Integrated Hazards Analysis

Using the strengths of multiple methods to maximize effectiveness

By Steven R. Trammell, Donald K. Lorenzo and Brett J. Davis

HAZARD ANALYSIS TECHNIQUES take many forms, with some uniquely developed to assess specific systems, processes or scenarios. Many well-known methods are also used on a wide variety of systems; these include what-if/checklist analysis, hazard and operability analysis (HazOp), and failure modes and effects analysis (FMEA). Unfortunately, these generalized methods often work well on only part of the risk assessment spectrum, such as failure mode identification, causal factor determination or risk prioritization; few of them effectively address all aspects of risk evaluation. This article discusses a hybrid methodology that uses the strengths of HazOp and FMEA to identify failure modes and priority rank risks, and layers of protection analysis to evaluate and apply effective controls. As part of the hybridized methodology development, a completely new risk prioritization chart was prepared that allows consideration of risks to the environment, people and business from both engineered processes and personnel operations.

Background

Effective manufacturing processes are generally viewed as those that create high-quality products efficiently, while protecting workers, the community, environment, customers and the company's physical assets. In today's global economy, it has also become increasingly important for these operations to run as efficiently as possible to provide effective competition in order to forestall relocation or closure of manufacturing facilities. These competitive business pressures create conflicts among the differing goals, especially in the areas of responsible manufacturing and profitability. However, with proper system evaluation techniques and the associated management of identified risks, an equitable balance can be attained that ultimately addresses the issue of competitiveness.

This article focuses on two main manufacturing methods—continuous (direct delivery) and batch processes—to which risk management concepts are applied. Of these two methods, continuous processes receive the most attention because these are the types of systems to which the integrated hazards analysis approach is most frequently applied. Piece-part manufacturing (such as assembly line processes), for which process failures and resulting product defects are generally predicted via techniques such as statistical process control (SPC) and for which predelivery quality assessment is possible, are also briefly addressed.

The advantages of using an integrated hazards analysis approach to determine and evaluate system risk are also discussed, focusing primarily on engineered systems. This represents only part of the risk spectrum for an operating system; additional risk evaluation techniques should be considered to capture the big picture of system risk. These might include design for SH&E concepts integrated into the process/product development phase, and life-cycle analysis to determine potential impacts of chemical use, product disposal and eventual system decommissioning.

The Problem Statement

Continuous, direct-delivery processes, such as plant utilities, must operate virtually without interruption. Controls that simply recognize failure or the onset of failure (such as deviation analysis typical of SPC programs) are inadequate

Steven R. Trammell, P.E., CSP, CHMM, *is a member of the technical staff for Motorola's Semiconductor Product Sector, in Austin, TX, where he is responsible for implementing and facilitating risk assessment programs for site operations worldwide. He has 22 years' experience developing and integrating risk management programs for major operations in the petrochemical, defense and electronics industries. Trammell is a member of ASSE's Central Texas Chapter, and is active in working groups for international fire and building code development and National Fire Protection Assn. He holds a B.S. in Mechanical Engineering from the University of Texas, as well as an M.B.A. from the University of Phoenix.*

Donald K. Lorenzo, P.E., *is a senior technical director of the Knoxville, TN, office of ABS Consulting. He has more than 25 years' experience in systems design and analysis for process facilities. Lorenzo has managed/performed more than 90 analyses of process hazards associated with manufacturing, using, separating, storing or destroying hazardous chemicals and radioactive materials. He is the author of* A Manager's Guide to Reducing Human Error, *and a coauthor of* A Manager's Guide to Quantitative Risk Assessment *and* Guidelines for Hazard Evaluation Procedures, 2nd ed.

Brett J. Davis, P.E., *is principal staff engineer for Motorola's Semiconductor Products Sector in Austin, TX. During his career, he has worked in the natural gas and semiconductor industries, and also spent several years as a chemical process regulator for the City of Austin Fire Dept. Davis has chaired the Travis County Local Emergency Planning Committee since 1995 and has been an officer of the Air & Waste Management Assn.'s Central Texas Chapter since 1998. He holds a B.S. in Chemical Engineering from the University of Texas and an M.S. in Hazardous Waste Management from National Technological University.*

Figure 1

Generic Risk Matrix

Increasing Severity →

Increasing Likelihood ↑

Risk Tolerance	Severity 1	Severity 2	Severity 3	Severity 4	Severity 5
Likelihood 6	Optional*	Optional*	Action at next opportunity	Immediate action	Immediate action
Likelihood 5	Optional*	Optional*	Optional*	Action at next opportunity	Immediate action
Likelihood 4	No further action	Optional*	Optional*	Action at next opportunity	Action at next opportunity
Likelihood 3	No further action	No further action	Optional*	Optional*	Action at next opportunity
Likelihood 2	No further action	No further action	No further action	Optional*	Optional*
Likelihood 1	No further action	No further action	No further action	No further action	Optional*

*Alternative action should be evaluated.

to prevent interruption. A specific example of this is a factory where power sags, partial interruptions or complete loss of electrical service is catastrophic to the process. Managing the risks of such processes requires selection of controls that are predictive and preventive, or that dramatically reduce severity.

