



Hazards Analysis Guide: A Reference Manual for Analyzing Safety Hazards on Semiconductor Manufacturing Equipment

SEMATECH and the **SEMATECH logo** are registered service marks of SEMATECH, Inc.
International SEMATECH and the **International SEMATECH logo** are registered service marks
of International SEMATECH, Inc., a wholly-owned subsidiary of SEMATECH, Inc.

Product names and company names used in this publication are for identification purposes only
and may be trademarks or service marks of their respective companies.

Hazards Analysis Guide: A Reference Manual for Analyzing Safety Hazards on Semiconductor Manufacturing Equipment

Technology Transfer # 99113846A-ENG

International SEMATECH

November 30, 1999

Abstract: The document provides guidance to key techniques and methods used within the semiconductor industry for identifying and documenting environment, safety, and health (ESH) hazards and their controls. It contains a tutorial that explains how to identify hazards, analyze hazards and controls, document the results of an analysis, and manage residual risk. A hazards checklist and examples of a hazard analysis are included.

Disclaimer:

This reference manual was prepared by the International SEMATECH equipment ESH council ("the Council") as a guide for use by safety engineers and other ESH professionals when conducting a hazards analysis of semiconductor manufacturing equipment. It contains ideas and suggestions provided by ESH professionals within the semiconductor industry for the use of established hazards analysis methodologies and associated protocols, including governmental and SEMI guidelines and standards. It does not claim to be nor is it intended to be a definitive reference guide or set of requirements for the industry.

In developing this manual, the Council attempted to address many key elements of an effective hazards analysis plan; however, specific regulations and code compliance requirements may not have been addressed. In the event of a conflict, compliance with legal and regulatory requirements must take precedence over any suggestions offered by this manual. Hazards analysis professionals and their companies retain responsibility for ensuring that their ESH programs are sound and complete and that they meet regulatory compliance requirements regardless of whether such requirements are addressed herein.

This document is made available "as is" and "where is" without any warranty, express or implied, made by the Council, International SEMATECH, or any member company of International SEMATECH and said parties further specifically disclaim liability for any losses or damages based on the contents of this manual.

Keywords: Equipment Safety, Procedures, Risk Assessment

Author: Mollie Foster, James Beasley, Brett Davis, Paul Kryska, Eddie Liu, Andy McIntyre, Mike Sherman, Brett Stringer, James Wright

Approvals: Mollie Foster, Author
Walter Worth, Program Manager
Steve Burnett, Project Manager
Bob Duffin, Director
Laurie Modrey, Technical Information Transfer Team Leader

Table of Contents

| | | |
|-------|--|----|
| 1 | EXECUTIVE SUMMARY | 1 |
| 2 | TUTORIAL | 1 |
| 2.1 | Hazards Identification | 1 |
| 2.1.1 | Data Collection | 1 |
| 2.1.2 | Hazards Inventory | 4 |
| 2.2 | Hazards Analysis and Controls | 4 |
| 2.2.1 | Define Scope or Boundaries of Analysis | 4 |
| 2.2.2 | Operational Phases | 5 |
| 2.2.3 | Operating Conditions | 5 |
| 2.2.4 | Unmitigated Consequence | 5 |
| 2.2.5 | Key ESH Controls | 6 |
| 2.2.6 | Barriers and Safety Features Against Hazard Propagation | 7 |
| 2.2.7 | Possible Release Mechanisms and/or Failure Mechanisms | 7 |
| 2.2.8 | Consequence of Accident | 7 |
| 2.2.9 | Likelihood of Accident | 8 |
| 2.3 | Documenting the Results | 8 |
| 2.3.1 | Description of the System Analyzed | 9 |
| 2.3.2 | Hazards Analysis Worksheet | 9 |
| 2.4 | Managing Residual Risk | 11 |
| 3 | USING HAZARDS ANALYSIS TECHNIQUES TO SUPPORT THE HAZARD ANALYSIS | 13 |
| 3.1 | "What If" Analysis | 14 |
| 3.1.1 | Assembling the Team | 14 |
| 3.1.2 | Choosing a Facilitator | 14 |
| 3.1.3 | Assembling the Reference Materials | 15 |
| 3.1.4 | Setting the Groundrules | 15 |
| 3.2 | Description of the "What If?" Analysis | 15 |
| 3.2.1 | Alternative Names | 15 |
| 3.2.2 | Purpose: | 16 |
| 3.2.3 | Methodology | 16 |
| 3.2.4 | Applications | 16 |
| 3.2.5 | Thoroughness | 16 |
| 3.2.6 | Mastery Required | 16 |
| 3.2.7 | Difficulty of Applications | 17 |
| 3.2.8 | General Comments | 17 |
| 3.2.9 | What If? Pros and Cons | 17 |
| 3.3 | Failure Modes and Effects Analysis (FMEA) | 21 |
| 3.3.1 | Alternative Names | 21 |
| 3.3.2 | Purpose | 21 |
| 3.3.3 | Method | 21 |
| 3.3.4 | Application | 22 |
| 3.3.5 | Thoroughness | 22 |
| 3.3.6 | Mastery Required | 22 |
| 3.3.7 | General Comments | 22 |

| | | |
|-------|--|----|
| 3.3.8 | FMEA Pros and Cons | 22 |
| 3.3.9 | Applications | 23 |
| 3.4 | Hazard and Operability Analysis (HAZOP)..... | 25 |
| 3.4.1 | Method | 25 |
| 3.4.2 | Helpful Hints..... | 26 |
| 3.5 | Example Hazard and Operability Analysis..... | 28 |
| 3.5.1 | Introduction and Scope | 28 |
| 3.5.2 | Assessment Methodology | 28 |
| 3.5.3 | Hazard Analysis Method..... | 28 |
| 3.5.4 | HAZOP Nodes and Guide Words..... | 29 |
| 3.5.5 | Action Item Determination | 29 |
| 3.5.6 | Summary Documentation | 29 |
| 3.5.7 | Results..... | 29 |
| 3.5.8 | Assessment..... | 29 |
| 4 | REFERENCES..... | 36 |

List of Figures

| | | |
|----------|--|----|
| Figure 1 | ACME Enterprises Super Tool System | 35 |
|----------|--|----|

List of Tables

| | | |
|----------|---|----|
| Table 1 | Sample Hazards Analysis Worksheet | 10 |
| Table 2 | Hazards Checklist | 12 |
| Table 3 | Hazards Analysis Techniques and Associated Information..... | 13 |
| Table 4 | Hazards Analysis Techniques and Associated Applications | 14 |
| Table 5 | Issues Requiring Hazards Analysis..... | 19 |
| Table 6 | Sample FMEA Worksheet | 24 |
| Table 7 | Deviation Guide Word Examples | 27 |
| Table 8 | Action Items Identified in ACME Super Tool HAZOP | 30 |
| Table 9 | Hazard Analysis Participants | 30 |
| Table 10 | HAZOP Summary – Gas Distribution Panel | 31 |

Terms and Definitions

Following are terms and definitions used in this guide. Effort was made to use definitions and terms common to the industry and in the safety arena. The sources of these definitions have been included where possible:

Hazard Analysis — Identifying hazards and characterizing the risks associated with potential mishaps arising out of the hazards.

Note 1: This term is used in the same sense in SEMI 2614d.

Note 2: This term is essentially the same as the term “risk analysis” as used in EN1050 and the 1991 IEC/ISO Guide 51.

Note 3: The process described by this term does *not* include the judgment of whether or not the risk is acceptable, which is considered either as part of the design process or a business decision. This judgment of acceptability of risk is known as “risk evaluation” in 1991 IEC/ISO Guide 51.

Risk Assessment — Determining the probability of a mishap and the severity of the resulting loss or harm.

Note 1: This term is essentially the same as SEMI 2614c’s “risk assessment” and prEN1050’s “risk estimation.”

Note 2: This term is quite different from EN1050’s use of the term “risk assessment.”

The following terms and definitions are taken from SEMI S10-1296:

Hazard — A condition that is a prerequisite to a mishap.

Likelihood — The expected frequency with which a mishap will occur. Usually expressed as a rate (e.g., events per year, per product, per wafer processed).

Mishap — An unplanned event or series of events that results in death, injury, occupational illness, damage to or loss of equipment or property, or environmental damage.

Risk — The expected losses from a mishap, expressed in terms of severity and likelihood.

Severity — The extent of the worst credible loss from a mishap caused by a specific hazard.

The following term and definition is taken from SEMI Document 2697D:

Residual Risk — That risk which remains after engineering, administrative, and work practice controls have been implemented.

1 EXECUTIVE SUMMARY

The key factor that separates the semiconductor industry from most others is the extraordinary rate of change in manufacturing and product technologies. This rate of change far exceeds the rate of change of the various Environmental, Safety & Health (ESH) codes, standards, or guidelines. As a result the semiconductor industry has set an expectation that hazards analysis be performed in supporting several industry guidelines (e.g., SEMI S2, SEMI S8 & SEMI S10, etc.).

The purpose of this reference is to outline key techniques and methods used within the industry for identifying and documenting hazards and their controls. The members of the International SEMATECH Equipment ESH Council have worked together to prepare this *Hazards Analysis Guide* as a tool to industry members, including, equipment manufacturers, third parties, and device manufacturers.

