and additional IPLs may not be required. (However, further risk reduction may be desirable.)

If the Mitigated Event Likelihood is more than the Target Mitigated Event Likelihood, then additional risk reduction is probably needed. The team should seek to reduce the risk, first by applying inherently safer concepts, and then by applying additional layers of protection. The LOPA table would be updated for the design changes.

Number of IPLs

The number of Independent Protection Layers is entered in column 9, Figure 2. Serious and Extensive Impact events normally require at least two IPLs.

SIS Needed

If the team finds that an SIS is needed to meet the Target Mitigated Event Likelihood, the team enters the SIS description in column 7 and assigns it a PFD. The SIL is entered in column 7, Figure 2.

The team should use an SIS only if other design changes (using inherently safer concepts) cannot reduce the Mitigated Event Likelihood to less than the target (CCPS, 1996). Avoid using safety interlocks (added-on features). If possible, use built-in features (inherent) to reduce risk.

The team continues the iterative process of increasing the number of protection layers and recalculating the Mitigated Event Likelihood until the Mitigated Event Likelihood is less than the Target Impact Event Likelihood.

Add Up All The Risk

After all the impact events are analyzed and tabulated in the LOPA Table in Figure 2, the team adds up all the Mitigated Event Likelihoods for Serious and Extensive Impact Events for each affected population group.

The Risk of Fatality for each affected population is calculated by the following formulas or their equivalents:

Fire:

Risk of Fatality = (Mitigated Event Likelihood of Release)

X (Probability of Ignition)

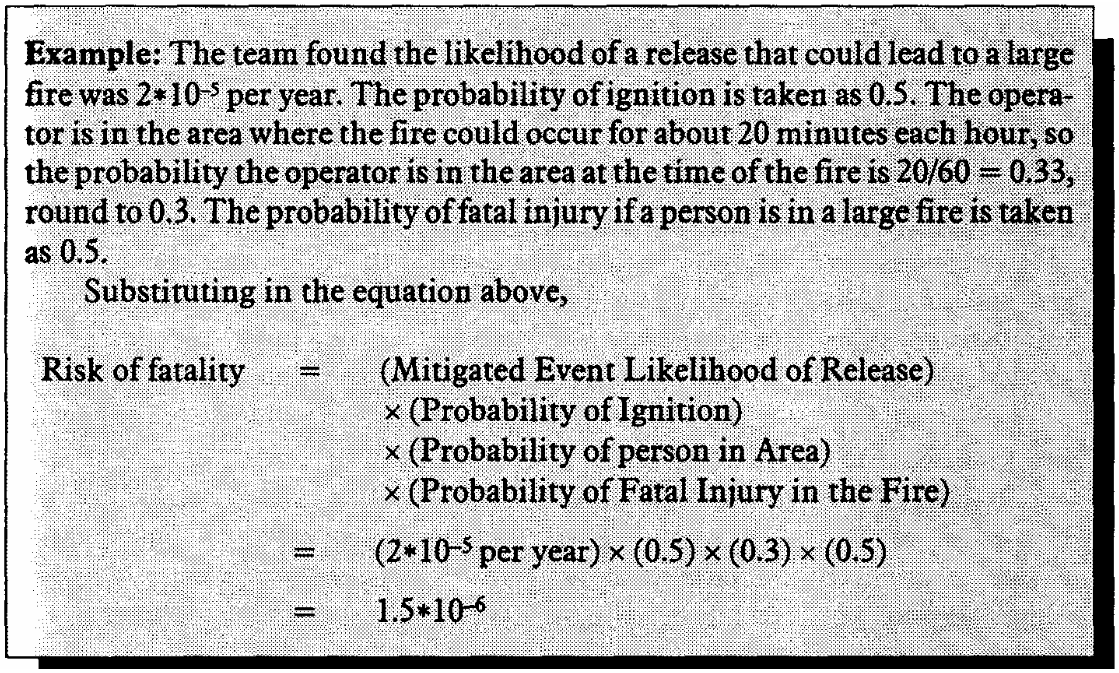
X (Probability of person in Area)

X (Probability of Fatal Injury in the Fire [usually 0.5])

Toxic Release:

Risk of Fatality (Mitigated Event Likelihood of Release) = (Probability of person in Area) x (Probability of Fatal Injury in the Release)

The team uses the Risk Analyst expertise and the knowledge of the team to adjust these equations for the conditions of the release and the work practices of the affected populations.



Example: The team found the likelihood of a release that could lead to a large fire was $2*10^{-5}$ per year. The probability of ignition is taken as 0.5. The operator is in the area where the fire could occur for about 20 minutes each hour, so the probability the operator is in the area at the time of the fire is 20/60 = 0.33, round to 0.3. The probability of fatal injury if a person is in a large fire is taken as 0.5.

Substituting in the equation above,

Risk of fatality = (Mitigated Event Likelihood of Release)
× (Probability of Ignition)
× (Probability of person in Area)
× (Probability of Fatal Injury in the Fire)

= ($2*10^{-5}$ per year) × (0.5) × (0.3) × (0.5)

= $1.5*10^{-6}$

Corporate Risk Criteria Test

The total risk from all impact events for the affected population should be compared to the Corporate Risk Criteria.

- If the total risk does not meet the criteria for the affected population, then the team should seek to reduce the risk, first by applying inherently safer concepts, and then by applying additional layers of protection. Such design changes will require an update to the LOPA table.

- If the total risk is less than the criteria for the affected population and additional risk reduction can be achieved by some additional cost, the Team should recommend those additional risk reduction features to the business (Renshaw, 1990).

- If the total risk is substantially less than the criteria for the affected population, then no further risk reduction is needed.

The objective is to be sure the total risk from the facility meets the Corporate Risk Criteria. The team should remember that employees and the community may have risk from other parts of the unit, from other projects, and from other units. That additional risk must be considered against the Corporate Risk Criteria.

Sample Problem

Part of a sample problem for Layer of Protection Analysis is shown in Figure 2. The system under study is an atmospheric distillation column with a steam reboiler and a cooling tower water condenser.

Impact Event 1

The HAZOP identified high pressure as a deviation. One consequence of high pressure in the column was catastrophic rupture of the column, if it exceeded its design pressure. In the LOPA, this impact event is listed as Extensive for Severity Class, since there is potential for five or more fatalities. The Maximum Target Likelihood for Extensive impact events is 1 x 10^{-8}/yr. The impact event, its class, and Maximum Target Likelihood are written in column I of Figure 2.