Hazards Determination

A methodology that systematically and effectively reduces risk must have several key attributes, any of which alone may provide insufficient information to generate useful solutions. The methodology must allow for review starting in the design phase. The most cost-effective and long-term design corrections are those that allow risks to be "engineered out" from the start. Unfortunately, this is where many typical methodologies are weakest—in the determination or prediction of system failure modes—because the system design itself is evolving during this phase.

A methodology must also identify all significant potential failure modes that pose risks to human safety and health, the environment, the facility and the process. Most engineered systems will contain aspects that can create risks within all four categories; therefore, an effective and integrated hazards analysis methodology should provide the ability to evaluate them all. Modern management systems approaches, such as those embraced by international environmental, safety and quality systems standards, contain requirements that drive the consideration of these multiple aspects. A methodology must allow for differentiation between controls that provide failure identification and those able to prevent failure or reduce consequences. As noted, direct-delivery systems will drive different levels of control acceptability than would a piece-parts manufacturing operation.

Risk Assessment

Understanding the hazards and the accepted tolerance for losses from these hazards is critical for success of the analysis. This risk tolerance or "appetite" is commonly expressed in some form of matrix or chart, showing how frequently the organization is willing to suffer losses of a given magnitude (Figure 1). To use the matrix, the methodology must allow the team to score the likelihood of each important failure mode and the severity of its consequences. If a scenario's likelihood and severity exceed the set risk tolerance, the methodology must allow the team to evaluate the effectiveness of controls that could reduce the risk.

This does not mean that additional controls or layers of protection must be applied to all failure scenarios regardless of consequence. Rather, when the risk tolerance is exceeded, the methodology must provide a systematic way to evaluate risk reduction measures. These measures may include changing the fundamental design to an inherently safer alternative, or adding layers of protection to the existing design. These layers may be engineering or administrative controls, and they may be active or passive in nature. Risk scoring with associated action levels is an important part of the analysis, as it provides the key guidance needed to evaluate the degree of risk reduction and required resources with minimal bias from the analysis team. It also provides documentation of the decision-making process when system risk is accepted for an identified failure mode.

Development of a Hybrid Methodology

Various analysis techniques can be used to identify a system's hazards, including the popular HazOp, what-if/checklist and FMEA techniques. Both HazOp and what-if/checklist are creative techniques based on brainstorming. Both are mature methodologies, and both divide complex systems into smaller, more manageable "nodes" for study. While either technique can produce a thorough list of important system failures, causes, consequences and controls, neither lends itself to rigorous risk acceptability analysis. Furthermore, neither technique is necessarily effective in prioritizing risks associated with identified failures, and neither provides a process to assess the relative effectiveness of proposed corrective actions.

On the other hand, FMEA focuses on individual components and their failure modes. Thus, each failure mode is only considered once, and all of its effects and controls are listed together. This allows a more-accurate assessment of the risk associated with each component failure. The QS-9000 version of FMEA includes a simple scoring methodology for quantifying the risk associated with each failure mode (AIAG). As the team scores the likelihood of the failure mode, the severity of its consequences and the effectiveness of detection, it gains a thorough understanding of the failure mechanism and, more importantly, insight on determining truly effective corrective actions.

FMEA also helps the team set priorities for failure mode effects so that resources can be applied more

Figure 2

Process Parameter/Guideword Definitions

Process Parameter \ Guideword	None	More	Less	Reverse	Part Of	Other Than	As Well As
Flow	flow stopped	flow greater than specification	flow less than specification	flow opposite specification		flow to wrong location (e.g. spill)	
Level	container empty	container filled above specification (e.g. overflowing)	container filled below specification			loss of containment (e.g. container leaking)	
pH		pH higher than specification	pH lower than specification		pH inconsistent		
Temperature (T)		T higher than specification	T lower than specification				
Pressure (P)	vacuum	P higher than specification	P lower than specification				
State		more phases than specification	fewer phases than specification	change of state		incorrect phases	
Reaction/Addition	no reaction	reaction more rapid than specification	reaction slower than specification	decomposition	reaction stops at intermediate	incorrect reaction product	more reactions than specification
Speed/Frequency	machine action stopped	machine action faster than specification	machine action slower than specification		machine action inconsistent	wrong machine action	
Time (typically for batch process)	process not started	process runs long	process runs short			process starts at wrong time (e.g. out of sequence)	
Composition/Mixing	mixing does not occur	more mixing than specification	less mixing than specification			separation occurs	contamination occurs
Voltage (V)/Current (I)	no electricity flow	V or I higher than specification	V or I lower than specification	current flowing opposite of specification		current to ground	
Information (com)	no com with BPCS (e.g. wires cut)	com faster than BPCS can store	com slower than needed for proper BPCS response		com incomplete	com incorrect	com interference

effectively. Unfortunately, a thorough QS-9000 FMEA requires the review of each system component and subcomponent. This "bolt-by-bolt" approach is extremely laborious and can quickly exceed available resources.

Combining the Strengths of HazOp & FMEA

Historically, certain groups within Motorola's environmental health and safety (EHS) and facilities organizations have used both HazOp and FMEA methods with varying degrees of success. As EHS moved toward a risk-based approach for decision making and as the importance of facility support systems' reliability grew, both organizations were looking for techniques that would improve the quality of these studies.