2 TUTORIAL

This section provides an overview of how to

- Identify hazards associated with a system, subsystem, tool, procedure, process, or facility during any phase
- Describe the hazard in terms that clearly state the safety concern
- Qualitatively describe the risk associated with a particular hazard

Specifically, the interrelated components of this overview comprise

1. Hazard identification
2. Hazards analysis and controls
3. Analysis documentation

2.1 Hazards Identification

Hazards identification involves itemizing all hazards associated with the system. By itemizing the list up front, the analyst can quickly formulate a mental picture as to the complexity or breadth of safety issues related to the system. To enhance the list of hazards, a brief description of each hazard should include the following:

1. The hazardous characteristic
2. The form and quantity of the hazard
3. Where and when in the system it is present
4. Under what conditions could the hazard propagate into an undesirable event (i.e., accident)

2.1.1 Data Collection

To properly assess the hazards, the analyst must understand the details of the particular area of concern, including its function, design, and anticipated end user installations. The following describes the best sources of information on a system and things to review.

2.1.1.1 Specifications

In the early phases of a design, functional requirements documents and specifications are likely to provide the most comprehensive source of information. When coupled with interviews of process and hardware engineers (see below), the analyst should be able to form a conceptual image of the tool or process and its operation.

The analyst should also use specifications to identify the basic process performance, hazardous energies, critical components, types of chemicals, and applications of interlocks.

2.1.1.2 Design Reviews

Design reviews provide excellent opportunities to learn about the system during the early development phase. The interactive format allows the analyst to ask further questions about the hazards associated with the system and safety subsystems designed to control those hazards as well as recommend control technologies to ensure proper levels of safety to the development engineers.

Design reviews are also the best method of identifying and addressing safety concerns associated with modifications to design or procedures. If necessary, the analyst should convene the appropriate engineers so that the appropriate questions can be posed and the design evaluated. The primary objective of the design review is to assess progress or audit the following:

1. Compliance with program system safety design requirements, including regulatory, customer, and derived
2. Achievement of system safety design and procedural objectives
3. Adequate identification of potential safety hazards and their appropriate resolution
4. Effects of engineering decisions, changes, and tradeoffs upon system safety engineering requirements
5. Review of current design documentation for compliance with identified system safety engineering requirements
6. Identification of potential safety design or procedural problems affecting personnel safety or the environment
7. Status of supplier product safety engineering activities
8. Status of previously approved design review actions

Since design reviews early in the development phase may lack specific details, the analyst should be looking for the major topics of concern. These can include

- The major tool components and planned control for hazards
- Hazardous electrical/mechanical energies
- Types of chemicals
- Chemical interaction or reaction byproducts
- Physical hazards (radio frequency [RF]/microwave, ultraviolet [UV], SMF, lasers, ionizing radiation [IR], noise, etc.)
- Pressure vessel concerns
- Application of critical components and interlocks
- System/subsystem interface hazards
- Facilitization and/or maintenance/accessibility concerns

2.1.1.3 Drawings and Schematics

As the product development cycle progresses, drawings and schematics are important, by allowing the analyst to review and verify that safety requirements and recommendations are being incorporated. For existing products being modified, drawings and schematics allow the analyst to evaluate the need for additional safety controls required by the introduction of new hardware, change of process, etc. Finally, drawings and schematics record what was analyzed and document system safety controls for future reference.

2.1.1.4 Previous Analyses and Lessons Learned

When preparing a hazards analysis for a product, it is advantageous to jumpstart from previous analyses on similar systems and to use lessons learned. Even for new or dissimilar products, some existing documentation probably can be leveraged for the analysis. The analyst should review past SEMI S2 evaluations, hazards analyses, field service safety issues, and even failure reports.

For new products, the analyst should review previous products that have similar components, have similar hazards, or performed similar tasks or processes. The hazards analyzed in these past documents should be included in the list of hazards for the system under evaluation, as long as they are applicable. Safety design solutions can also be found from previous hazards analyses and an assessment of their success and applicability for the design under evaluation.

Failure reports provide insight into what does not work; if the design was sound, then the reports will provide insight into what can randomly go wrong and what is needed to develop a more robust or fault-tolerant system.

2.1.1.5 Interviews

For mature systems, discussions with individuals currently using the system/components or with field service personnel with extensive experience can also be insightful. These individuals often develop their own set of concerns or observations about a product's shortcomings as well a description of useful features. Operators also can provide a picture of how the tool is actually operated, the thought process that goes into troubleshooting modes, and the typical sequence of events and duration of activities. These insights cannot typically be obtained from the design engineers or maintenance manuals. As the new or modified design matures, analyst participation in multi-disciplinary or cross-functional teams is essential. These teams include professionals from related disciplines, such as the field and maintenance engineers, reliability, manufacturing, technical publications, purchasing, supplier quality, and other product groups.

2.1.1.6 Related Requirements

A basic review of requirements for the system can facilitate later compliance evaluations and target hazards that may require particular focus. All requirements, however, must be interpreted and applied to effectively meet the intent of the requirement. Requirement documents seldom fully explain the intent of any particular requirement. Better understanding can be gained by a thorough hazard analysis. These requirements include the following:

1. Adopted industry consensus guidelines, such as SEMI or ANSI documents
2. Regulatory directives and requirements, such as Occupational Safety and Health Administration (OSHA), Uniform Fire Code (UFC), or Uniform Building Code (UBC)
3. Customer internal requirements, as outlined on the procurement specification

4. Derived requirements, such as from hazards analyses or pertinent to state-of-the-art technology
5. Supplier quality control

2.1.2 Hazards Inventory

This section provides a methodology for identifying and organizing hazards associated with a system, tool or component.

2.1.2.1 Hazardous Energy Sources

One of the primary steps to identifying hazards is to pinpoint all energy sources. This activity leads to the majority of hazards associated with a system. Examples of energy sources include chemical, pressure, flammable materials, electrical, radiation, and moving parts. A more detailed list is provided in the Hazards Checklist (Section 2.4). When describing the energy sources, include a brief title or descriptor, the form, its quantity, and operational phase, if applicable; for example:

- *Electrical energy*: 208 VAC; dry pump, cryopump, heat exchanger, cassette loader

2.1.2.2 Hazards Checklist

Table 2 provides a hazards checklist as a starting point for identifying hazards. Every industry and most safety professionals have their own customized hazards checklist, which is built and modified as necessary to meet the needs of individual analysts. It should never be considered an “absolute” list. Rather, it should be tailored based on experience, new products and designs, and lessons learned. For this reason, users are encouraged to modify and tailor the checklist in Section 2.4. The checklist summarizes the hazards addressed in a particular analysis.

2.2 Hazards Analysis and Controls

Once preliminary information has been gathered and assessed, the hazards analysis activity begins. The purpose of this analysis is to determine if credible means exist, typically through failures, that could result in an incident or other undesirable event. It should be emphasized that hazards analysis considers events and actions both planned and unplanned, including both normal process steps as well as failures associated with equipment, processes, people, and procedures.

2.2.1 Define Scope or Boundaries of Analysis

The scope simply defines which part of a system is being analyzed and the operating phases being considered. Defining what is being reviewed facilitates understanding of what was analyzed. For example, flammable gas supply could cross the boundary of the scope of the analysis since gases are typically provided from the fab gas pad. Therefore, the analyst might define the boundary of the gas system as the point at which the facilities supplied gas is connected to the tool. The interfaces that cross the boundary must be examined for hazards as well. In this example, hazards that must be considered would include excessively high pressure delivery, loss of flow, and possibly wrong gas used or plumbed.

2.2.2 Operational Phases

The presence of hazards often depends upon the operational phase of a tool. Some hazards may appear in several phases but may likewise be absent in others. When identifying and evaluating hazards, it is important to document the applicable phases. A basic list of phases would include the following:

- Installation
- System qualification
- Production
- Standby
- Planned shut down
- Emergency stop and shut down
- Maintenance (preventive and troubleshooting)
- Decommissioning

2.2.3 Operating Conditions

The environmental and end user fab conditions can have an effect on the likelihood of failure and the modes of failure. For equipment located in the benign environment of a cleanroom, environmental conditions generally will not be a factor. However, equipment located in facility chases, in unoccupied basement areas, or in the open may experience degradation related to temperature extremes, humidity, rain, or UV radiation. Corrosive chemicals and chemical reactions are also factors that will affect the safety of semiconductor tools.

The performance of workers will also be impacted by operating conditions. Noise, temperature extremes, and even clothing can degrade performance by diverting their attention or distracting them.

For components, consideration must be given to their suitability for localized temperatures, the chemical environment, and electromagnetic interference.

2.2.4 Unmitigated Consequence

The unmitigated consequence is defined as the worst-case consequence that could occur if the hazard were allowed to be released, or propagated into an accident. The purpose of determining the unmitigated consequence is twofold: (1) to evaluate whether the unmitigated consequence is high enough to warrant some sort of safety response and (2) to establish a baseline consequence against which safety responses can be evaluated.