Note that Figure 2 uses an alternate notation for scientific numbers for better legibility at smaller font sizes (I x 10^{-8} = IE-8).

The HAZOP listed several Initiating Causes for this impact event. One initiating cause was loss of cooling tower water to the main condenser. The operators said this happened about once every ten years. The Initiating Cause is written in column 2 of Figure 2, and the Challenge Likelihood is written in column 3 (1/10 yr = 1 x 10^{-1}.

The LOPA team identified one Process Design IPL for this impact event and this cause. The maximum allowable working pressure of the distillation column and connected equipment is greater than the maximum pressure that can be generated by the steam reboiler during a cooling tower water failure. Its PFD is 1 x 10^{-2}. This design feature is listed in column 4 of Figure 2.

The Basic Process Control System for this plant is a Distributed Control System (DCS). The DCS contains logic that trips the steam flow valve and a steam RCV on high pressure or high temperature of the distillation column. This logic's primary purpose is to place the control system in the shut-down condition after a trip so that the system can be restarted in a controlled manner. It is listed in column 5, Figure 2, since it can prevent the impact event. However, no PFD credit is given for this logic since the valves it uses are the same valves used by the SIS – the DCS logic does not meet the test of independence for an IPL.

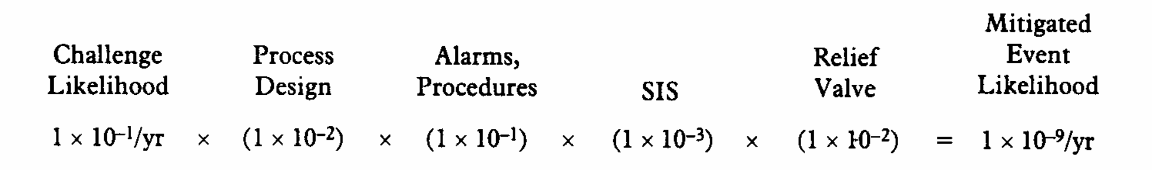
High pressure and temperature alarms displayed on the DCS can alert the operator to shut off the steam to the distillation column, using a manual valve if necessary. This protection layer meets the criteria for an IPL-the sensors for these alarms are separate from the sensors used by the SIS. The operators should be trained and drilled in the response to these alarms. This information is recorded in Figure 2, column 6, with the PFD of 10^{-1}.

SIS logic implemented in a PLC will trip the steam flow valve and a steam RCV on high distillation column pressure or high temperature using dual sensors separate from the DCS. The PLC has sufficient redundancy and diagnostics such that the SIS has a PFD of 10^{-3} or SIL 3. This information is written in column 7 of Figure 2.

The distillation column has Additional Mitigation of a pressure relief valve designed to maintain the distillation column pressure below the maximum allowable working pressure when cooling tower water is lost to the condenser. Its PFD is 10^{-2}. This information is recorded in column 8, Figure 2.

The number of independent protection layers is 3. This value is entered in column 9 of Figure 2.

The Mitigated Event Likelihood for this cause-consequence pair is calculated by multiplying the Challenge Likelihood in column 3 by the IPL PFDs in columns 4,6, 7, and 8:



Challenge Likelihood		Process Design		Alarms, Procedures		SIS		Relief Valve		Mitigated Event Likelihood
1×10^{-1}/yr	×	(1×10^{-2})	×	(1×10^{-1})	×	(1×10^{-3})	×	(1×10^{-2})	=	1×10^{-9}/yr

The Mitigated Event Likelihood is entered in column 10 of Figure 2. The value of I x 10^{-9} is less than the maximum target likelihood of I x 10^{-8} for extensive impact events.

Note that the relief valve protects against catastrophic rupture of the distillation column, but it introduces another impact event-a toxic release. The toxic release is entered on the Layer of Protection Analysis form as Impact Event #2.

Impact Event 2

The toxic release from the distillation column is classed as a Serious event. The impact event description, severity, and maximum target likelihood are entered in column I of Figure 2.

The Initiating Cause and Challenge Likelihood are the same for Impact Events I and 2. The information in columns 2 and 3 in Figure 2 is copied into the row for Impact Event 2.

The process design IPL of Impact Event 1 can protect against the relief valve release only if the relief valve set pressure is greater than the maximum pressure from the steam reboiler. For this example, the relief valve set pressure is less than the maximum pressure produced by the steam reboiler. Thus, there is no process design IPL for this impact event.

The Impact Event I information in the IPL columns of BPCS, Alarms, Procedures, and SIS also applies to Impact Event 2. Columns 5, 6, and 7 are thus duplicated.

The pressure relief valve does not prevent the release. There is no additional mitigation for this event.

The number of IPLs for this event is 2. This is written in column 9 of Figure 2.

The Mitigated Event Likelihood for this cause-consequence pair is calculated by multiplying the Challenge Likelihood in column 3 by the IPL PFDs in columns 6 and 7:

Challenge Likelihood		Alarms, Procedures		SIS		Mitigated Event Likelihood
$(1 \times 10^{-1}/yr)$	×	(1×10^{-1})	×	$(1x10^{-3})$	=	$1 \times 10^{-5}/yr$

The Mitigated Event Likelihood is entered in column 10 of Figure 2. The value of $1 \text{ x } 10^{-5}$ is more than the maximum target likelihood of $1 \text{ x } 10^{-6}$ for extensive impact events. The team should consider if the design could be changed to be inherently safer to avoid the toxic release. Additional independent protection layers may be needed. A scrubber or flare could be added to treat the release from the relief valve. Alternately, the relief valve set pressure could be increased to the maximum allowable working pressure of the equipment.

Add Up All The Risk

After all the impact events and all the cause have been analyzed and recorded in the layer of protection analysis form, the team will add up all the Mitigated Event Likelihoods for all the Serious and Extensive Impact Events. The Risk of Fatality will be calculated as described above in this paper and compared with the Corporate Risk Criteria to be sure the distillation column and the other processing units do not impose intolerable risk on affected populations.

