Using a Modified Hazop/FMEA Methodology for Assessing System Risk

By
Steven R. Trammell, Ronald D. Wright and Brett J. Davis
Motorola, Semiconductor Products Sector
6501 William Cannon Drive West
Austin, TX 78735-8598
512.895.2380
steve.trammell@motorola.com

Abstract

As semiconductor manufacturing processes become more complex and the costs associated with manufacturing line downtime soar, the reliability of the supporting systems have become a major area of focus. Preventive and predictive maintenance, real time system status monitoring, and periodic inspections are typical methods used to help reduce unexpected system failures. Although these methods are proactive, they are typically applied on the basis of perceived risk or solely on the historical perspective of the designer or owner. Utilization of a robust and flexible system risk assessment method early in the design phase is a highly effective approach to increasing system up time and identifying design weaknesses. This paper will present a risk assessment approach based on strengths of both Hazard and Operability Study (Hazop), and Failure Mode and Effects Analysis (FMEA) methodologies.

Reasons to Use Risk Assessment

Many regulatory programs and customer quality and environmental management expectations have been the impetus for Motorola to institute risk management processes utilizing both qualitative and quantitative risk assessment techniques. As briefly described below, in some cases the regulator or customer has prescribed the risk assessment techniques to be used for risk management, while in other cases there is leeway given to select a risk assessment technique of choice.

Motorola's experience in the implementation of these risk management activities has demonstrated the synergistic benefits from cross-functional risk assessments of process designs and modifications. Participation by environmental and safety compliance, operations, maintenance and engineering functions allows for risks to be properly ranked and for agreement on acceptable levels of residual risk. We have founded a risk assessment "core team" that facilitates and keeps records of many of the required risk assessments as well as those initiated by Motorola for process quality assurance and control. For these latter assessments, the core team has developed a risk assessment technique that is tailored to effective analysis of a wide range of our processes. The team also keeps the formal records of risk assessments, ensuring the tracking of best practices and lessons learned.

Regulatory Required Risk Assessments

The United States Environmental Protection Agency's (EPA) Risk Management Program (RMP) prescribes a risk assessment methodology for listed substances above an established storage quantity threshold. Risk is determined by calculating the "populations potentially affected" by worst and alternative case releases of gases and vapors. In this risk assessment, risk is essentially equated to consequence alone. Likelihood is not quantified, but the program attempts to reduce it by mandating the development of release prevention and response plans.

The United States Occupational, Safety and Health Administration's (OSHA) Process Safety Management (PSM) program requires risk assessments, known as hazard analyses, for listed substances above an established storage quantity threshold. A variety of risk assessment methodologies are identified as acceptable under the standard, including Hazop and FMEA. In addition, the program calls for written procedures for management of change. While Motorola does not have any above threshold processes for either the RMP or PSM programs, we have accepted our responsibilities under the General Duty Clause of the RMP program to perform risk assessments on a variety of hazardous chemicals and wastes, stored in quantities below the RMP and PSM thresholds. OSHA's Voluntary Protection Program requires Job Safety Analyses (JSA) be performed to ensure that safety is considered in the development of operational procedures. At Motorola we perform JSAs to identify hazards and develop procedures or physical system changes required to perform tasks safety. JSAs are also used to comply with OSHA regulations (29 CFR 1910.132) requiring employers to base selection of personal protective equipment on a hazard assessment of the subject work process.

The Uniform Fire Code (UFC) allows the chief to authorize "alternate materials and methods" that comply with the "intent of the code" (1997 UFC 103.1.2). The Austin Fire Department (AFD) encourages the use of quantitative risk to compare the level of risk provided by code compliant design and an alternative. Motorola has used Fault Tree Analyses (FTA) to accomplish this comparison and successfully demonstrate that an alternative design is safer than that prescribed by the UFC. AFD has recently implemented a "distinct hazard" policy prohibiting bulk chemical storage operations that represent a risk exceeding 1.4×10^{-6} exposed persons per year. This risk equates to the generally accepted risk from underground storage at a gasoline station. The risk calculation is a function of consequence determined using a gas dispersion model and population density, and probability of component failure and fire, using established component failure rates and fire rates based upon AFD experience. Motorola has developed a spreadsheet that allows an assessment of whether or not any proposed bulk chemical system will be designated as a distinct hazard, in which case risk reduction strategies are employed typically to reduce the likelihood of release.