A couple of examples follow for clarity. If electrical energy were identified as a hazard, the system may have 24, 208 and 480 V sources. Evaluating the 24 V exposures, the analyst would likely determine that even in a worst case—unmitigated exposure of a worker to 24V—the consequences are not sufficiently high to warrant additional safety precautions. For such a hazard, no further analysis would be considered.

For a 480V line, the worst-case exposure would result in death. This consequence provides the baseline by which further analysis is conducted. For this example, the baseline consequence is unacceptable. Therefore, the analyst would determine the consequence and likelihood of accident based on the incorporation of safety features. These safety features then become safety critical

components and tracked as such through evaluation and acceptance. If the unmitigated consequence of a hazard is considered acceptable (i.e., brief exposure to inert gas), then it becomes the residual risk, and no further evaluation of that hazard is conducted.

2.2.5 Key ESH Controls

It is important to understand what existing safety controls and features exist. For new systems, few or no controls may be in place. For systems that are introducing component changes or enhancements, there should be a well documented list of hazard controls and features. Of course, only those controls and features relevant to the system or component being evaluated need to be included.

2.2.5.1 Interlocks

Hardware and software interlocks are intended to interrupt a sequence of events that could lead to an accident. Hardware interlocks are typically electrical or mechanical devices that “fail-safe” in their operation. They are typically used in critical safety applications, primarily to control hazardous energy sources. Software interlocks, while not recognized as “interlocks” by SEMI S2, are often used to interrupt a process before activating a hardware interlock. In this capacity, the hardware interlocks back-up the software interlocks.

Documenting all of the safety interlocks (both hardware and software) helps build the hazard picture for the analyst and reviewers. Describing the interlocks within a table that lists the interlock, the action taken, and the protection provided will allow for easy incorporation into system manuals after the product is released.

2.2.5.2 ESH Design Features

ESH design features can directly or indirectly influence the safety of a system. Design features are items integral to the product that reduce the consequence or likelihood of the hazard propagating into an accident. Features that are factored into the overall safety of a product or tool should be explicitly described and recognized during the hazards analysis. These design features then become part of the safety basis for the product. Examples of safety features include the following:

- Low flow rates for hazardous chemicals
- Small storage containers for chemicals
- Water lines routed below or away from electrical cables and connectors
- Separate manifolds for chemical segregation of incompatibles
- Substitution for robots using less force

2.2.5.3 Regulatory-Based Controls

Regulatory based controls are those features that are required to meet the specific regulations of a customer's government agency or own internal requirements. Although these controls typically enhance the safety of the tool, it should not be assumed that by implementing these regulatory-based controls that the safety risk has been adequately reduced, either for the customer or for one's own internal risk management program. The opposite can be true as well. A tool may have sufficient safety controls and features designed into it to meet a supplier's risk acceptability, while external requirements may demand that additional safety features be incorporated to meet jurisdictional regulations for specific locales. In such a case, the supplier may decide to either

provide those additional safety features as an option or standardize the product, thereby reducing the number of configurations.

2.2.6 Barriers and Safety Features Against Hazard Propagation

The analyst should identify all existing barriers and safety features that interrupt the sequence of events that produces the incident or mitigates the consequence if the incident occurs. These barriers and safety features are evaluated to determine their adequacy in controlling the particular hazards.

Identifying the accident sequence requires a mental picture of the hazard and possible consequences, then fitting in discrete events that link the two. Typically, there are numerous paths to reaching an accident consequence. One technique that can be used to help identify accident paths is to brainstorm these different paths, then present the path that is most likely to occur. One method for identifying the accident path is to divide the accident sequence into initiating events, system responses, human actions, and structural responses. The resulting consequence may be acceptable or unacceptable. For example, process interruption is not acceptable for operation, but is acceptable from an ESH standpoint.

2.2.7 Possible Release Mechanisms and/or Failure Mechanisms

Once a hazard has been identified and the mitigated consequence(s) determined as unacceptable, the analyst needs to evaluate how the hazard could propagate into an accident. The analyst then determines what combination of events and failures must occur for the hazard to result in an undesirable event or accident. Failure of safety devices should be considered. This activity involves identifying all credible failure modes. Normal activities or actions, when combined with specific failures to release the hazard, should be included in the analysis. All single points of failure and credible multiple points of failure should be considered. The analyst should be aware that there may be more than one sequence of events that could lead to an accident. The analyst should exercise engineering judgement when identifying such events. The creation of accident sequences is a bit of an art, but the analyst should look for the shortest (most likely) path to an incident based on possible initiating events, system failures, and normal system responses that would contribute to a credible incident. For example, a meteor impact upon a gas box will cause a release of silane, but it is not very credible. However, a seismic event, in certain regions of the world, is a very credible initiating event for a silane release.

2.2.8 Consequence of Accident

Based on the sequence of failures and normal steps that cause a hazard to become an accident, the analyst then determines the consequences of the hazard. The consequence should be based on the worst credible case of the events. For example, if electrical wires are shorted, they can overheat. It is possible the wires may only get hot, or they may ignite. In such a situation, the analyst must assume that a fire occurs, unless there is specific test data or other protective devices that would preclude a fire.

Because the consequence is likely to be only an estimate, it is important to quantify the source term. In determining the consequence, the analyst should consider how the hazard is influenced by the sequence of events that lead to the accident to determine the quantity of the hazard released. A source term is the material, energy or item available for release to cause the consequence related to the incident. Examples of source terms include 100 cc of diborane,

208 VAC, 75 lbs., etc. The consequences of exposure to these source terms can be debated, but if everyone has a clear and agreed upon source term, it makes the discussions much more coherent.

Other SEMI documents, such as S10-96, *Safety Guideline for Risk Assessment*, provide additional guidance for categorizing consequences into bins that correlate with the degree of severity.

2.2.9 Likelihood of Accident

Determining the likelihood of an accident provides the analyst with perspective on the plausibility of a hazard propagating into an accident. The likelihood of the accident is based on the likelihood or plausibility that the sequence of events and failures will propagate into an accident. The likelihood value represents the frequency that the system will fail and cause the above described consequence.

The analyst can take two paths: the quantitative approach or the qualitative approach.

The quantitative approach is the highly rigorous, often grueling method of using statistical and experience-based data associated with component failure data, human error probability, equipment and procedure use frequency to derive a defensible likelihood number for a given accident scenario. Quantitative calculations are typically used when the consequence or cost of a failure or accident is critical (i.e., engine failure on a passenger aircraft or loss of coolant in a nuclear reactor).

Qualitative analysis is more common and uses more of an engineering estimate approach, but is still based on probability data derived from representative equipment and system failure data, human reliability data, and engineering judgment. Reference sources are available for quantifying the failure rates of items. Failure rates for electrical and mechanical devices can typically be found in engineering reference books. For larger subsystems, such as pumps, the supplier may have information based on their reliability testing or generic values can be derived from industry and government sources. While a great deal of research has been done on human reliability, some simple, conservative values can be used [Gertman, 1994].

Other SEMI documents, such as S10, *Safety Guideline for Risk Assessment*, provides additional guidance for categorizing likelihood into bins that can be used with the consequence bins to derive a risk-based list of hazards.

2.3 Documenting the Results

The selected system safety analysis techniques and formats of documentation, such as those discussed in Section 3, are used to provide the following to the overall product safety review and evaluation:

1. Systematic and thorough analyses of potential hazards
2. Assurance that credible hazards are not overlooked
3. Permanent record for hazard/risk data on compliance tracking database
4. Quick reference of critical systems safety and ergonomic areas
5. Additional risk-based requirements
6. Point of reference for third-party evaluations

2.3.1 Description of the System Analyzed

The system description serves two important functions:

1. It provides a clear picture of the features evaluated, an ability to recognize the hazards described, and an understanding of any recommendations related to unacceptable hazards.
2. For the analyst, by documenting the system, insight is gained into the function and operation, the safety features inherent in the design, and hazards and weaknesses associated with the design.

A main purpose should be included to define the boundaries and rationale for the analysis. The purpose should note whether the item under review is new or an upgrade or modification. The system description can also be used to document engineering changes that are being evaluated for safety.

The system description should also briefly describe the overall tool function or the component's interaction with the larger system. In detail, this section should describe those features of the system or component that are important to safety, including

- Operational phases
- Operating conditions (i.e., temperature, humidity)
- Main energy sources
- Types and quantities of hazardous materials
- Interlocks
- Design features which promote or ensure safety

By providing information on the above topics, the reader can determine the state of the system or component being evaluated.

2.3.2 Hazards Analysis Worksheet

A typical method of documenting the hazards analysis is by using a hazards analysis worksheet. A worksheet allows all of the pertinent information related to a hazard to be presented on a single page. There is no standard layout for a worksheet, rather they typically get modified based on user preference and need. A sample worksheet is provided in Table 1. The elements of the worksheet are described below.