LOPA Advantages

LOPA focuses greater risk reduction efforts on Impact Events with high severity and high likelihood. It ensures that all the identified Initiating Causes are considered, and it confirms which Independent Layers of Protection are effective for each Initiating Cause. LOPA can be used to allocate risk reduction resources efficiently, so that one Impact Event is not left with too little protection, while another is overly protected.

LOPA encourages thinking from a system perspective. Formerly, interlocks were labeled by the sensor, as in "High Reactor Pressure." LOPA shows the Layers of Protection for different Impact Events stemming from the same Initiating Cause: for example, "catastrophic rupture of the reactor" and "release of reactor contents through the relief valve."

LOPA gives clarity in the reasoning process and it documents everything that was considered. While this method uses numbers, judgment and experience are not excluded. In some cases, the team's "gut feel" was uncomfortable with the number calculated, so it went back and reviewed the assumptions for the frequency of the initiating event. The method makes the input from "gut feel" explicit, rather than implicit.

In addition, LOPA offers a rational basis for managing Layers of Protection that may be taken out of service - e.g., interlock bypass.

LOPA is more quantitative than the qualitative hazard consequence and likelihood categories often used to estimate risk rankings in a HAZOP, but it is less work than Fault Tree Analysis or Quantitative Risk Analysis.

ACKNOWLEDGEMENTS

To the CCPS and ISA committees who wrote the Guidelines for Safe Automation of Chemical Processes and the ISA-S84-01, respectively. To Dallas Green, David Patlovany, Rich Sypek, and Mieng Tran, who sharpened my thinking as we wrote internal interlock guidelines. To W. H. Johnson, Jr., who gives excellent training in LOPA. To Paul Gruhn, who asks excellent questions.

DISCLAIMER

Although we believe the information contained in this paper is factual, no warranty or representation, expressed or implied, is made with respect to any or all of the content thereof, and no legal responsibility is assumed therefore. The examples shown are simply for illustration, and as such do not necessarily represent Rohm and Haas Company guidelines. The readers should use data, methodology, and guidelines that are appropriate for their situations.

REFERENCES

Center for Chemical Process Safety (CCPS) (1993). Guidelines for Safe Automation of Chemical Processes. New York: American Institute of Chemical Engineers.

Center for Chemical Process Safety (CCPS) (1996). Inherently Safer Chemical Processes: A Life Cycle Approach. New York: American Institute of Chemical Engineers.

Fryman, C. (1996). "Managing HazOp Recommendations Using an Action Classification Scheme," AlChE Spring National Meeting, New Orleans, LA, February 25-29,1996. Green, D. L. (1993). Personal communication to A. M. Dowell, III, June, 1993.

Green, D. L., and A. M. Dowell, 111 (1995). "How to Design, Verify, and Validate Emergency Shutdown Systems." ISA Transactions 34, 261-272

Instrument Society of America (ISA) (1996). ISA-S84.01-1996. Application of Safety Instrumented Systems to the Process Industries. Research Triangle Park, NC: Instrument Society of America.

Renshaw, F. M. (1990). "A Major Accident Prevention Program" Plant/0perations Progress 9,3 (July), 194-7

LIST OF ACRONYMS

BPCS	Basic Process Control System
CCPS	Center for Chemical Process Safety
DCS	Distributed Control System
FTA	Fault Tree Analysis
HAZOP	HAZard and OPerability Analysis
IPL	Independent Protection Layer
ISA	International Society for Measurement and Control

LOPA	Layer of Protection Analysis
PFD	Probability of Failure on Demand
PHA	Process Hazard Analysis
PLC	Programmable Logic Controller
QRA	Quantitative Risk Analysis
RCV	Remote control valve
SIL	Safety Integrity Level
SIS	Safety Instrumented System (also sometimes called Safety Interlock System)

1997 CCPS Conference and Workshop Proceedings
Risk Acceptance Criteria and Risk Judgment Tools *(now called Layer of Protection Analysis [LOPA])* Applied Worldwide within a Chemical Company

American Institute of Chemical Engineers
3 Park Avenue
New York, New York 10016-5991

It is sincerely hoped that the information presented in this volume will lead to an even more impressive safety record for the entire industry; however, the American Institute of Chemical Engineers, its consultants, CCPS Subcommittee members, their employers, and their employers officers and directors disclaim making or giving any warranties or representations, express or implied, including with respect to fitness, intended purpose, use or merchantability and/or correctness or accuracy of the content of the information presented in this document. As between (1) American Institute of Chemical Engineers, its consultants, CCPS Subcommittee members, their employers, their employers officers and directors and (2) the user of this document, the user accepts any legal liability or responsibility whatsoever for the consequences of its use or misuse.

Risk Acceptance Criteria and Risk Judgment Tools *(now called Layer of Protection Analysis [LOPA])* Applied Worldwide within a Chemical Company

William G. Bridges and Tom R. Williams JBF Associates, Inc., 1000 Technology Drive,
Knoxville, TN 37932-3353.

(first published in "International Conference and Workshop on Risk Analysis in Process Safety", 1997, CCPS/AIChE)

ABSTRACT

From 1994 through early 1996, a multinational chemical company developed a standard for evaluating risk of potential accident scenarios. This standard was developed to help users (i.e., engineers, chemists, managers, and other technical staff) determine (1) when sufficient safeguards were in place for an identified scenario and (2) which of these safeguards were critical to achieving (or maintaining) the tolerable risk level. Plant management was held accountable for upholding this standard, and they were also held accountable for maintaining (to an extremely high level of availability) the critical safety features that were identified. In applying this standard, the users found they needed more guidance on selecting the appropriate methodology for judging risk; some used methodologies that were deemed too rigorous for the questions being answered and others in the company used purely qualitative judgment tools. The users in the company agreed to a set of three methods for judging risk and developed a decision tree, followed by training, to help the users (1) choose the proper methodology and (2) apply the methodology chosen consistently. The new guidelines for risk acceptance and risk judgment were taught to technical staff (those who lead hazard reviews and design new processes) worldwide in early 1996. This paper presents the evolution of the risk tolerance and risk judgment approach used by the company.