It was also observed during several FMEA studies that the review team struggled with the basic concept of failure mode identification. The typical component-by-component review takes a considerable amount of time, and teams were becoming frustrated by the fact that most components assessed had minimal, if any, impact on the system. As a result, teams had stopped reviewing certain (sometimes critical) components based solely on the perception that no hazard existed. This led to a "shotgun-type" approach to failure mode identification, as team members selected which components to review based on incident/maintenance history or personal experience. Clearly, a structured approach to system evaluation was needed.

The authors' experience with HazOp led to the idea of marrying its systematic and deductive reasoning process for identifying causes of expected consequences to FMEA's inductive reasoning process for selection of detection and response systems and relative risk ranking (Venugopal). Documentation of typical HazOp and FMEA studies was reviewed, and with slight modification of the QS-9000-based FMEA spreadsheet, a documentation scheme was developed that captured results from the HazOp-type failure mode identification method and kept the risk scoring and prioritization method used in FMEA.

This combined methodology has proven to be particularly well-suited to continuous, near-instantaneous delivery processes (e.g., most utilities, electrical power, deionized water, air handling, bulk gases and wastewater treatment systems); it is also able to identify virtually all potential failure modes prior to operation. This allows the review team to ensure that the process design can effectively detect actual or incipient failures and can either prevent those failures or mitigate the consequences.

Figure 3

Motorola's HazOp/FMEA Methodology Worksheet

FMEA WORKSHEET

Issue: 0

PROJECT TITLE _____ **Control Number/Issue:** _____

FMEA Type: _ Design _ System **Company,Group,Site/Business Unit:** _____

Prepared By: _____ date _____ (Rev.)

Core Team:

Process Function/ Requirements (Hazop Node / Item)	Potential Failure Mode (Hazop Deviation)	Potential Effect(s) of Failure (Hazop Consequences)	SEV	Potential Cause(s)/ Mechanisms (Hazop Causes)	OCC	Current Design/ Process Controls	DET	RPN	Recommended Action(s)	SEV	OCC	DET	RPN

HazOp & FMEA Risk Assessment Methodology

As a component of risk management, risk assessment involves several steps, generally described as system definition, hazard identification, risk estimation, and risk evaluation and reduction. The HazOp/FMEA technique incorporates all of these steps, allowing risk reduction in a process design.

The starting point for a HazOp/FMEA is obtaining a complete set of the piping and instrumentation diagrams or electrical diagrams. Having a design with preliminary acceptance from all stakeholders (e.g., process, electrical, mechanical, safety and environmental engineering) helps the facilitator keep the team focused on evaluating failure modes, their effects and the appropriateness of detections rather than on trying to re-engineer the design. Preliminary design reviews are useful in identifying any gross weaknesses in the design, but the final analysis should be delayed until the design is complete.

System Definition

The challenge of evaluating a complex piping diagram can be overcome by dividing the system into manageable sections. These are typically called "nodes" for the purpose of the assessment. Nodes are sections of the design that have definite boundaries, such as line sections between major pieces of equipment, tanks, pumps, etc. In addition, the operating mode for each node must be defined because the effect of a component failure during startup, for example, may be vastly different from the consequences of its failure during normal operation.

Hazard Identification

The power of HazOp lies in systematically identifying failure modes through consideration of potential process deviations. HazOp uses process parameters and guideword pairs to describe possible process deviations. Figure 2 is a matrix of typical HazOp guidewords (e.g., no, low, high) and process parameters (e.g., flow, level, pH). For each meaningful pairing of guideword and parameter, a definition is provided in the matrix to ensure common usage.

For each node, all applicable HazOp deviations are noted on the HazOp/FMEA methodology worksheet; these are shown in Figure 3 as a "potential failure mode." Each deviation is then reviewed to determine resulting consequences (with little regard for plausibility), which are logged on the worksheet as "potential effect(s) of failure." For each effect, hereafter called consequence, all envisionable causes are deduced and logged on the form under "potential cause(s)/mechanisms." This procedure allows the team to assess the risks of an array of possible cause-consequence pairs, not simply the worst-case or most credible case cause-consequence. In fact, these HazOp/FMEA results can be used for "risk profiling," in which the percentage of total process risk is determined for each cause-consequence pair, system component or node.

For each cause-consequence pair, the systems and/or procedures that are intended to reduce the potential effect(s) of failure or potential cause(s)/mechanisms are identified and listed in the "current design/process controls" column on the worksheet. When assessing a process using guideword pairs, it is important to consider all possible operating scenarios for variable-state processes—such as the pH adjustment process in a wastewater treatment system—to ensure that detections are in place for enabling events at the extremes of normal operation.