Table 1 Sample Hazards Analysis Worksheet

| Hazard Description | Hazard Controls | Accident Sequence and Risk | Recommendations and Comments |
|--|--|--|---|
| <p>Describe exposure route, components, phase, and unmitigated consequence.</p> | <p>Indicate all existing or planned hazard controls.</p> | <p>Qualify the consequence and likelihood of a bounding accident based on means of initiation, safety features, and credible consequences.</p> | <p>If risk is unacceptable, indicate here, describe verification activities.</p> |
| <p>1) <u>Flammable Gas – Fire Due to Leak in Foreline:</u> Hydrogen is purged to the foreline, either by deliberate means using nitrogen, mixing with air, and is ignited by friction in the dry pump.</p> | <p>Control of this hazardous event is maintained by direct supply of nitrogen to the dry pump in quantities that ensure the hydrogen concentration is below lower explosive limit (LEL):</p> <ul style="list-style-type: none"> • Nitrogen dilution to the dry pump at a rate of 2 slm, which ensures that the hydrogen concentration stays at or below 5% (Per S2 Application Guide, Appendix C, part 8.2.3.1). • Nitrogen dilution flow is interlocked to the hydrogen supply valve. | <p><u>Accident Scenario:</u> Hydrogen is purged to the foreline, either by deliberate means using nitrogen or accidentally under maximum flow conditions due to failure (open) of V25 and V23A. Nitrogen dilution is lost at the purge pump and the interlock fails to detect the loss of flow. This would result in the maximum consequence. A more likely scenario is hydrogen pushed through the chamber and purge nitrogen is lost. The H₂ flow would be limited to 100 sccm through the mass flow controller. Ignition of hydrogen at the pump would likely cause replacement of the pump.</p> <p><u>Consequences:</u> Moderate (III) <u>Likelihood:</u> Extremely Unlikely (C) <u>Risk:</u> III-C, Low. No further action required.</p> | |
| <p>2) <u>Flammable Gas – Fire During Maintenance of Gas Box:</u> Hydrogen is leaked from the lines during maintenance, mixing with air and ignited.</p> | <ul style="list-style-type: none"> • The gas box door is interlocked to the hydrogen supply valve, V22A. • The hydrogen supply valve has lockout/tagout capability. | <p><u>Accident Scenario:</u> During maintenance, technician fails to LOTO the hydrogen valve before breaking the line. The supply valve fails to close, thus allowing hydrogen to flow when the line is breached.</p> <p><u>Consequences:</u> Severe (II) <u>Likelihood:</u> Incredible (D) <u>Risk:</u> II-D, Very low. No further action required.</p> | <ul style="list-style-type: none"> • Verify that the following procedures are included in the maintenance manual: a) manual purge and b) LOTO procedure. |

2.3.2.1 Hazard Description

Of primary importance for presentation in the hazards analysis table is a listing of the hazard, its quantity, form, and applicability. The purpose is to concisely present the issue for the analyst and subsequently for the design engineer tasked with solving the safety issue.

2.3.2.2 Hazard Controls

The hazard controls are those features, interlocks and procedures that are relied upon to ensure that the hazard either does not propagate into an accident, or if it does, that the severity of the consequence is acceptably low. Items listed in this column (column 2, Table 1) then become the safety critical items.

2.3.2.3 Accident Sequence and Outcome

This column (column 3, Table 1) is used to describe a worst-case credible accident, taking into account whether the safety controls described above either work or fail. The description will include initiating events, system responses, human reactions, and structural responses. Based on the sequence of events, the analyst can assign values for likelihood of occurrence and consequence. These values can then be used to evaluate the risk of the hazard.

2.3.2.4 Recommendations and Comments

This column (column 4, Table 1) is used to document any actions that are necessary or observations. For example, if the risk associated with a hazard is unacceptable, then recommendations for reducing that risk would be provided here. Another example would be verification of hazard controls. If an analyst took credit for a procedure requiring that lockout/tagout be performed (because that is normal practice at the company), the analyst may verify that the new procedure does include this requirement.

2.4 Managing Residual Risk

Once the hazards have been identified and the consequences and likelihood associated with those hazards propagating into an accident evaluated, the analyst must determine the risk of those hazards and whether the risk is unacceptable and implement changes to reduce the risk, if necessary. Risk analysis, risk reduction, risk acceptance, and residual risk—collectively known as risk management—are not discussed in this document. Those topics are covered in SEMI S10-96 and other documents; they are considered the next step after hazards identification and analysis.

Table 2 Hazards Checklist

| Hazard Source/Description | Potential Accidents/Effects |
|---|---|
| <p>Chemical Energy Chemical disassociation or replacement of fuels, oxidizers, explosives, organic materials or compounds</p> | <p>Fire Explosion Non-explosive exothermic reaction Material degradation Toxic gas production Corrosion fraction production</p> |
| <p>Contamination Producing or introducing contaminants to surfaces, orifices, filters, etc.</p> | <p>Clogging or blocking components Deterioration of fluids Degradation of performance sensors or operating components</p> |
| <p>Electrical Energy System or component potential energy release or failure. Includes shock, thermal, and static.</p> | <p>Electrocution/involuntary personnel reaction Personnel burns Ignition of combustibles Equipment burnout Inadvertent activation of equipment Release of holding devices Interruption of communications (facility interface) Electrical short circuiting</p> |
| <p>Human Hazards Human hazards including perception (inadequate control/display identification), dexterity (inaccessible control location), life support, and error probability (inadequate data for decision making). Conditions due to position (hazardous location/height), equipment (inadequate visual/audible warnings or heavy lifting), or other elements that could cause injury to personnel.</p> | <p>Personnel injury due to: Skin abrasion, cuts, bruises, burns, falls etc. Muscle/bone damage Sensory impairment or loss Death Equipment damage by improper operation/handling may also occur</p> |
| <p>Kinetic/Mechanical Energy (Acceleration) System/component linear or rotary motion. Change in velocity, impact energy of vehicles, components or fluids.</p> | <p>Impact Disintegration of rotating components Displacement of parts or piping Seating or unseating valves or electrical contact Detonation of shock sensitive explosives Disruption of metering equipment Friction between moving surfaces</p> |
| <p>Material Deformation Degradation of material due to an external catalyst (i.e., corrosion, aging, embrittlement, fatigue, etc.).</p> | <p>Change in physical or chemical properties; corrosion, aging, embrittlement, oxidation, etc. Structural failure De-lamination of layered material Electrical insulation breakdown</p> |
| <p>Natural Environment Conditions including lightning, wind, flood, temperature extremes, pressure, gravity, humidity, etc.</p> | <p>Structural damage from wind Equipment damage Personnel injury</p> |
| <p>Pressure System/component (e.g., fluid systems, air systems, etc.) potential energy including high, low, or changing pressure.</p> | <p>Blast/fragmentation from container over-pressure rupture Line/hose whipping Container implosion System leaks Aero-embolism, bends, choking, or shock Uncontrolled pressure changes in air/fluid systems</p> |
| <p>Radiation Conditions including electromagnetic, ionizing, thermal, or ultraviolet radiation (including lasers/and optical fibers).</p> | <p>Uncontrolled initiation of safety control systems & interlocks Electronic equipment interference Human tissue damage Charring of organic material Decomposition of chlorinated hydrocarbons into toxic gases Fuel ignition</p> |

| Hazard Source/Description | Potential Accidents/Effects |
|--|--|
| Thermal High, low, or changing temperature | Ignition of combustibles Initiation of other reactions Expansion/contraction of solids or fluids Liquid compound stratification |
| Toxicants Inhalation or ingestion of substances by personnel | Respiratory system damage Blood system damage Body organ damage Skin irritation or damage Nervous system effects |
| Vibration/Sound System/component produced energy | Material failure Pressure/shock wave effects Loosing of parts Chattering of valves or contacts Verbal communications interference Impairment or failure of displays |

3 USING HAZARDS ANALYSIS TECHNIQUES TO SUPPORT THE HAZARD ANALYSIS

Table 3 and Table 4 summarize the techniques with their associated information and suggested application. Only the FMEA, HAZOP and What If? analyses techniques are discussed further in this guide. The remaining techniques will be provided in a supplement.

Table 3 Hazards Analysis Techniques and Associated Information

| Method | Data Sources | Attributes | Applications |
|--|---|---|--|
| Fault Tree Analysis (FTA) | <ul style="list-style-type: none"> Drawings Equipment and Operations Specs Maintenance Records | <ul style="list-style-type: none"> Systematic Identifies Combination Failures | <ul style="list-style-type: none"> Decision Tool Cause Analysis Incident Investigation |
| Failure Modes, Effects, and Criticality Analysis (FMECA) | <ul style="list-style-type: none"> Drawings Operational records | <ul style="list-style-type: none"> Systematic Quantifies risk No combination failures | <ul style="list-style-type: none"> Cause and consequence analysis Systems risk assessment |
| Hazards and Operability Analysis (HAZOP) | <ul style="list-style-type: none"> PIDs Installation specifications Operational specifications | <ul style="list-style-type: none"> Experience-based Identifies combination failures | <ul style="list-style-type: none"> Analysis of deviations from design intents Risk ranking |
| Hazard Survey | <ul style="list-style-type: none"> Drawings Management systems Codes and regulations | <ul style="list-style-type: none"> Reduces major hazards Quantifies risk No combination failures | <ul style="list-style-type: none"> Equipment audits Safety self assessment |
| Process Safety Checklist | <ul style="list-style-type: none"> Drawings Equipment specifications Codes and regulations | <ul style="list-style-type: none"> Systematic Not stand-alone Qualitative | <ul style="list-style-type: none"> Equipment qualification Shut-down and start-up Design review |
| “What If?” Analysis | <ul style="list-style-type: none"> Drawings Procedures Experience | <ul style="list-style-type: none"> Non-systematic No combination failures | <ul style="list-style-type: none"> Identification of obvious hazards Design review |