Background

This paper is written on behalf of a major chemical company headquartered in the USA. The company wishes to remain anonymous because of the litigious environment in the USA. This environment ultimately penalizes any company that recognizes the necessity of accepting or tolerating any risk level above "zero" risk. However, the only way to reach zero risk is to go out of business altogether. All chemical processing operations contain risk factors that must be managed to reasonably reduce the risk to people and the environment to tolerable levels, but the risk factors cannot be entirely eliminated. This chemical company has made significant strides in recent years in risk management; particularly, the company has implemented effective risk judgment and risk acceptance (tolerance) criteria. Because JBF Associates, Inc. (JBFA) has worked with the company in the training steps related to these criteria, the company has agreed to allow JBFA to share a synopsis of the company's approach in the hope that others can benefit from the lessons learned to date.

To understand the risk management systems described in this paper, a brief portrait of the chemical company is essential. The company conducts operations principally in North America, Asia, and Europe. The operations include more than 20 petrochemical, specialty chemicals, and polymer processing plants, along with several related terminals and blending facilities. The processes involve flammable, toxic, and highly reactive chemicals. The company is subject to OSHA process safety management (PSM) and EPA risk management program (RMP) regulations in the USA, and they have a corporate process safety standard that applies worldwide. Each plant has technical staff who implement the process safety standards and related standards and guidelines. The company has been successful in worldwide implementation of strategies described in this paper.

One key to this success is holding each plant manager accountable for implementation of the risk management policies and standards; any deviation from a standard or criteria based on a standard, must be pre-approved by the responsible vice president of operation.

In our experience, many companies claim to hold plant managers accountable, but in the final analysis production goals usually take precedence over safety requirements; this company has shown equal vigilance in enforcement of safety- (risk-) related standards.

Chronology of Risk Judgment Implementation

Figure 1 and the following paragraphs present a synopsis of this company's efforts to implement a risk-based judgment system, which is now producing significant return for the company. Although other companies may follow a different path to achieve the same goals, there are valuable lessons to be learned from this company's particular experiences.

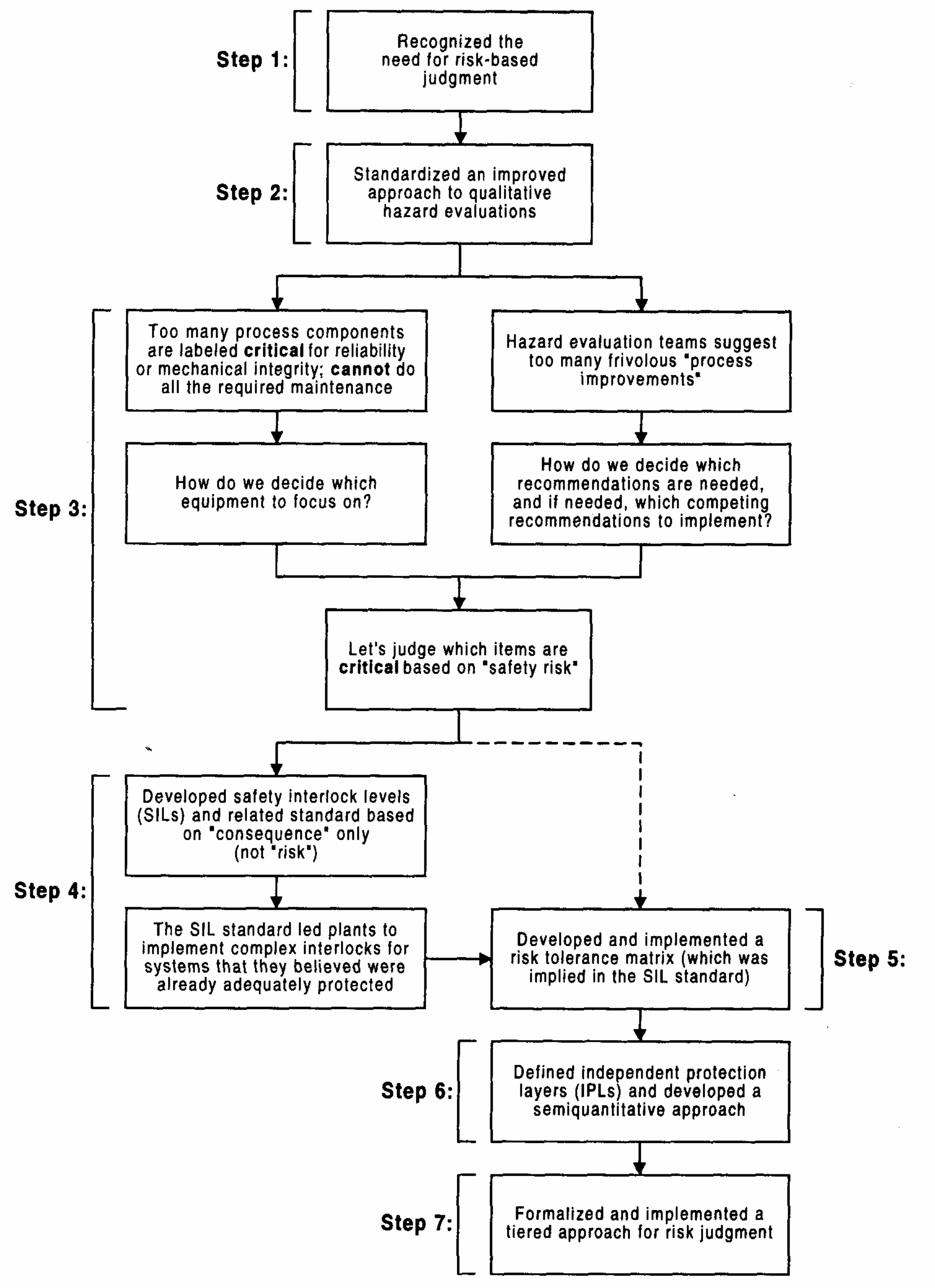
STEP 1: RECOGNIZE THE NEED FOR RISK-BASED JUDGMENT

The technical personnel who were responsible for judging risk of accident scenarios for the company recognized the need for adequately understanding and evaluating risk many years ago. However, most decisions about plant operations were made subjectively without comparing relative risk of the accident scenarios. Not until a couple of major accidents occurred did key line managers, including operations vice presidents, become convinced of the value of risk judgment and the need to include risk analysis in the decision-making process.