Risk Estimation

The next step in the FMEA evaluation is to rate the severity, occurrence and detection of the potential

Figure 4

Motorola's FMEA Scoring Chart

SCORE	Severity Severity is a rating corresponding to the seriousness of an effect of the potential failure mode. [IN THE ABSENCE OF DETECTION] EHS	Severity Facilities	Occurrence Occurrence is an evaluation of the rate at which a first level cause and the failure mode will occur, with standard preventive maintenance. [1,2,3,4] [IN THE ABSENCE OF DETECTION]	Detection - Process Detection is a rating of the likelihood that the current controls will predict/detect the failure mode and respond to lessen/prevent the consequence. [2,5,6]	Detection - Procedure Detection is a rating of the likelihood that the current controls will predict/detect the failure mode and respond to lessen/prevent the consequence. [7]
1	No effect on people. No regulatory compliance impacts.	No production impact. Process utility in spec. System or equipment or operations failures can be corrected after an extended period.	Failure barely plausible <1 x 10^{-6} events/hour (1 event in more than 100 years)	Redesign of process eliminating hazard. Rescore RPN for new hazard. *Example: Replacing toxic process chemical with non-toxic chemical.*	Elimination of human based process. *Example: Replace procedure with automated process (which should be separately assessed for risk).*
2	People will probably not notice the failure. Nuisance effects.	No production impact. Process utility in spec. System or equipment or operations failure can be corrected at next scheduled maintenance.	Failure unlikely in similar processes or products. No industry history of failure. >1x10^{-6} events/hour (1 event in 100 years)	Automatic controls highly likely to predict a failure mode and initiate automatic response, preventing the failure mode. *Example: Pressure sensor modifies process conditions to prevent overpressure that would have caused leak.*	Control and release of hazardous energy, with written procedure and independent verification. *Example: Block and bleed of high pressure fluid pipeline, with written procedures and supervisor inspection.*
3	Minor short term irritation effects to people. Moderate, short term non-compliance.	No production impact. Process utility in spec. Equipment or operations failures to be corrected ASAP.	Remote chance of failures. Some industry history. (1 event every couple of decades)	Automatic controls likely to predict a failure mode and initiate manual response, preventing the failure mode. *Example: Pressure sensor activates alarm initiating prepared response plan to prevent overpressure that would have caused leak.*	Control of hazardous energy, with written procedure and independent verification. *Example: Block of high pressure fluid pipeline, with supervisor inspection.*
4	Moderate short term irritation effects to people. Moderate, short term non-compliance.	No production impact. Process utility in spec. Equipment or operations failures to be corrected immediately.	Very few failures likely. >1x10^{-5} events/hour (1 event in 10 years)	Automatic controls likely to detect the failure mode and initiate automatic response, preventing the consequence. *Example: Redundant pH probe in wastewater treatment system, preventing out of control reagent feed.*	Control and release of hazardous energy with written procedures and without independent verification. *Example: Block and bleed of high pressure fluid pipeline, without supervisor verification.*
5	Moderate extended irritation effects to people or environment. Medical intervention needed. Moderate extended non-compliance. Notice of violation (NOV) unlikely.	No production impact. Process utility out of spec. No tool impact. No product scrap.	Few failures likely. Some company history. (1 event every few years)	Manual controls likely to predict the failure mode and initiate manual response, preventing the consequence. *Example: Routine inspection based parametric monitoring program with defined repair program.*	Control of hazardous energy, with written procedure and without independent verification. *Example: Block of high pressure fluid pipeline, without supervisor inspection.*
6	Moderate extended irritation effects to people or environment. Medical intervention needed. Moderate extended non-compliance. NOV likely.	Localized production impact confirmed or likely. Critical process utility out of spec. One or more production tools impacted. Possible product scrap.	Occasional failures. >1x10^{-4} events/hour (1 event per year)	Automatic controls likely to detect the failure mode and initiate automatic response, lessening the consequence. *Example: Ambient air gas sensor activating process shutdown, thereby minimizing leak.*	Cell left blank intentionally to clarify the safety gap between tasks performed with control of hazardous energy and those without control of hazardous energy.
7	Significant but self-recovering effects to people or environment. Moderate extended non-compliance. NOV certain.	Widespread production outage <8 hrs. Critical process utility outage <4hrs or severely out of spec <4 hrs. Product scrap likely.	Moderate number of failures. (1 event every few months)	Automatic controls likely to detect the failure mode and initiate manual response, lessening the consequence. *Example: Exterior leak sensor activates alarm initiating prepared response plan to limit volume of leak.*	No control of hazardous energy, with written procedures and independent oversight. *Example: Electrical hot-work with partner.*
8	Significant but remediable effects to people or environment. Significant long term non-compliance NOV and media attention certain.	Widespread production outage <24 hrs. Critical process utility outage 4-12 hrs or severely out of spec 4-12 hrs. Substantial product scrap likely.	Frequent failures likely. >1x10^{-3} events/hour (1 event every 1.5 months)	Manual controls fairly likely to detect the failure mode and initiate manual response, lessening the consequence. *Example: Routine inspections, with parametric monitoring, with defined measurement thresholds requiring repair.*	No control of hazardous energy, with written procedures and without oversight. *Example: Electrical hot-work without partner.*
9	Probably major injury to people or environment. Regulatory action including fines and process shutdown likely.	Widespread production outage < 48 hrs. Critical process utility outage 12-24 hrs. or moderate contamination of cleanroom or process utility. Substantial product scrap likely.	High number of failures. (1 event every few weeks)	Manual controls might randomly detect failure mode and initiate manual response, lessening the consequence. *Example: Routine walk-by inspections, without parametric monitoring, with defined observed conditions requiring repair.*	Control of hazardous energy, without written procedure.
10	Probably severe injury to people or environment. Regulatory action including fines and process shutdown certain.	Widespread production outage >48 hrs. Critical process utility outage>24 hrs or severe contamination of cleanroom or process utility. Substantial product scrap likely.	Failure certain to occur in near future. >1x10^{-2} events/hour (2 or more events per week)	Controls unlikely to detect the failure mode. *Example: Device fails silent or device not routinely inspected/observed.*	No control of hazardous energy and no written procedures.