Table 4 Hazards Analysis Techniques and Associated Applications

| Method | Application | | | | |
|--------------------------|---------------|------------------------|---------------------------|----------------|----------------------|
| | Design Review | Incident Investigation | Change Control Management | Process Safety | Equipment Evaluation |
| Fault Tree Analysis | | X | X | | |
| FMEA | X | | X | X | X |
| HAZOP | X | | | X | X |
| Hazard Survey | X | X | | | X |
| Process Safety Checklist | | | | X | |
| “What If?” Analysis | X | X | X | | X |

3.1 "What If" Analysis

The “What If?” analysis technique is an approach to hazard analysis that is directly reflected by its name. In using a “What if?” analysis, the team or facilitator uses questions posed in the form of “What if...?” statements, such as; “What if the cooling water to the chamber stops?” The team then continues to determine what the outcome would be (assuming there were no protections). In the case of this sample question, the outcome could be “ Chamber overheating, element burn out, bad process etc.” From here the team then determines if systems and protections are in place to protect against these occurrences. Again taking this sample question, the protections could be “Cooling water flow switch that shuts down process when it gets below XX set point,” or “Over temperature interlock switch on the chamber that shuts down power to the chamber heat source when the temperature reaches XX°C.” As can be seen, this technique requires very little training and can be done formally or informally by large or small groups.

3.1.1 Assembling the Team

As with all hazard analysis techniques, the team doing the analysis is as important as the technique itself. With the “What If?” approach, the team should be experienced with the equipment and its systems. Because the “What If?” approach is based on questions posed by the team, the effectiveness of the analysis depends on the quality of the questions asked. The team must understand the inherent hazards within the tool as well as those possible failure points to be thorough and effective in identifying single failures that could lead to a hazard risk.

Because the comprehensiveness and the quality of the hazard analysis is largely dependent on the team, assembling teams with experience and, as importantly, diversity is crucial. All critical disciplines should be represented. Technical expertise that should be represented in a team includes, as appropriate, electrical engineering, chemical or process engineering, and mechanical or structural engineering. Service and installation engineering personnel should not be overlooked. Often, design teams have little understanding of what really happens after installation. Service and installation should not be forgotten.

3.1.2 Choosing a Facilitator

Facilitators can dictate the outcome of a hazard analysis. A facilitator that is not organized, cannot keep the group on track, or that cannot lead the team to a successful completion might as well not participate. A facilitator should understand the mechanics of the hazard analysis technique chosen and know the team well. Ideally this is a safety professional, trained in hazard analysis techniques. The facilitator should be able to allow the participants to contribute. The

facilitator should also be able to draw the participation out of the team when the flow appears to stall. The good facilitator should be more of a coach than a dictator. In any case, choosing the right facilitator is critical to the success of the analysis.

3.1.3 Assembling the Reference Materials

Reference materials are essential during the analysis. These materials should include references such as piping and instrumentation diagrams (PIDs), schematics, drawings, interlock tables, service manuals, and component specifications.

3.1.4 Setting the Groundrules

Before diving into the hazard analysis, the boundaries and groundrules for the analysis should be established and communicated. Boundary conditions should be clear; for instance, will multiple failures be considered? If the answer is yes, a different technique should be considered. The team should also establish what parts of the equipment, or equipment lifecycles, are being considered. Thinking about the scope of hazards that will be considered is also useful. If the team is really looking at issues from an operator perspective, perhaps maintenance issues are to be evaluated at a later date. Section 2 provides useful guidance on the types and sets of hazards that could be considered. The team should also consider whether specific processes are being included or left out of the analysis. Looking at a process that uses inert gases will not turn up the same results as one that includes flammable or toxic chemistries. The scope of the hardware is also important to consider. If the team will be including support equipment or if there is an operator or maintenance interface associated with a subsystem, is it going to be considered?

In all of these conditions, it is important to also identify the boundaries of acceptable consequence. In some cases, minor damage to the equipment may be acceptable, especially if it means that a larger hazard is avoided. For instance, the risk of damaging a turbo pump through a hard emergency off (EMO) is much less than the risk of injury to a person caught in a moving part if the EMO were provided with a time delay. The team should decide what is acceptable so that they can determine when a consequence calls for control.

The best advice for the novice team is to start small. Focus the analysis into a manageable scope to ensure that the team does not get bogged down and wander from the task at hand. Look at the equipment from only one performance aspect—normal production operation, for instance. Once completed successfully, the team can go back and build on that analysis to include maintenance and service operation. As the team begins to grasp the basics, expanding the scope, and tackling larger projects is in order.

3.2 Description of the “What If?” Analysis

Following is a description of the “What if?” analysis technique from the System Safety Society Handbook. This excerpt was provided with the permission of the System Safety Society.

3.2.1 Alternative Names

None. Related to the "What-If/Checklist Analysis."

3.2.2 Purpose:

The purpose of the What-If Analysis methodology is to identify hazards, hazardous situations, or specific accident events that could produce an undesirable consequence. The What-If Analysis methodology is described in more detail in the first and second references at the conclusion of this discussion.

3.2.3 Methodology

The What-If Analysis technique is a brainstorming approach in which a group of experienced individuals familiar with a process ask questions or

Voice concerns about possible undesired events in the process. It is not inherently structured as some other techniques, such as the Hazard and Operability Study (HAZOP) or a Failure Mode and Effects Analysis (FEMA) which are also presented in this section. Rather, it requires the analysts to adapt the basic concept to the specific application.

The What-If Analysis Concept encourages an analysis team to think of questions that begin with "What If." Through this questioning process, an experienced group of individuals identify possible accident situations, their consequences, and existing safeguards, then suggest alternative for risk reduction. The potential accidents identified are neither ranked nor given quantitative implications.

The analysis team reviews the process from raw material to final product. At each step they ask "what if" questions dealing with procedural errors, hardware failures, and software errors. The What-If Analysis technique may simply generated a list of questions and answers about the consequences, safeguards, and possible options for risk reduction.

The What-If Analysis uses and produces a tabular listing of narrative-style questions and answers which constitute potential accident scenarios, their qualitative consequences, and possible risk reduction methods. Although some What-If analyses are documented in a narrative-style format, a matrix table makes the documentation more organized and easier to use.

3.2.4 Applications

The What-If Analysis can be applied to almost any operation or system process. It is specifically identified as an analysis method for use in the OSHA Process Safety Management regulations (see reference). The techniques may also be applied to contingency planning and accident analysis.

3.2.5 Thoroughness

The degree of thoroughness in the application of the What-If Analysis methodology is directly dependent upon team make-up and the exhaustive nature of the "what-if" questions asked. As in the HAZOPS, a diverse team in appropriate with at least one individual identified who is familiar with the process or operation being analyzed.

3.2.6 Mastery Required

The OSHA process safety management regulations requires that the analysis be performed by a team with expertise in engineering and process operation. It must include at least one person experienced and knowledgeable in the process, and one knowledgeable in the analysis method. For simple process, two or three people may be assigned to perform the analysis. However,

larger teams may be required for more complex processes. When a large team is required, the process may be divided logically into smaller portions, and a subset of the team may analyze a particular portion.

3.2.7 Difficulty of Applications

Performing a What-If Analysis for a given process requires a basic understanding of the process intention, along with the ability to mentally combine possible deviations from the design intent that could result in an accident. As the processes or operations under study becomes more complex, the difficulty of applications is increased.

3.2.8 General Comments

The What-If Analysis can be a useful tool if the analysis team is experienced and well organized. Otherwise, because of the relatively unstructured approach to the technique, the results are likely to be incomplete.

A small interdisciplinary team is usually more effective.

The advantages of the What-If Analysis are that it is simple, user friendly, and cheap.

The disadvantages are that it is good only for relatively simple systems and usually will not pick up on the potential for multiple failures or synergistic effects.

3.2.9 What If? Pros and Cons

As discussed above, the “What if?” approach is not inherently thorough and foolproof. For these reasons, the team should be organized and work with a systematic and deliberate approach. Other methods are very systematic by design, such as Hazards and Operability Analysis; however, the “What if?” approach is less inherently systematic and thorough, so it relies heavily on the team. This results in a hazard analysis method that is easy to perform for the team that is not trained in other forms of formal hazard analysis, but is considered less thorough and foolproof than other methods. When a fast method for determining single point failures is necessary and when an experienced team is available, the What If approach is a valuable tool.

3.2.9.1 Attributes

As noted above, this technique is easy to facilitate and can be used by a team that is relatively inexperienced in hazard analysis. The technique also provides a good qualitative analysis of the hazards present. It should be noted, however, that this method typically works to identify only single point failures.

3.2.9.2 Applications

This form of analysis lends itself to identifying single point failures and obvious hazards. It can also be effective in the design review to challenge designs and protections. The semiconductor industry has also found this technique useful in determining compliance with industry safety requirements for single fault hazard analysis, at any point in development of equipment.

3.2.9.3 Example

Below is an example of a typical “What If?” analysis. The example question is developed along with others to show the variations in application and approach.