STEP 2: STANDARDIZE AN IMPROVED APPROACH TO HAZARD EVALUATION

The company realized that the best chance for managing risk was to maximize the opportunity for identifying key accident scenarios. Therefore, the first enhancement was to improve the specifications for process hazard analyses (PHAs) and provide training to PHA leaders to meet these specifications. A standard and a related guideline were developed prior to training. The standard became one of the process safety standards that plant management was not allowed to circumvent without prior approval. The guideline provided corporate's interpretation of the standard, and although all plants were strongly advised to follow the guideline, plant managers were allowed flexibility to develop their own plant-specific guidelines. The major enhancements to the PHA specification were (1) to require a step-by-step analysis of critical operating procedures (because deviations from these procedures lead to most accidents), (2) improve consideration of human factors, and (3) improve consideration of facility siting issues. The company also began using quantitative risk assessment (QRA) to evaluate complex scenarios.

FIGURE 1: The Evolution of a Risk judgment Approach


Step 1:
Recognized the need for risk-based judgment
Step 2:
Standardized an improved approach to qualitative hazard evaluations
Step 3:
Too many process components are labeled critical for reliability or mechanical integrity; cannot do all the required maintenance
Hazard evaluation teams suggest too many frivolous "process improvements"
How do we decide which equipment to focus on?
How do we decide which recommendations are needed, and if needed, which competing recommendations to implement?
Let's judge which items are critical based on "safety risk"
Step 4:
Developed safety interlock levels (SILs) and related standard based on "consequence" only (not "risk")
The SIL standard led plants to implement complex interlocks for systems that they believed were already adequately protected
Developed and implemented a risk tolerance matrix (which was implied in the SIL standard)
Step 5:
Step 6:
Defined independent protection layers (IPLs) and developed a semiquantitative approach
Step 7:
Formalized and implemented a tiered approach for risk judgment

STEP 3: DETERMINE IF PURELY QUALITATIVE RISK-BASED JUDGMENT IS SUFFICIENT

These improvements to the hazard identification methodologies led to many recommendations for improvements. Managers were left with the daunting task of resolving each recommendation, which included deciding between competing alternatives and deciding which recommendations to reject. Their only tool was pure qualitative judgment.

Simultaneously, the company began to intensify its efforts in mechanical integrity. Without any definitive guidance on how to determine critical safety features, the company identified a large portion of the engineered features as "critical" to safe operation. The company recognized that many of the equipment/instrument features listed in the mechanical integrity system did little to minimize risk to the employees, public, or environment. They also recognized that it would be wasting valuable maintenance and operations resources to consider all of these features to be critical. So, the company had to decide which of the engineered features (protection layers) were most critical.

With all of the impending effort to maintain critical design features and to implement or decide between competing recommendations, the company began a search for a risk-based decision methodology. They decided to focus on "safety risk" as the key parameter, rather than "economic" or "quality" risk. The company had a few individuals who were well trained and experienced in using QRA, but this tool was too resource intensive for evaluating the risk associated with each critical feature recommendation, even when the focus of the decision was narrowed to "safety risk." So the managers (decision makers) in charge of resolving the hazard review recommendations and deciding which components were critical, were left with qualitative judgment only; this proved too inconsistent and led many managers to wonder if they were performing a re-analysis to decide between alternatives.

Corporate management realized that they needed to make a baseline decision on the "safety-related" risk the company was willing to tolerate. They also needed a methodology to estimate more consistently if they were within the tolerable risk range

STEP 4: PREVENT HIGH CONSEQUENCE ACCIDENT SCENARIOS

Many companies would not have this as the next chronological step, but about this time, the company recognized that they also needed a corporate standard for safety interlocks to control design, use, and maintenance of key safety features throughout their global operations. So, the company developed definitions for safety interlock levels (SILs) and developed standards for the maintenance of interlocks within each SIL. Then the company developed a guideline that required the implementation of specified SILs based solely on safety consequence levels (instead of risk levels). If a process had the potential for an overpressure event resulting in a catastrophic release of a toxic material or a fire or explosion (defined as a Category V consequence as listed in Table 1) due to a runaway chemical reaction, then a Class A interlock (triple redundant sensors and double redundant actuator) was required by the company for preventing the condition that could lead to the runaway.

However, basing this decision solely on the safety consequence levels, did not give any credit for existing safeguards or alternate approaches to reducing the risk of the overpressure scenario. As a result, this SIL standard skewed accident prevention toward installing and maintaining complex (albeit highly reliable) interlocks. The technical personnel in the plants very loudly voiced their concern about this extreme "belts and suspenders" approach.