1. Failure rates are assumed to apply to continuous processes. Intermittent equipment operational failure rates may be higher due to start up failure, failure to operate at specification, and/or human error.
2. Controls involving design "hardening" (such as stronger materials of construction) are equivalent to QS9000 Type 1 controls and thereby modify Occurrence.
3. If industry average failure rates used and preventive maintenance is less frequent that manufacturer's recommendation, add 1 to Occurrence score.
4. If industry average failure rate used and proven predictive maintenance is utilized, subtract 1 from Occurrence score.
5. Controls that only detect consequence rate a 10 for detection.
6. The reliability of automatic systems and manual procedures is assumed very high. Otherwise, these systems should be assessed separately.
7. The term "hazardous energy" is intended to represent any hazard, including electrical, hydraulic, mechanical (e.g. sharp edge), radiation, chemical, etc.

Cell Color Key:

- Inherently safer design/passive controls.
- Highest order active controls.
- Generally adequate active controls.
- Human based active controls.
- No controls.

effect(s) of failure, potential cause(s)/mechanisms and current design/process controls, respectively. The following definitions are used for the risk estimation elements:

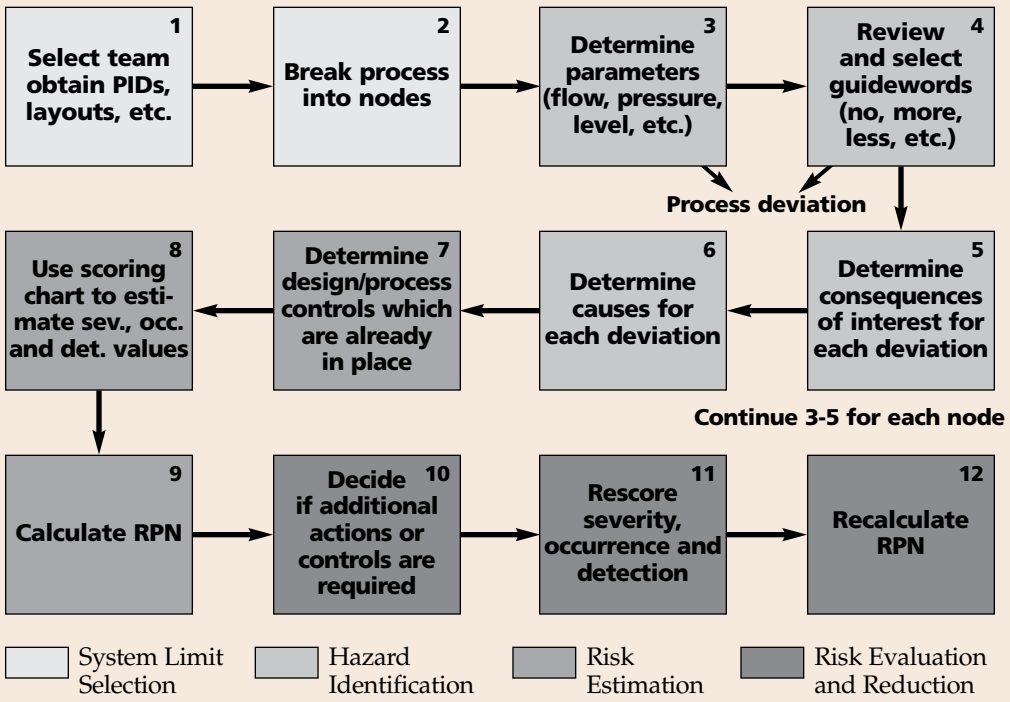
Severity: A rating that corresponds to the seriousness of an effect of the potential failure mode, in the absence of any controls.

Occurrence: An evaluation of the rate at which a potential cause will occur in the absence of controls.

Detection: A rating of the likelihood that the current controls will detect and contain or prevent the failure mode (by either preventing the cause or minimizing or preventing the consequence) before it affects persons, the process or the facility.

Figure 5

Hazop/FMEA Process Flow



All cause-consequence pairs for each node of the diagram are evaluated, then rated using the FMEA method. The severity of the potential effect(s) of failure, the occurrence of the potential cause(s)/mechanisms and the detection of the current design/process controls are ranked by the cross-functional FMEA team. A typical ranking scale is integer values from 1 to 10.

Each risk estimation element is rated and multiplied together. The risk priority number (RPN) is the product of the severity, occurrence and detection ratings. RPN allows comparison of the relative risk of each cause-consequence pair. Accordingly, for a given facility, the same scoring chart should be used to ensure consistent risk estimation and reduction. Figure 4 shows a scoring chart developed by Motorola for continuous processes.