“WHAT IF?” HAZARD ANALYSIS

Introduction

On October 2, 1998, a “What-If?” Hazard Analysis was conducted on ABC’s CVD tool to determine the potential for deviations from the intended system design that could pose an increased risk of hazard. This method of hazard analysis is discussed by the American Institute of Chemical Engineers (AIChE) in their *Guidelines for Hazard Evaluation Procedures*. In this analysis, the design or operating intent of the system is discussed, and questions (generally beginning with the phrase “What-If?”) are asked about possible deviations from design intent. The potential consequences of each pertinent deviation were discussed and evaluated.

If any single deviation was determined to potentially result in a release of a hazardous material, or other unsafe condition, then that deviation was deemed to be a single point failure and not compliant with the S2-93A guidelines.

Scope of the “What-If?” Hazard Analysis

The “What-If?” Hazard Analysis was performed to determine system compliance with the requirement of SEMI S2-93A that “no single point failure or operational error should allow immediate exposure of personnel, facilities or community to hazards or directly result in injury, death or equipment loss.” Therefore, the analysis focused on only single point failures and should not be considered a comprehensive process hazard analysis. Hazards that were identified as requiring more than one failure to occur were not studied further (i.e., to determine consequence or actions required).

The documented results are intended to represent the consensus of the “What-If?” team identified below. Systems Analysis, Inc. (SAI) did not investigate the veracity or thoroughness of all statements made by ABC’s representatives during the “What-If?” session and accepts no liability for issues that were not identified during the session and that are later found to pose hazardous consequences.

Team Members

Team members for the October 2, 1998, hazard analysis were as follows:

- John McEnroe, SAI, Facilitator
- Thomas Jefferson, SAI, Scribe
- Alex Bell, Mechanical Engineer, ABC
- Nick Copernicus, Electrical Engineer, ABC
- Maria Mitchell, Software Engineer, ABC
- Margaret Mead, Process Engineer, ABC
- Blaise Pascal, Technician, ABC

Issues identified for the analysis are listed in Table 5.

Table 5 Issues Requiring Hazards Analysis

| What If.....? | Consequence | Protection | Comments/Actions |
|--|---|---|--|
| Loss of Gas Box Exhaust | Potential release of HPM | Exhaust flow switch interlock circuit, which is hardware-based and shuts down all HPM valves. However, exhaust IL was not provided on the tool. | Non-Compliance Level B: ABC to provide NRTL approved tamper-proof photohelic exhaust monitor. See Paragraph 5.1 |
| Loss of vacuum/exhaust and N ₂ (process/backside/purge) still flowing | Overpressurize Chamber with process chemistry inside. Potential release of HPM | None | Non-Compliance Level A: Backside nitrogen gas valve (VL36) and slit purge valve (VL45) should be interlocked with the vacuum pressure switch. See Paragraph 4.5 Review UPC to confirm it will not supply nitrogen above 50 torr to chamber See Paragraph 4.5 |
| SiH ₄ /NH ₃ and TDEAT mix in the exhaust line | None (Small amount of TDEAT <2 ml/min flow) | None | None |
| TDEAT Over pressurized from facility source | Potential ruptured line Potential release | All components rated at least 140 psi (LFC, all others higher) Inlet is labeled with operating pressure. LEL detector provided which will close all valves if diethylamine is detected above 20 % of LEL. Spill tray currently installed in gas box. | Information Required - Include requirement in the manual that TDEAT supply is 40 PSI or lower. See Paragraph 18.2 |
| TDEAT mechanical fitting (pressurized) in oven leaks. | TDEAT released into oven with no exhaust/spill containment | None | Non-Compliance Level A: ABC to move mechanical fitting into the gas cabinet. See Paragraph 6.5 |
| Loss of Purge Nitrogen | Cannot purge gas lines | Can be purged by vacuum only(more slowly) | Information Required: ABC should document this procedure in the final manual and should include the need to verify that the purge has occurred. See Paragraph 18.2 |

| What If.....? | Consequence | Protection | Comments/Actions |
|--|--|--|---|
| Air to pneumatics is... A. Low B. No air pressure | Pneumatics close | All process valves are normally closed | None |
| Cooling CDA to chamber lid is... A. Low B. No air pressure | Over heat shower and increase deposition | CDA Interlock will shut down heaters if CDA is lost | None |
| High air pressure to loadlock/gate valves | Valves would slam shut Equipment damage | Needle valve on HVA valves. VAT valve does not need protection | None |
| Lose turbo pump | Process only | | None |
| High voltage on with chamber open | Shock and burn | 100 Torr pressure switch (hardware and NRTL approved) shuts off RF. RF cage interlock shuts off RF | None |
| Pedestal moves during maintenance | Moving hazard, pinch point | Gap size is large enough so that there is no pinch point (pumping ring is not fixed) | None |
| Chamber Isolation Valve closes with hand inside during maintenance | Moving hazard | Distance is too far to allow access | None |
| RF connector removed from A. Chamber B. RF match C. RF source | RF Exposure, burn, shock | Hardware interlocks are provided on generator cover, cables, match cover, Firmware RF disable Interlock provided for oven lid switch and chamber vacuum IL | Information Required ABC is in the process of changing the FW interlock to a hardware, fail-safe design. See Paragraph 5.1. |
| Heater Shorts (all) | Fire hazard | CB-10A | None |
| Heater overheat (all) | Temperature and equipment damage | Redundant Overtemp controller cut out contactor for heaters Additional thermal snap switch (175°C) on evaporator | None |
| Computer fails | Run away process | 24 VDC heart beat fails and then all system shuts | None |
| Tool loses power | Process | Entire system shuts done in safe state and manual reset required | None |
| Silane leak in gas box | Silane could impinge on adjacent gas lines | Silane line is enclosed in a stainless steel flame impingement panel | None |

3.3 Failure Modes and Effects Analysis (FMEA)

3.3.1 Alternative Names

There are several techniques analogous to the FMEA, including the Fault Hazard Analysis, the Failure Mode and Effects Criticality Analysis, and the Damage Mode and Effects Analysis. This class of methods uses deductive logic to evaluate a system or process for safety hazards and ultimately to assess risk.

3.3.2 Purpose

The purpose of the FMEA is to determine the results of effects of sub-element failures on a system operation and to classify each potential failure according to its severity. Often associated with an FMEA is an additional criticality analysis with the FMEA is referred to as the FMECA.

3.3.3 Method

1. The first step in preparing an FMEA is to define the system to be analyzed. The boundaries of the analysis are important and should be defined. Interfaces that cross the design boundary should be included in the analysis.
2. The analyst should obtain all necessary, available documents, including drawings, specifications, schematics, component lists, etc., to complete the analysis.
3. The system then is divided into manageable units for analysis. Typically, a system is divided into functional elements, such as RF, gas delivery, or data management.
4. Elements can be subdivided to piece parts if appropriate. Typically, an FMEA starts at a high subsystem level; if unacceptable consequences are discovered, then the particular subsystem is divided even further to identify the vulnerable link in the design.
5. The results of the analysis are recorded on a worksheet. A sample worksheet is provided as Table 6.
6. Once the system element has been identified, the analyst then must ask if any failure of the element will result in an unacceptable system loss. If the answer is No, then no further analysis of the element is necessary. If the answer is Yes, then the element must be examined further.
7. The analyst must look at the system and determine what kind of failures could occur and what the effect of such a failure would be. Failure causes are also identified.
8. The next step is to determine what provisions are in place to detect and/or control the consequence of a failure.
9. Failure modes are then evaluated for their magnitude of consequence and likelihood of occurrence. This process is the risk assessment portion of the analysis. It has also been the “Criticality” component in the Failure Modes and Effects Criticality Analysis (FMECA). Current practice has led to the FMEA including the “criticality” or risk assessment component within its scope.
10. By continuing in this manner of postulating the various failure modes, determining consequences, and assigning a risk value to the failure modes, the resulting document will provide a risk-ranked list of single point failures for the system.
11. When the analysis is complete, the analyst can then determine which failures require additional safety features and which do not.

3.3.4 Application

The technique is universally applicable to systems, sub-systems, components, procedures, interfaces etc. When applied to procedures, systems and the like must be sufficiently documented or otherwise formalized to lend themselves to the necessary analysis (see Procedure Analysis).

A small interdisciplinary team is usually the most effective approach.

3.3.5 Thoroughness

Thoroughness is dictated by the following:

1. The degree to which failure modes are identified and explored
2. The degree to which effect “avenues” are identified and to which they are explored for each failure mode
3. The degree to which the effects of multiple, co-existent failure modes are analyzed.

3.3.6 Mastery Required

Mastery for the uninitiated, seeking to analyze systems of more than trivial complexity, requires from several days to several weeks of formal instruction or study and practical experience. Working knowledge of Boolean algebra is helpful.