Customer Required Risk Assessments

ANSI/ISO 14001-1996 requires an annual analysis of potential impacts from "environmental aspects" of an operation for the determination of environmental objectives. At Motorola, ranking the impacts using a quantitative risk assessment methodology prescribed in a Management Systems (MS) document enhances this analysis. Action items are assigned to environmental staff to reduce the severity and/or likelihood of any impacts above an acceptability threshold established in the MS document. In addition, formal and informal processes are in place to identify pending process changes requiring risk management.

Motorola's semiconductor manufacturing operations are required to be QS 9000 certified by our automotive industry customers. The QS system mandates management of change to minimize impact to product quality. At Motorola, this objective is accomplished by performing an FMEA risk assessment on all new or modified processes, including environmental and safety systems.

Motorola Required Risk Assessments

Motorola requires that all semiconductor manufacturing equipment that it purchases be compliant with Semiconductor Equipment and Materials International (SEMI) Safety Guideline S2, Environmental, Health and Safety Guideline for Semiconductor Manufacturing Equipment which establishes a risk assessment requirement for a variety of hazards posed by such equipment. The technique to be used for these risk assessments, in which hazards are ranked to determine which are acceptable and which require further mitigation, is prescribed in SEMI S10, Safety Guideline for Risk Assessment.

And finally, for quality assurance of new processes and quality control of process modifications, Motorola has developed a hybridized Hazop and FMEA technique that is the primary focus of this paper. The risk prioritization method developed for this technique allows separate consideration of risks to human safety, the environment, facility or product damage and business interruption. Because of this multiple functionality, this hybrid Hazop/FMEA technique has been well accepted by the Environmental, Health and Safety, Facilities Operations, Maintenance and Engineering, and Manufacturing Operations functions. Process designs are no longer considered complete until a thorough Hazop/FMEA has been performed.

Development of the Hazop + FMEA Methodology

The purpose of developing a risk assessment methodology is to provide a systematic method to thoroughly review failure modes of complex, interacting system components, and the effects of failures on the overall system. Required within the methodology is the requirement and ability to review effects on safety of personnel, the facility and/or infrastructure, and on the manufacturing process (ability to manufacture good product). The addition of the business interruption review element was a logical evolution of the methodology. Although the analysis method could be applied to individual EHS and system reliability evaluation efforts, it is clearly evident that much commonality exists, both in review team members and solution development when reviewing overall effects

of failure events. Accordingly, we realize significant efficiencies when combining EHS and reliability assessments with regard to utilization of personnel resources.

Methodologies

Several risk assessment methodologies are used within Motorola. The Hazop and the FMEA are most common, although Fault Tree Analysis has been used for specific assessment efforts involving fire and building code alternative method submittals. Hazop has historically been used as a general risk assessment technique on systems to evaluate potential hazards mainly to personnel and the environment. This method is favored by many of our design consultants because of its relative ease of use, ability to draw on diverse expertise and proven track record in the chemical processing industry. Many of the risk assessments performed by third party evaluators on purchased equipment or packaged chemical delivery systems are of the Hazop type. The FMEA is the method of choice for the Reliability and Quality Assurance (R&QA) organizations within Motorola. Although used mainly for evaluations in the product design phase, process systems and some support systems within the manufacturing envelope have also been subject to FMEA. The primary driver for use of this methodology within R&QA is the requirements set by QS9000. All of our automotive customers require Motorola to comply with the methods within QS9000, including the requirement to systematically review a system for failure modes.[1] Although FMEA is not mandated, it is the method most preferred by the customer.