Development of the FMEA Scoring Chart

Motorola's FMEA scoring chart has been refined over several years of use. Many key concepts are embedded within the various score definitions for severity, occurrence and detection. One concept deserves mention before the rest because it is easily overlooked by the FMEA team. For a given cause-consequence pair, both severity and occurrence are always rated "in the absence of detection." Otherwise, the risk management exercise will not result in consideration of inherently less-hazardous processes, such as a water-based instead of a flammable-solvent-based chemistry, or more reliable components. Thus, the severity rating should reflect the ultimate consequence from the failure mode should all layers of protection—the systems and procedures for prevention (of either the cause or the consequence) and/or minimization (of the consequence)—fail. Similarly, the occurrence rating should reflect the frequency of the cause (initiating event) resulting in these consequences, assuming the same failures (but not as a function of these failures, as that is considered within the detection definitions).

The severity ratings are divided into subcategories of scores for EHS- and facilities-related consequences. Within the EHS scores, separate considerations are given for increasingly undesirable consequences for personnel injury, environmental damage, negative publicity and regulatory action, including fines and process closure. Within the facilities scores, separate considerations are given for increasingly undesirable consequences related to product damage, process interruption, facility damage and support utilities outage.

Occurrence ratings are defined so that two scoring blocks span approximately an order of magnitude difference in frequency. The parenthetical explanations of the time between events have been "rounded" slightly to result in conventional periods that FMEA team members can easily comprehend and use.

Like the severity ratings, the detection ratings have also been divided, except two separate headings are used instead of one heading and two subcategories. This segregation of "detection-process" and "detection-procedure" was made to clarify that generally for design risk assessments of engineered systems only the detection-process definitions should be necessary. For design risk assessments, the detection-procedure will be needed only occasionally—when human interface is inseparable from the process operation (which in these days of automation has become less desirable and common). Detection-procedure ratings will find use more commonly for engineered systems when failure events

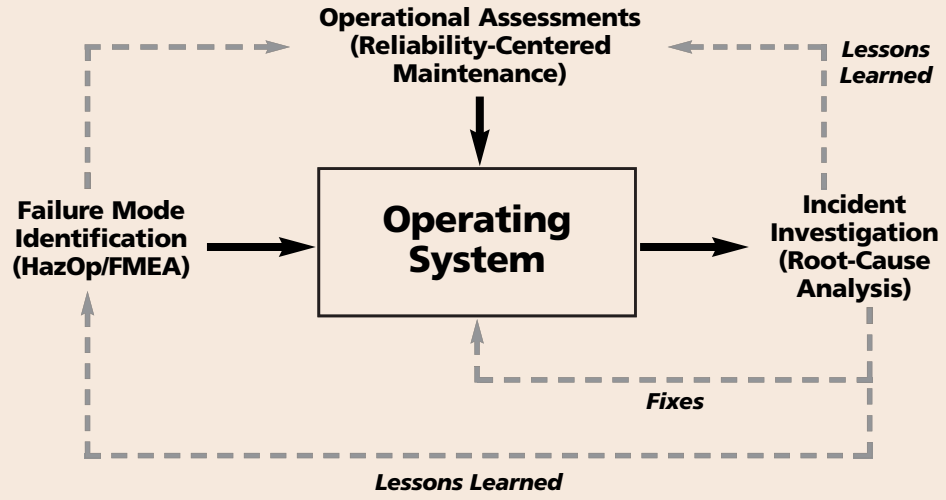
are reviewed through such techniques as incident diagnostics and root-cause analysis, because human error is commonly a contributor to process failure. The detection-process rating definitions incorporate the perspectives that it is better to prevent the failure mode than to prevent or minimize the consequence, and that automated systems are generally more reliable than manual, human-based ones.

Detection-procedure ratings are also useful when assessing the robustness of personnel systems through job safety analyses (JSAs) or accident investigations. An embedded concept in these ratings is that no credit is given for any procedure that is not written. (An explicit assumption buried within the terminologies of these ratings is that written procedures incorporate competent training with skills demonstration.) Also, any procedure performed with the hazard present (such as energized electrical work) is considered inherently more dangerous and thereby cannot score better than a 7 for detection. Reducing detection below 6 requires the use of hazard control and/or removal. (The definitions use the terms "control" and "release," which are meant to correspond to the commonly understood concepts of block and bleed used for pressurized fluids and lockout and deenergize for electricity.)

Seven additional notes are provided in the FMEA rating scales, corresponding to specific considerations when determining occurrence and detection. Notes 2 and 5 are intended to address concepts that often result in FMEA team confusion. The second note clarifies that design hardening is equivalent to process redesign (see detection-process score 1 definition) and, therefore, will modify the occurrence rating. The fifth note clarifies that detection of the consequence inherently provides no reduction in its severity or frequency and, thereby, rates a detection score of 10. The key words are "detection of the consequence." Thus, detection of a blackout after transformer failure rates a detection score of 10, but detection of transformer oil degradation—which could lead to a transformer failure and blackout—might rate a detection score of 4.

Figure 6

Risk Management Model: Engineered Systems



Risk Evaluation & Reduction

RPN values should be used to rank order the cause-consequence pairs in the process in Pareto fashion. Corrective action should be proposed for those pairs with an RPN above an acceptability threshold. QS-9000 sets this threshold at 150, but this number may be reduced when time and budget allow, or exceeded when the cost of additional detection is disproportionate to the level of risk reduction achieved. The effect of the proposed corrective actions can be reevaluated for severity, occurrence and detection, with the resulting RPN noted in the FMEA worksheet. In this manner, FMEA is an iterative process that can be used to reduce engineered system risks.