3.3.7 General Comments

These helpful hints will enhance the usefulness of the analysis and make the analysis effort more manageable:

1. Determine the scope of consequences before you begin. For example, is the only concern worker safety? Other concerns can include equipment damage, environmental impact, facility damage, tool downtime (reliability), or financial loss.
2. When documenting the failure modes, use unique numbers for each failure mode. It is best to use a combination of letters and numbers that help to identify the subsystem and the failure type.
3. Do not analyze elements for which a failure will not result in an undesirable consequence. For instance, if the purpose of an analysis is to identify only those consequences that might impact worker safety, then there may be no point in analyzing a low voltage data acquisition element.
4. Remember to look at interfaces. For example, if the boundary of a tool excludes remotely located water pumps, it is still important to examine the consequences from loss of cooling water.
5. Once the analysis is complete, it is prudent for the analyst to look at combinations of failures to see if there are combinations that might result in “large-scale” consequences. To do this requires some intuitive skills to focus on the mostly likely failure combinations.
6. Do not depend on personnel as a safety device or expect them to detect system failures.

References: From SSS

3.3.8 FMEA Pros and Cons

The FMEA is a very structured and reliable method for evaluating hardware and systems. The concept and application can be easy to learn and apply, even by a novice, and the approach

makes evaluating even complex systems easy to do. The drawbacks to the FMEA format are that it can be very time-consuming (and expensive) and does not readily identify areas of multiple fault that could occur. This method does not easily lend itself to procedural review as it may not identify areas of human error in the process.

3.3.9 Applications

The FMEA can be used at the design stage to evaluate critical assemblies or processes before hardware manufacture. Possible undesirable failure modes of a component or subsystem can be identified for redesign or further assessment before hardware manufacture.

Table 6 Sample FMEA Worksheet

| DESCRIPTION OF FMEA: | | | | | | | FMEA #: | |
|----------------------|----------------|------------------------|----------------|-------------------------|--------|--------------|---|-----------------|
| SYSTEM/MODULE NAME: | | | | | | | <input type="checkbox"/> Original FMEA | |
| CORE TEAM: | | | | | | | <input type="checkbox"/> Follow-up FMEA | |
| FMEA PREPARED BY: | | | | | | | Date: | |
| ID # | Item/ Function | Failure Mode and Cause | Failure Effect | Current Design Controls | Target | Severity (S) | Likelihood (L) | Action Required |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

EXAMPLE

3.4 Hazard and Operability Analysis (HAZOP)

HAZOP is a hazard analysis technique that systematically divides a system, equipment, or process into a series of nodes for careful examination. This methodology provides a systematic means of identifying a multitude of process hazards. HAZOP can be used to identify potential hazards and operability problems early in the Design for Safety cycle or on a released product or subsystem. This hazard analysis technique can be applied to both hardware considerations and procedures.

3.4.1 Method

The first step in preparing a HAZOP is to define the system to be analyzed. Once the system is defined, then nodes (boundaries) are selected that provide a logical breakdown of major subsystems (or components) for examination. For example, a typical chemical vapor deposition (CVD) process (see Figure 1) may be divided into the following nodes:

- Gas panel (to process module or chamber input)
- Liquid delivery system (to process module or chamber) input
- Process module (to input to vacuum pump)
- Vacuum pump (to input of abatement system)
- Abatement system (to input of customer's exhaust system)

Once the nodes are selected, the analyst should obtain all necessary, available documents, including drawings, specifications, schematics, component lists, etc., to complete the analysis. Piping and instrumentation drawings (PID) are critical to a thorough examination where process piping and chemical distribution systems are part of a node(s).

A team of interdisciplinary experts should be assembled so that a competent examination of each node is performed. For a process-intensive system, the team should be comprised of representatives from product safety, process engineering, product development, and field service. At the heart of the effort, the team identifies the means through which deviation from the design intent can occur. It further determines whether these deviations, collectively or individually, might create hazard. The team should be led by individuals serving as a facilitator and a technical scribe. At the start of the session, the facilitator should remind the team of the analysis boundaries and recommended nodes and ensure that this focus is kept throughout the analysis.

Steps used to examine each node include the following:

- Developing the "intention(s)" and associated parameters (design intent) for each element.
- Brainstorming deviations from the design intent (parameter) using guide word identifiers; e.g., "high," "low," or "none" for the parameter "pressure." (See Table 7 for a detailed matrix of deviation guide words.) Once the guide word is applied, then the deviation is identified; e.g., "high pressure" or "low pressure."
- Determining causes and consequences of the deviating elements.
- Recommending effective mitigation or protection(s) to eliminate the consequences of identified single point hazards.
- Adding a column to capture comments and action items.

The results of the analysis are recorded on a worksheet. A sample hazard analysis of a CVD system that focuses on one key node (gas panel to process module) is shown in Table 10.

3.4.2 Helpful Hints

These helpful hints will enhance the usefulness of the analysis and make the effort more manageable:

1. When determining nodes, select a portion of the process or equipment that is *anticipated* to act the same with regard to applicable parameters and potential important consequences. Examples:
 - A tank, its pump, and associated piping within a given containment area might be one node (with regard to chemical leak).
 - The above-atmospheric section of gas piping might be a different node than the subatmospheric section (with regard to breach of containment).
2. As the study progresses, if potential consequences are determined to be different within a node, the analysis may be simplified by reducing the scope (bringing in the boundaries) of that node. Examples:
 - A leak to containment vs. a leak to environment
 - Leaks that may result in chemical incompatibility based on manifolding
3. The facilitator should be very disciplined in reminding the team of the analysis boundaries (physical, operating, and scope).
4. The facilitator can save the analysis team considerable time and effort by determining appropriate nodes before the session and gaining team consensus before the session.

Table 7 Deviation Guide Word Examples

| Design Parameters | Guide Words | | | | | | |
|----------------------|--------------------|-------------------|---------------|------------------|---------------------|-----------------------|---------------------|
| | More | Less | None | Reverse | Part of | As well as | Other than |
| Flow | High Flow | Low Flow | No Flow | Back Flow | | | Loss of Containment |
| Pressure | High Pressure | Low Pressure | Vacuum | | Partial Pressure | | |
| Temperature | High Temperature | Low Temperature | | | Cryogenic | | |
| Level | High Level | Low Level | No Level | | | | Loss of Containment |
| Composition or State | Additional Phase | Loss of Phase | | Change of State | Wrong Concentration | Contaminants | Wrong Material |
| Reaction | High Reaction Rate | Low Reaction Rate | No Reaction | Reverse Reaction | Incomplete Reaction | Side Reaction | Wrong Reaction |
| Time | Too Long | Too Short | | | | | Wrong Time |
| Sequence | Step Too Late | Step Too Early | Step Left Out | Steps Backwards | Step Left Out | Extra Action Included | Wrong Action Taken |

3.5 Example Hazard and Operability Analysis

3.5.1 Introduction and Scope

A hazard analysis was facilitated and documented by Hazards Analysis Consulting (HAC) on the ACME Super Tool System designed by ACME Enterprises. The assessment was conducted on December 31, 1999.

Participants in the assessment included representatives from ACME's design engineering team. A list of participants is shown in Appendix A. The scope of the assessment included a review of the design of the Super Tool system, including the gas panel, process module, and exhaust system (applicable drawings and schematics are included in Figure 1). The assessment focused on equipment design or operating deviations that could result in an unexpected release or reaction of process chemistry or in a thermal hazard. Detailed consideration of electrical and mechanical hazards was not included in the assessment. The assessment included formal hazard analysis sessions, which were documented by ACME HAZOP facilitator. This documentation represents the statements and consensus of the participants during the sessions.

3.5.2 Assessment Methodology

The assessment consisted of one hazard analysis session attended by a cross-functional expert team from ACME Enterprises. A list of participants is shown in Appendix A.

3.5.3 Hazard Analysis Method

Several hazard analysis methods are available as recommended by the American Institute of Chemical Engineers (AIChE) in their publication, *Guidelines for Hazard Evaluation Procedures*. In general, the complexity of the hazard analysis method chosen should reflect the complexity of the process. For the subject system, which involves somewhat complex piping and instrumentation, and a significant number of equipment items and system components, the hazard analysis method selected was the Guide Word Approach Hazard and Operability (HAZOP) Study. HAZOP studies convene a cross-functional team to perform a methodical analysis of a system to determine the consequences of potential deviations. Before the session, the HAZOP facilitator conducted a brief review on the hazard analysis methodology for all participants.

For the subject system, each equipment item was reviewed separately as an operating "node." For each node, upset conditions or deviations from design conditions were determined by using "guide words" (e.g., high or low) combined with process parameters (e.g., operating temperature, pressure, or flow rate) which were determined by the consensus of the HAZOP team. For each upset condition or deviation, a cause or causes were determined by the consensus of the HAZOP team. Potential consequences were also determined by consensus, and protective devices were identified and discussed. Based on the team's determination of the adequacy of protective devices for the severity of each of the potential consequence(s), preventive actions and mitigation strategies were determined by the team and documented.