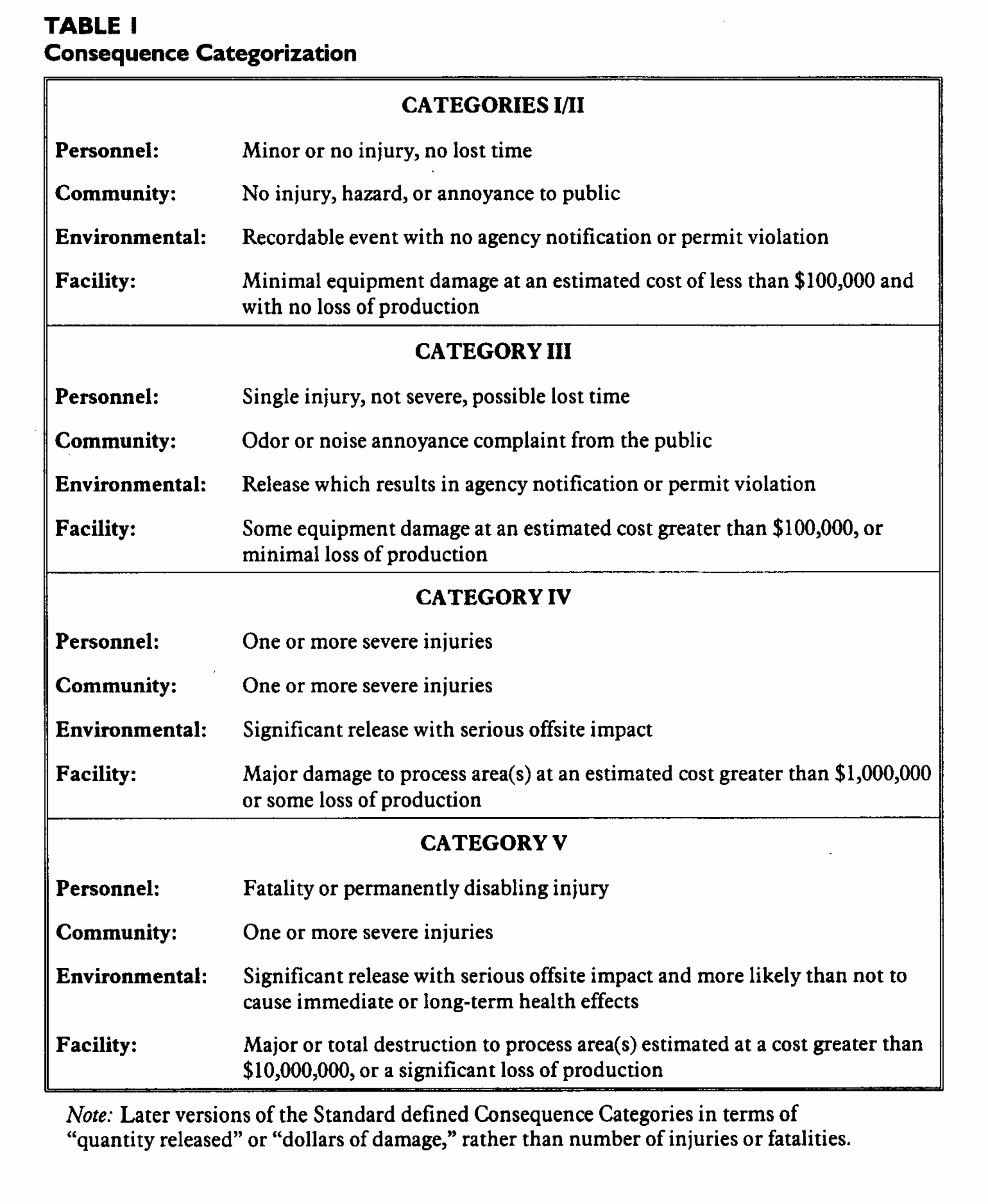


TABLE I
Consequence Categorization

	CATEGORIES I/II
Personnel:	Minor or no injury, no lost time
Community:	No injury, hazard, or annoyance to public
Environmental:	Recordable event with no agency notification or permit violation
Facility:	Minimal equipment damage at an estimated cost of less than $100,000 and with no loss of production
	CATEGORY III
Personnel:	Single injury, not severe, possible lost time
Community:	Odor or noise annoyance complaint from the public
Environmental:	Release which results in agency notification or permit violation
Facility:	Some equipment damage at an estimated cost greater than $100,000, or minimal loss of production
	CATEGORY IV
Personnel:	One or more severe injuries
Community:	One or more severe injuries
Environmental:	Significant release with serious offsite impact
Facility:	Major damage to process area(s) at an estimated cost greater than $1,000,000 or some loss of production
	CATEGORY V
Personnel:	Fatality or permanently disabling injury
Community:	One or more severe injuries
Environmental:	Significant release with serious offsite impact and more likely than not to cause immediate or long-term health effects
Facility:	Major or total destruction to process area(s) estimated at a cost greater than $10,000,000, or a significant loss of production

Note: Later versions of the Standard defined Consequence Categories in terms of "quantity released" or "dollars of damage," rather than number of injuries or fatalities.

STEP 5: MANAGE RISK OF ALL SAFETY-IMPACT SCENARIOS

Before the company's self-imposed deadline for compliance with the corporate SIL standard, the company agreed with the plants that alternate risk-reduction measures should be given proper credit. To make this feasible, the company had to begin to evaluate the overall risk of a scenario, not just the consequences. They decided to develop a corporate standard and guidelines for estimating the mitigated risk of accident scenarios. (This development had actually begun at the end of Step 3, but the momentum in this direction slowed when emphasis for risk control shifted temporarily to safety interlocks.)

First, a risk matrix was developed with five consequence categories (as were used for the SILs described earlier), and seven frequency categories (ranging from 1/year to 1/10 million years). Next, the company delineated the risk matrix into three major areas:

- Tolerable Risk-Implementation of further risk reduction measures was not required; in fact, it was strongly discouraged so that focus would not be taken off of maintaining existing or implementing new critical layers of protection
- Intolerable Risk-Action was required to reduce the risk further
- Optional-An intermediate zone was defined, which allowed plant management the option to implement further risk reduction measures, as they deemed necessary

Figure 2 shows the company's risk matrix.

Some companies would have called this a semiquantitative approach, but in this company, the PHA teams used this matrix to "qualitatively" judge risk. Teams would vote on which consequence and frequency categories an accident scenario belonged (considering the qualitative merits of each existing safeguard), and they would generate recommendations for scenarios not in the Tolerable Risk area. This approach worked well for most scenarios, but the company soon found considerable inconsistencies in the application of the risk matrix in qualitative risk judgments. Also, the company observed that too many accident scenarios were requiring resource-intensive QRAs. It was clear that an intermediate approach for judging the risk of moderately complex scenarios was needed. And, the company still needed to eliminate the conflict between the risk matrix and the SIL standard.

STEP 6: DEVELOP A SEMIQUANTITATIVE APPROACH (THE BEGINNINGS OF A TIERED APPROACH) FOR RISK JUDGMENT

This was a very significant step for the company to take; the effort began in early 1995 and was implemented in early 1996. Along with the inconsistencies in applying risk judgment tools, there was still confusion among plant personnel about when and how they should use the SIL standard and the risk matrix. Both were useful tools that the company had spent considerable resources to develop and implement. The new guidelines would need to somehow integrate the SILs and the risk matrix categories to form a single standard for making decisions. And the plants also needed a tool (or multiple tools), besides the extremes of pure qualitative judgment and a QRA, to decide on the best alternative for controlling the risk of an identified scenario. The technical personnel from the corporate offices and from the plants worked together to develop a semiquantitative tool and to define the needed guidelines.

Consequence Category / Frequency of Consequence (per Year)*	Category I	Category II	Category III	Category IV	Category V
10^{-0}	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at next opportunity (notify corporate management)	Immediate action (notify corporate management)	Immediate action (notify corporate management)
10^{-1}	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at next opportunity (notify corporate management)	Immediate action (notify corporate management)
10^{-2}	No further action	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at next opportunity (notify corporate management)	Action at next opportunity (notify corporate management)
10^{-3}	No further action	No further action	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at next opportunity (notify corporate management)
10^{-4}	No further action	No further action	No further action	Optional (evaluate alternatives)	Optional (evaluate alternatives)
10^{-5}	No further action	No further action	No further action	No further action	Optional (evaluate alternatives)
10^{-6}	No further action	No further action	No further action	No further action	No further action
10^{-7}					

FIGURE 2. Risk Matrix

*For example, 10^{-2} is equivalent to 1/100 years.