Changes to process design typically lower the severity rating, while changes to more reliable system components lower the occurrence rating. Changes to controls only lower the detection rating because, by definition, severity and occurrence are both rated in the absence of controls. Also, sensors that generate electrical signals and solid-state/software-based controls, especially those that can be modified by the user, may require a separate reliability assessment to ensure that a low detection rating is merited.

Occasionally, recommended corrective actions result in significant modifications to the original process design. In these cases, it should be determined whether the HazOp/FMEA procedure should be repeated for the affected nodes. Figure 5 is a simplified flow diagram of the HazOp/FMEA process.

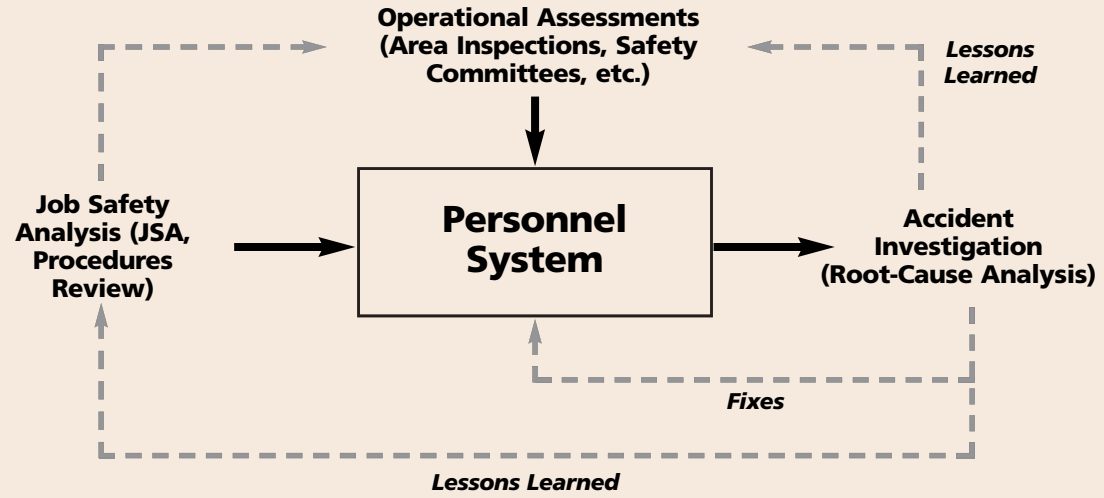
Use of a risk assessment technique for process design improvement, no matter how robust, does not guarantee that risk assessment recommendations will be implemented. Therefore, procedures must be developed to track implementation of these recommendations as the process is being constructed. Records should be kept of both implementation results of recommendations and reasons why recommendations were not implemented.

Selecting Appropriate Detections

In theory, once target RPN has been achieved for a specific cause-consequence pair, detections are judged

Figure 7

Risk Management Model: Personnel Systems



appropriate (or will be appropriate after resolution of the recommendations). Note that detections evaluated and scored per the RPN scoring chart definitions are considered to be independent protection layers (IPLs). The HazOp/FMEA scoring approach also only credits the best detection or control, and does not consider the benefit of multiple layers of protection.

For example, a temperature sensor may regulate the flow of cooling water to a critical device and sound an alarm if the temperature gets too high. Additionally, an in-line flow sensor will activate a separate alarm if flow falls below a predetermined setting. If the analysis team is considering detections for a no- or low-flow scenario, two independent levels of protection exist, for which the HazOp/FMEA will only provide consideration of the best or most-reliable device (either the temperature sensor or the flow sensor). For such a scenario, and especially for situations where consequences are estimated to be severe, a more-detailed analysis of the protection layer itself is needed. Such an assessment is especially important for systems that incorporate software-based control logic, such as a basic process control system, for which the potential for human errors and common-cause failures is high. Sophisticated tools such as fault tree analysis may be used for this purpose, but their widespread use would require more resources than are typically available.

A new tool, called layer of protection analysis (LOPA) can be used to provide sufficient information for decision making (in most cases) with relatively low resource requirements (Bridges). The concepts of LOPA are to 1) identify those detections (protections) that are truly independent of the cause and each other; and 2) score those IPLs on a predetermined, simplified scale. This separate assessment of the detection for selected cause-consequence pairs helps ensure that the team does not overlook critical weaknesses and underestimate RPN. It is also valuable in ensuring consistent risk judgments within and among analysis teams across the organization.

Obviously, only those devices, systems or actions that could effectively detect or mitigate the undesired event are candidate protection layers. However, to qualify as an IPL, the device, system or action must in no way cause an undesired event (e.g., a temperature sensor fails low, results in an overheating condition and fails to sound the alarm) nor can its effectiveness be adversely affected by the event's cause or consequences (e.g., a fire preventing human access to the fire extinguisher). Furthermore, the IPL cannot be adversely affected by the failure of any component or action of any other IPL credited for the same scenario. Thus, if the same smoke alarm should trigger an automatic ventilation shutdown and sound an alarm to trigger a manual ventilation shutdown, only one IPL would be credited, not two.