Strengths and Weaknesses

Hazop is a mature methodology, with system failure mode identification as its strength. By dividing complex systems into smaller more manageable "nodes" for study, and the systematic identification of process parameter deviations, makes for a thorough identification of system failure modes. However, a typical Hazop is not strong or necessarily effective in prioritization of effects of the failures. Also, a Hazop usually does not study the relative effectiveness of identified corrective actions. On the other hand, the QS9000 based FMEA method contains a thorough, semi-quantitative evaluation of effects of failure modes. By studying and scoring based on severity, occurrence and detection attributes, the team gains a through understanding of the failure mechanism, and more importantly, insight on determining truly effective corrective actions. The FMEA method also assisting in prioritizing failure mode effects such that resources can be applied more effectively. Conversely, the FMEA is relatively weak in failure mode identification, as it does not provide a systematic method of evaluating system deviations (other than reviewing every individual component and subcomponent of a system). This "bolt-by-bolt" approach is extremely laborious and can become an extreme challenge to the long-term efficiency of the study team.

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 towards a risk-based approach for decision making

[1] "Potential Failure Mode and Effects Analysis (FMEA) Reference Manual" ASQC/AIAG, Second Edition, Feb.1995.

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 a number of FMEA studies, that the review team struggled with the basic concept of failure mode identification. The typical component-by-component review was taking a considerable amount of time, and the teams were becoming frustrated with the fact that the majority of components assessed had minimal if any impact on the system. Soon the teams were skipping review of certain; sometimes potentially critical components based solely on the perception that no potential hazard existed. This led to a "shotgun" type approach to failure mode identification as the team members picked system components to review based on personal history or experience. It was clear that a structured approach to system evaluation was needed. Our experience with Hazop lead to the idea that if the failure mode identification method utilizing the concept of deviations from known or expected process parameters could be married to the strong scoring mechanism of the FMEA, the overall methodology could be improved. Documentation of typical Hazop and FMEA studies were reviewed, and with slight modification of our QS9000 based FMEA spreadsheet, we were able to develop a documentation scheme which captured results from our Hazop-type failure mode identification method, while keeping the risk scoring and prioritization method used in the FMEA.

Hazop and FMEA Methodology

The starting point for the Hazop/FMEA process is to obtain a complete set of the piping and instrumentation diagrams. If the design is still in progress, the FMEA should be delayed until the design is complete, because the process review will be a better product if the design package is fairly complete. A key point in the process is for the facilitator to keep the team focused on evaluation of the failure modes and to avoid the tendency to try to "engineer" the corrective actions. Determining improvements to the design have a place in the FMEA process; however, this should take place in an orderly fashion. The FMEA process is more efficient if the role of facilitator and scribe are kept seperated.

The challenge of evaluating a complex piping diagram is overcome by breaking the system into manageable sections. These are typically called nodes for the purposes of the study. Nodes are sections of the design with definite boundaries, such as line sections between major pieces of equipment, tanks, pumps, etc. The power of the Hazop lies in identifying the failure modes through the Hazop deviation. The Hazop utilizes process parameters and guidewords to systematically identify deviations to the system or failure modes. An example of a guidewords and process parameters chart is shown in the following:

Hazop Guidewords	Hazop Process Parameters	
No	Flow	Voltage
Less	Level	Addition
More	pH	Temperature
Part of	Viscosity	Composition
As well as	Mixing	Frequency
Reverse	Pressure	Information
Other than	Time	Separation
	Speed	

Deviations to be evaluated would be “no flow”, “less flow”, “more flow”, “reverse flow”, etc. As these deviations are identified, the Hazop node and the deviation are logged on the worksheet. Hazop deviations are noted on the FMEA worksheet as potential failure modes. Each of these deviations are reviewed to determine the consequences and logged onto the FMEA worksheet as potential Effects failure. The Hazop causes are logged onto the FMEA form as Potential Cause Mechanisms. Note the worksheet in Figure 1.

Hazop/FMEA Methodology Worksheet

MOTOROLA — FMEA WORKSHEET

PROJECT TITLE — Control Number/Issue:

FMEA Type: __Design _ System — Company,Group,Site/Business Unit:

Prepared By: (Rev.)

Core Team:

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

Figure 1

The next step in the FMEA evaluation is the rating of the severity, occurrence and detection of the failure modes and effects. The following definitions are used:

Severity: A rating corresponding to the seriousness of an effect of the potential failure mode.

Occurrence: An evaluation of the rate at which a first level cause and the failure mode will occur.