One effort toward a semiquantitative tool involved defining a new term called an independent protection layer (IPL), which would represent a single layer of safety for an accident scenario. Defining this new term required developing examples of IPLs to which the plant personnel would be able to relate. For example, a spring-loaded relief valve is independent from a high-pressure alarm; thus a system protected by both of these devices has two IPLs. On the other hand, a system protected by a high-pressure alarm and a shutdown interlock using the same transmitter has only one IPL. Class A, B, and C safety interlocks (which were defined previously in the SIL standard) were also included as example IPLs.

To ensure consistent application of IPLs (i.e., to account for the relative reliability/availability of various types of IPLs), it was necessary to identify how much "credit" plant personnel could claim for a particular type of IPL. For example, a Class A safety interlock would deserve more credit than a Class B interlock, and a relief valve would be given more credit than a process alarm. This need was addressed by assigning a "maximum credit number" for each example IPL (see Table 2). The credit is essentially the order of magnitude of the risk reduction anticipated by claiming the safeguard as an IPL for the accident scenario. The company believed that when PHA teams or designers used the IPL definitions and related credit numbers, the consistency between risk analyses at the numerous plants would improve.

Another (parallel) effort involved assigning frequency categories to typical "initiating events" for accident scenarios (see Table 3); these initiating events were intended to represent the types of events that could occur at any of the various plants. The frequency categories were derived from QRA experience within the company and provided a consistent starting point for semiquantitative analysis.

Finally, a semiquantitative approach for estimating risk was developed, incorporating the frequency of initiating events and the IPL credits described previously. Although this approach used standard equations and calculation sheets not described here, the basic approach required teams to:

- Identify the ultimate consequence of the accident scenario and document the scenario as clearly as possible, stating the initiating event and any assumptions.
- Estimate the frequency of the initiating event (using a frequency from Table 3, if possible)
- Estimate the risk of the unmitigated event and determine from the risk matrix if the risk is tolerable as is:
    - If the risk is not tolerable, take credit for existing IPLs until the risk reaches a tolerable level in the risk matrix; use best judgment in defining IPLs and deciding which ones to take credit for first
    - If the risk is still not tolerable, develop a recommendation(s) that will lower the risk to a tolerable level

- Record the specific safety features (IPLs) that were used to reach a tolerable risk level

TABLE 2
Credits for Independent Protection Layers (IPLs)

Example IPL	Maximum Credit Number for IPL
Basic Process Control Systems	
Automatic control loop (If failure is not a significant initiating event contributor and is independent of the Class A, B, or C interlock [if applicable] and final element is tested at least once per 4 years)	1
Human Intervention	
Manual response in field with more than 10 minutes available for response (If sensor/alarm are independent of the Class A, B, or C interlock [if applicable] and operator training includes required response)	1
Manual response in field with more than 40 minutes available for response (If sensor/alarm are independent of the Class A, B, or C interlock [if applicable] and operator training includes required response)	2
*Passive Devices**	
Secondary containment such as a dike (If good administrative control over drain valves exists)	2
Spring-loaded relief valve in clean service	3
Safety Interlocks	
Class A interlock (Provided independent of other interlocks)	3
Class B interlock (Provided independent of other interlocks)	2
Class C interlock (Provided independent of other interlocks)	1

* Claiming passive devices, such as a relief valve, in conjunction with the interlock in question, should be the exception.

TABLE 3
Initiating Event Frequencies

Event	Estimated Frequency
Loss of cooling (Standard simplex system)	1/year
Loss of power (Standard simplex system)	1/year
Human error (Routine, once per day opportunity)	1/year
Human error (Routine, once per month opportunity)	1/10 years
Basic process control loop failure	1/10 years
Large fire	1/100 years* 1/1,000 years

*Fire frequency for an individual process system of 1/100 years is conservative.

The company demanded "zero" tolerance for deviating from inspection, testing, or calibration of the documented hardware IPLs and enforcement of administrative IPLs. (Any deviation without prior approval was considered a serious deficiency on internal audits.) Other features not credited as IPLs could be kept if they served a quality, productivity, or environmental protection purpose; otherwise, these items could be "run to failure" or removed because doing so would have no effect on the risk level.

This serniquantitative approach explicitly met a need expressed in Step 3: determining which of the engineered features was critical to managing risk. PHA teams began applying this approach to validate their qualitative risk judgments. However, the company still needed to (1) formalize guidelines for when to use qualitative, semiquantitative, and quantitative risk judgment tools and (2) standardize the use each tool.

STEP 7: FORMALIZE AND IMPLEMENT THE TIERED APPROACH

The company decided that the best way to standardize risk judgment in all of the plants was to (1) revise the risk tolerance standard, (2) revise the SIL standard, (3) formalize a guideline for deciding when and how to use each risk judgment tool, and (4) provide training to all potential users of the standards and guidelines (including engineers at the plants and corporate offices, PHA leaders, maintenance and production superintendents, and plant managers). The formal guideline and training would be based on a decision tree dictating the complexity of analysis required to adequately judge risk. The company's first attempt at a decision tree is shown in Figure 3.

After the training needs were assessed for each type of user, the company produced training materials and exercises (including the decision tree) to meet those needs. The training took approximately I day for managers and superintendents (because their needs were essentially to understand and ensure adherence to the standards) and approximately 4 days for process engineers, design engineers, production engineers, PHA leaders, and QRA leaders. The training was initiated in early 1996, and early returns have shown strong acceptance of this approach, particularly in Europe, where the experience in the use of quantitative methods is much broader. The most significant early benefits have been:

- A reduced number of safety features (IPLs) labeled as "critical"

- Less frivolous recommendations from PHA teams, which now have a better understanding of risk and risk tolerance

- Better decisions on when to use a QRA (because there is now an intermediate alternative)

Path Forward

The next steps are to continually evaluate the current approach and modify it as necessary to meet the changing needs of the corporation and the plant personnel. For instance, the decision criteria for when to use the semiquantitative or the QRA method may change; the credit given to IPLs may need to change. More training is probably necessary on selected topics; for example, the personnel in the United States need additional training on the use of the serniquantitative approach and on how to mesh risk-based judgments with OSHA PSM and EPA RMP compliance efforts (there is an excellent opportunity for synergy here). A computer program may be developed to simplify some of the decisions, calculations, tracking, and reporting.