Once the candidate list of detections has been pared down to the IPLs, the effectiveness of each IPL must be scored. A key simplification of the LOPA approach is the use of a standard scale for scoring IPLs, regardless of their specific details. (Analysts who want to account for other factors may do so, but they must use a different method such as fault tree or event tree analysis. A detailed discussion of the development of IPL scoring scales can be found in Bridges's *Layer of Protection Analysis: Simplified Process Risk Assessment*.)

When performing LOPA, the team must consider all possible operating scenarios, not just steady-state conditions, to ensure that appropriate detections are in place for special situations, such as startup, shutdown or maintenance, when normal detections may be shut down or bypassed.

Risk Management of Engineered & Personnel Systems

It is vital to understand the limits of the application of the HazOp/FMEA as a risk management tool for both engineered systems and personnel systems. Risks associated with engineered systems should be assessed and managed as shown in Figure 6. After the process is constructed per the results of the risk assessment design review, an effective management of change system should be implemented, incorporating routine maintenance, assessments of risk due to changes in human procedures, process components or reagents and/or process steps, and a program to learn from incidents (Burns).

Risks related to human interface with the process, whether during normal operation or maintenance, should be assessed using techniques such as JSA, and managed as shown in Figure 7. Typically, a JSA developed by a cross-functional team that includes those performing the operation or maintenance results in effective administrative procedures for personnel (as opposed to engineered systems) risk management. However, should a JSA result in a proposed process modification, then the HazOp/FMEA should be repeated for the affected nodes.

Resources & Lessons Learned

For any risk management strategy to be successful, including the introduction and application of an effective and structured assessment methodology, adequate resources must be applied. In addition to knowledgeable analysts who can efficiently lead the assessment team, time and resources must be allowed in advance to carefully choose the appropriate methodology, determine how competing risks will be prioritized and gather appropriate supporting materials. In advance of any assessment effort, the management team should determine acceptable risk levels that correspond with the organization's risk tolerances. Once this risk tolerance level is established, the definitions within the chosen scoring chart can be determined and adjusted appropriately.

This is not a simple exercise. Establishing companywide tolerable risk levels that have across-the-board buy-in may take many months. Typically, the risk scoring schemes (and hence the tolerable risk levels) will constantly be adjusted as more and more risk scenarios are evaluated and scored. It is important to ensure that all analysis teams are always using the most current scoring chart, and that the facilitators (at least) are aware of its change history.

In addition, adequate personnel resources must be applied to the analysis effort for the assessment to be successful. A typical assessment team will include a facilitator and scribe, both of whom are familiar with the analysis methodology; process engineers and technologists who are experts in the intended outcomes of the system; maintenance and operations specialists who will lend a "real world" view of system operation; and compliance specialists such as environmental or SH&E engineers who can help determine regulatory impacts of the consequences from uncovered failure modes.

Rigid documentation and follow-up of action items or recommendations is an often-overlooked aspect of the analysis effort. Regardless of the level of effort applied to the planning and execution of the risk assessment, no degree of risk reduction can be realized if corrective actions are not applied. In fact, a false sense of security may result if members of the analysis team who were instrumental in the discovery of credible failure modes come away from the meetings expecting these weaknesses to be corrected, but they are never acted upon. A designated individual should be assigned to monitor the progress of agreed-upon corrective actions, and have the responsibility and authority to escalate nonaction to higher levels of management.

Conclusion

The HazOp portion of this method allows for easy selection of system limits and hazard identification, while the FMEA portion results in effective risk estimation and evaluation. Adding LOPA to specifically evaluate and quantify existing or proposed IPLs helps ensure that appropriate controls are identified. While the analysis method could be applied separately to EHS and system reliability evaluation efforts, it is evident that much commonality exists. Thus, significant personnel time savings and synergistic design improvements have been realized by combining EHS and process reliability assessments. Furthermore, this powerful, integrated approach to system risk assessment helps ensure that appropriate controls are implemented to consistently manage risk at a tolerable level across the facility, site and organization. ■

References

Automotive Industry Action Group (AIAG)/American Society for Quality Control. *Potential Failure Mode and Effects Analysis (FMEA) Reference Manual.* 2nd ed. Southfield, MI: AIAG, Feb. 1995.

Bridges, W. *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: American Institute of Chemical Engineers, Center for Chemical Process Safety, 2001.

Burns, J.M. "The Role of Incident Reporting and Response in Product Stewardship: What Comes Before and After a Risk Assessment." *Proceedings of the Semiconductor Environmental Safety and Health Assn. Symposium.* McLean, VA: SESHA, April 2001.

Dowell, A.M. III(a). "Layer of Protection Analysis: A New PHA Tool, After HazOp, Before Fault Tree." International Conference and Workshop on Risk Analysis in Process Safety. Atlanta: 1997, 13-28.

Dowell, A.M. III(b). "Layer of Protection Analysis: A Worked Distillation Example." ISA Tech/1999, Philadelphia. Research Triangle Park, NC: Instrument Society of America, 1999.

Manuele, F.A. *On The Practice of Safety.* 2nd ed. New York: Van Nostrand Reinhold, 1997.

Sutton, I.S. *Process Reliability and Risk Management.* New York: Van Nostrand Reinhold, 1992.

Venugopal, B. "Minimizing the Risk of Thermal Runaways." *Chemical Engineering.* June 2002.