Detection: A rating of the likelihood that the current controls will detect/contain the failure mode before it affects persons, process or the facility. Each of the nodes of the diagram are evaluated and then rated using the FMEA method. The severity of the “Potential Effect of Failure”, the occurrence of the “Potential Cause 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. A standardized scoring chart should be used to maintain consistency. A typical scoring chart is shown in Figure 2.

Hazop & FMEA Scoring Chart

	Severity **Severity is a rating corresponding to the seriousness of an effect of the potential failure mode.**	**Occurrence** **Occurrence is an evaluation of the rate at which a first level cause and the failure mode will occur.**	**Detection** **Detection is a rating of the likelihood that the current control will detect/contain the failure mode before it affects persons, process or facility.**
1	No effect on people, process or facility (PPF).	Failure unlikely in similar processes or products. No industry history of failure. $\leq 1x10^{-6}$	Reliable detection controls are known with similar processes or products.
2	PPF will probably not notice the failure. Nuisance faults.	Remote chance of failures. $\leq 5x10^{-6}$	History with similar processes or products is available. Controls very likely to detect failure mode.
3	Slight effects. No process down time, < $100 facility damage.	Very few failures likely. $\leq 1x10^{-5}$	Controls highly likely to detect the failure mode. (Highly reliable automatic control)
4	Minor effects. No process downtime, <$1K facility damage.	Few failures likely. $\leq 5x10^{-5}$	Controls likely to detect the failure mode. (Moderately reliable automatic control)
5	Equipment down time. <$100 product loss, <$1000 facility damage.	Occasional failures. $\leq 1x10^{-4}$	Controls might detect the failure mode. (Low reliability automatic control + human-based control backup)
6	Equip. down <8 hrs. Product loss < $1K. Facility damage <$5K.	Moderate number of failures. $\leq 5x10^{-4}$	Low likelihood that controls will detect the failure mode. (Highest reliable human-only based control method).
7	Equip. down <24 hrs. Product loss <$5K. Facility damage <10K.	Frequent failures likely. $\leq 1x10^{-3}$	Slight likelihood that controls will detect failure mode. (Typical human-only based control)
8	Equip. down <72 hrs. Product loss <$10K. Facility damage <25K. Possible minor injury or regulatory investigation.	High number of failures likely. $\leq 5x10^{-3}$	Estimates based upon similar products or processes. Controls unlikely to detect the failure mode.
9	Equip. down <1 week. Product loss <$25K. Facility damage <$50K. Possible major injury or regulatory action.	Failures certain to occur in near future. Some industry history. $\leq 1x10^{-2}$	Estimates based upon similar products or processes. Controls remotely likely to detect the failure mode.
10	Equip. down >1 week. Product loss >$25K. Facility damage >$50K. Possible severe injury or regulatory action will occur.	Certain to occur soon. Significant industry history. $\leq 1x10^{-1}$	Controls are almost certain not to detect the failure mode. No controls are available.

Figure 2

Each of the parameters is ranked and multiplied together. The Risk Priority Number (RPN) is the product of Severity, Occurrence and Detection rankings. The RPN values should be used to rank order the concern in the process in Pareto fashion. The resulting RPNs are evaluated for recommended actions that could reduce the calculated risk through corrective actions. Corrective action should be directed at the highest ranked RPN. Effort should be applied to identify positive corrective actions to minimize risk from the failure mode by eliminating or controlling the potential cause mechanisms. The effect of the recommended actions can be reevaluated for the Severity, Occurrence, and Detection with the resulting RPN noted. Properly applied, the FMEA ranking method is an interactive continuous improvement process that can be used to minimize the system risk.

Conclusion

Multiple assessments using the Hazop+FMEA methodology have been performed to date. In all cases, the diverse teams of EHS, Facilities, Maintenance, Engineering and Manufacturing worked well and efficiently with the method. It was noted that about 15 minutes of method description with simplistic worked samples was enough to orient the team to the method. Within an hour of the meetings, all team members were fully engaged and participating in the review. One key to maximizing effectiveness was the presence of a strong facilitator familiar with the methodology and a dedicated scribe recording the results. Another key to the success of the method is the previous familiarity of most manufacturing personnel to the QS9000 FMEA method. This “automatic” buy in of the scoring criteria resulted in minimal debate on validity of the method.