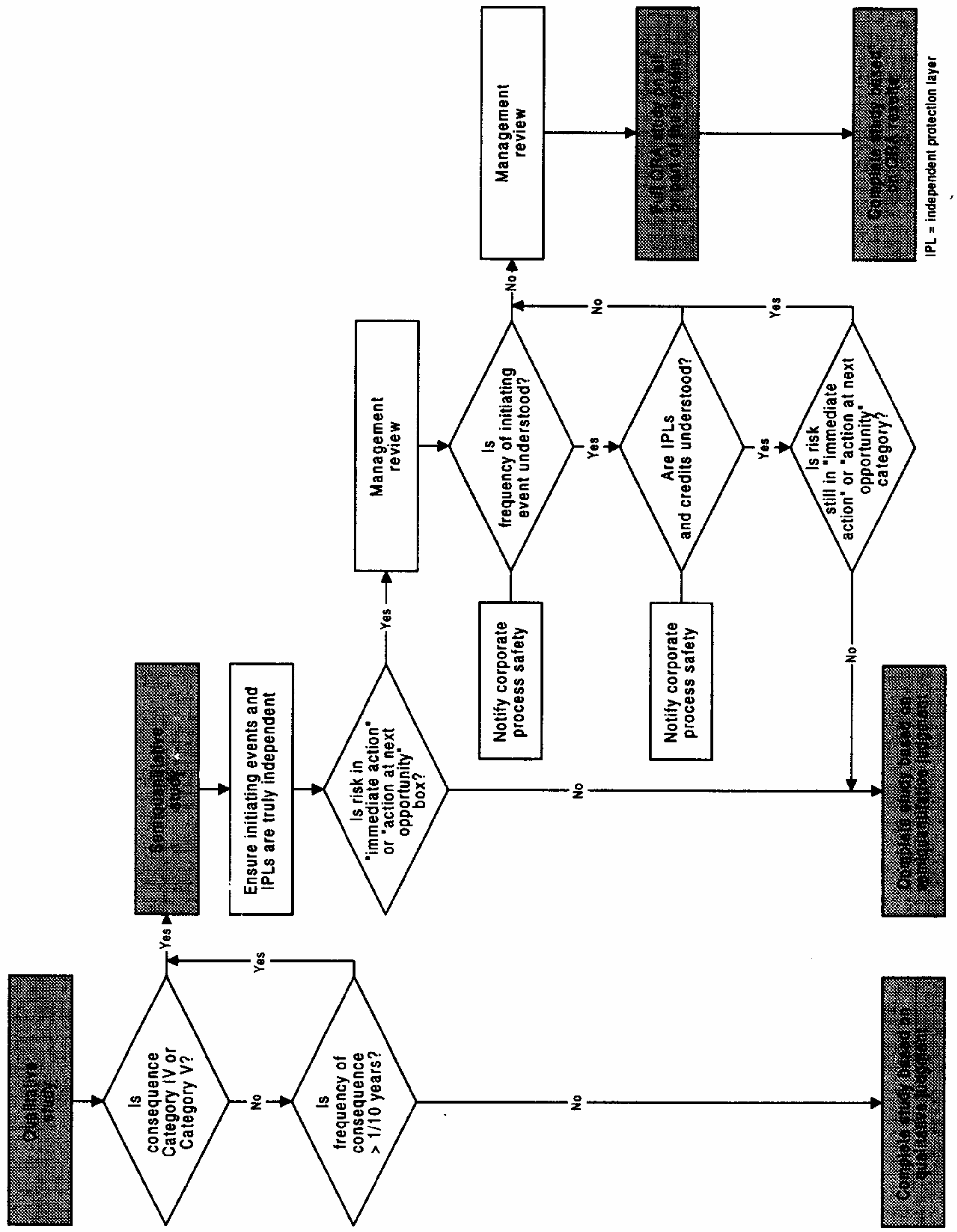

Qualitative study
Is consequence Category IV or Category V?
No
Is frequency of consequence > 1/10 years?
Yes
Yes
No
Complete study based on qualitative judgment
Semiquantitative study
Ensure initiating events and IPLs are truly independent
Is risk in "immediate action" or "action at next opportunity" box?
Yes
No
Complete study based on semiquantitative judgment
Management review
Is frequency of initiating event understood?
Notify corporate process safety
Yes
Are IPLs and credits understood?
Notify corporate process safety
Yes
Is risk still in "immediate action" or "action at next opportunity" category?
No
No
Yes
No
Management review
Full QRA study on all or part of the system
Complete study based on QRA results
IPL = independent protection layer

FIGURE 3 Decision Tree Dictating Which Risk Judgment Tool to Use

Conclusions

The company believes they have experienced major reductions in risk throughout the stepwise implementation of this approach. The approach helps the company manage their risk control resources wisely and helps to more defensibly justify decisions with regulatory and legal implications. The key to the success of this program lies beyond the mechanics of the risk-judgment approach; it lies with the care company personnel have taken to understand and manage risk on a day-to-day basis. Company management has developed clear, comprehensive standards, guidelines, and training to ensure the plants manage risk appropriately. This is reinforced by company management taking an aggressive stance on enforcing adherence by the plants to company standards. The risk judgment standards and guidelines appear to be working to effectively reduce risk while minimizing the cost of maintaining "critical" safeguards. This company's success serves as only one example that risk management throughout a multinational chemical company is possible, practical, and necessary.

Bibliography

Advanced Process Hazard Analysis Leader Training, Process Safety Institute, Knoxville, TN, 1993.

Guidelines for Chemical Process Quantitative Risk Analysis, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 1989.

Guidelines for Hazard Evaluation Procedures, 2nd Edition with Worked Examples, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 1992.

F. P. Lees, Loss Prevention in the Process Industries, Vols. 1 and 2, Butterworth's, London, 1980.

D. F. Montague, "Process Risk Evaluation-What Method to Use," Reliability Engineering and System Safety, Vol. 29, Elsevier Science Publishers Ltd., England, 1990.