3.5.4 HAZOP Nodes and Guide Words

The HAZOP *equipment* nodes for this assessment were as follows:

- Node 1: Super Tool Gas Panel
- Node 2: Super Tool Process Module
- Node 3: Super tool Exhaust System

Design process parameters used during the equipment HAZOP session were process and carrier gas flow rate, direction, and identity; purge gas flow (rate and direction); system pressure and temperature; containment; cooling water flow (for the chamber and heater). Guide words used during the session were as follows:

| <u>Guide Word</u> | <u>Description</u> |
|-------------------|---|
| High | Increase in value of process parameter (e.g., high temperature) |
| Low | Decrease in value of process parameter (e.g., low pressure) |
| No, none | Negation of process variable (e.g., no flow) |
| Wrong | Inappropriate value of process parameter (e.g., wrong flow direction) |
| Misapplication | Inappropriate application of process parameter (e.g., misapplication of energy) |
| Breach | Leak from containment |

3.5.5 Action Item Determination

When the protective devices and procedures did not, in the consensus of the HAZOP team, adequately mitigate potential hazardous consequences, the team assigned action items intended to increase the protection. In addition to those actions protecting against significant hazards, the team assigned action items to enhance the inherent safety of the system/equipment/procedure or to obtain useful information about the system.

3.5.6 Summary Documentation

Documentation of the analysis discussion is presented in Table 8. This documentation represents the statements and consensus of the session.

3.5.7 Results

3.5.8 Assessment

The assessment revealed several design, operating, or procedural deviations that could result in hazards. These hazards were primarily the potential for release of corrosive, pyrophoric, and oxidizing gases and their potential incompatible reaction(s): To facilitate tracking the completion of action items, the action items documented on the HAZOP summary tables (Table 10) are listed below. Only an example of the gas panel node is provided.

Table 8 Action Items Identified in ACME Super Tool HAZOP**NODE 1: Gas Panel**

| # | Action | Due Date | Individual Assignee |
|---|--|----------|--|
| 1 | Potential unreacted silane through chamber to vacuum pump. Potential insufficient dilution at pump discharge may lead to fire/explosion hazard . ACME to determine failed MFC flow rate and confirm normal pump dilution rate does not achieve SiH ₄ LFL | 1/1/00 | Super Duper Process Engineer/Super Duper Product Safety Engineer |
| 2 | Continued | | |

NODE 2: Process Module

| # | Action | Due Date | Individual Assignee |
|---|-----------|----------|---------------------|
| 1 | Continued | | |
| 2 | Continued | | |

NODE 3: Exhaust System

| # | Action | Due Date | Individual Assignee |
|---|-----------|----------|---------------------|
| 1 | Continued | | |
| 2 | Continued | | |

Table 9 Hazard Analysis Participants

| | | | |
|--------------------------------|-----|---------------------------------------|------|
| Super Duper Facilitator | CSP | Product Safety Manager | ACME |
| Super Duper Field Engineer | | World Wide Field Engineering Manager | ACME |
| Super Duper Product Engineer | | Product Engineering | ACME |
| Super Duper Process Engineer | | Research and Development Applications | ACME |
| Super Duper Scribe | | Product Safety | ACME |
| Super Duper Technology Manager | | | ACME |

Table 10 HAZOP Summary – Gas Distribution Panel

| Parameter | Guide Word | Deviation | Cause(s) | Consequence(s) | Protection | Comments/Action |
|----------------|--------------|---|--|--|--|--|
| Flow of silane | High | High silane flow rate during processing | MFC failure | Potential unreacted silane through chamber to vacuum pump. Potential insufficient dilution at pump discharge may lead to fire/explosion hazard . | | Action: Determine failed MFC flow rate and confirm normal pump dilution rate does not achieve SiH ₄ LFL. |
| | | | By-pass V-13 opened (manual valve) | Same as above | Valve labeled as to correct position | Action: Determine bypass flow and confirm normal pump dilution rate does not achieve SiH ₄ LFL. |
| | | Flow when no flow should occur | By-pass V-15 fails open | Same as above | | |
| | | | Valve V-14 leak-by | Potential flow of incompatible gases, causing reaction . (See Wrong Flow, below). If maintenance personnel open line, potential exposure to flow of gas. | Dual valve isolation required by maintenance procedure prior to opening any hazardous gas line | |
| | Low Flow | Low silane flow rate | Loss of silane supply | Process quality issue only. No anticipated hazard. | | |
| Reverse Flow | Reverse Flow | Silane flows to N ₂ supply | Loss of N ₂ supply pressure and V-13 open | Contamination of N ₂ supply; potential reaction in other tools if this is not dedicated supply. | Pressure transducer on N ₂ supply line is observed prior to operation | Comment: Pressure profile prevents unless by-pass open (manifold connection downstream of MFC, so flow is sub-atmospheric) |
| | | Silane flows to NF ₃ or PH ₃ supply | Recipe error | Cross-contamination of process gas supply; potential reaction . | Interlock on final valves (V-7, V-14) prevents flow of both gases simultaneously | |
| | Wrong | Silane flows at wrong time | – Controller error – Recipe error | Potential flow of incompatible gases, causing reaction . However, gases would mix at subatmospheric pressure, so reaction is reduced. | – Interlock on final valves (V-7, V-14) prevents flow of both gases simultaneously – Pressure interlock disallows gas flow to chamber unless sub-atmospheric pressure | Action: Confirm interlocks are hardware, not firmware (hardware requiring software control) |

| Parameter | Guide Word | Deviation | Cause(s) | Consequence(s) | Protection | Comments/Action |
|--|--------------|--|---|---|--|---|
| Flow of NF ₃ or PH ₃ | High | High process gas flow rate | MFC failure | Potential un-reacted process gas through chamber to vacuum pump. PH ₃ additional flow may cause phosphorus buildup , requiring additional maintenance and associated hazards. | Dilution at pump discharge sized for silane, so more than adequate for MFC failed flows of other process gases | |
| | Low Flow | Low process gas flow rate | Loss of supply | Process quality issue only. No anticipated hazard. | | |
| | Reverse Flow | One gas flows back toward another's' supply (or to purge) | Loss of supply | Worst-case: Cross-contamination of process gas is flow of both gases called for simultaneously. Potential reaction | | |
| | Wrong | Wrong process gas flows | – Controller error – Recipe error | Potential flow of Incompatible gases, causing reaction. See above. | | |
| Flow of purge gas | High | High purge gas flow | Upstream regulator failure | None | Components rated to high pressure | |
| | Low | Low N ₂ flow, or no N ₂ flow to portions of line | Current configuration has no way to purge silane line upstream of MFC | Maintenance personnel may open unpurged line, potential exposure to residual gas. (See also pressure low regarding reverse flow) | | Comment: Most applicable to filter change. Action: Supply isolation capability with lockout/tagout to enable isolation for filter change and dual valve isolation of MFC change out. |
| | No | No N ₂ flow | Loss of purge supply | Same as above | Pressure transducer is required to be observed before starting maintenance procedure | |

| Parameter | Guide Word | Deviation | Cause(s) | Consequence(s) | Protection | Comments/Action |
|-----------------------------------|------------|----------------------------------|--|--|---|--|
| Process Gas Pressure | High | High process gas pressure (any) | Upstream regulator failure | Panel components subjected to higher pressure (example, SiH ₄ pressure may be ~2100 psi if only one regulator from cylinder to panel). Worst case: May cause component failure, release to exhausted panel enclosure (See Containment Breach, below). | (See Containment Breach, below) | <p>Comment: No regulator in panel</p> <p>Action: Obtain pressure ratings of components, compare to maximum upstream pressure. If vulnerable to highest assumed bottle pressure (2100 psi) add pressure regulation or end-user instruction in manual for dual pressure control.</p> <p>Action: Determine reaction of MFC to high system pressure (higher or lower flow?).</p> |
| | Low | Low process gas pressure | -Low delivery pressure -Loss of supply | If purge supply lost, may achieve reverse flow of process gas to N ₂ line when recipe calls for purge (see above). | Normally-closed manifold valves, auto-purge cycle with software controls to limit process gas flow during purging | |
| Temperature | High | High temperature | Fire in panel (e.g., due to SiH ₄ leak) | Assumptions: Poly lines for pneumatics would melt; once SiH ₄ source removed, fire is not self-sustaining (see Protection, right) | -Limited combustible materials -Metal enclosure -Valves normally closed | |
| | Low | Low Temperature | N/A | | | |
| Primary Containment (line) | Breach | Leak from line | Fitting failure | <p>Release to exhausted enclosure. For SiH₄: fire, potential explosion</p> <p>For NF₃/PH₃: potential toxic release (removed by enclosure, see Protection, right).</p> | <p>- Provide flame impingement panels to prevent SiH₄ fire from impacting adjacent lines</p> <p>- See also Protection for high temperature.</p> <p>- Enclosure passes tracer gas testing for NF₃ and PH₃ worst-case releases</p> | Action: Confirm flow across fittings is sufficient to prevent SiH ₄ explosion. |
| Secondary Containment (enclosure) | Breach | Failure of secondary containment | Door open | Not a hazard unless primary containment also fails, then insufficient capture leading to personnel exposure . | | |

| Parameter | Guide Word | Deviation | Cause(s) | Consequence(s) | Protection | Comments/Action |
|------------------------|------------|----------------------------------|---------------------------|----------------|--|--|
| Enclosure Exhaust Flow | No | No exhaust flow at enclosure | Exhaust system failure | Same as above | Emergency Notification System shuts down gas flow at the source. | |
| | Low | Insufficient exhaust for capture | Incorrect damper position | Same as above | Observation of magnehelic required on daily rounds | Action: Consider photohelic with notification of low flow to replace magnehelic gauge. |

EXAMPLE

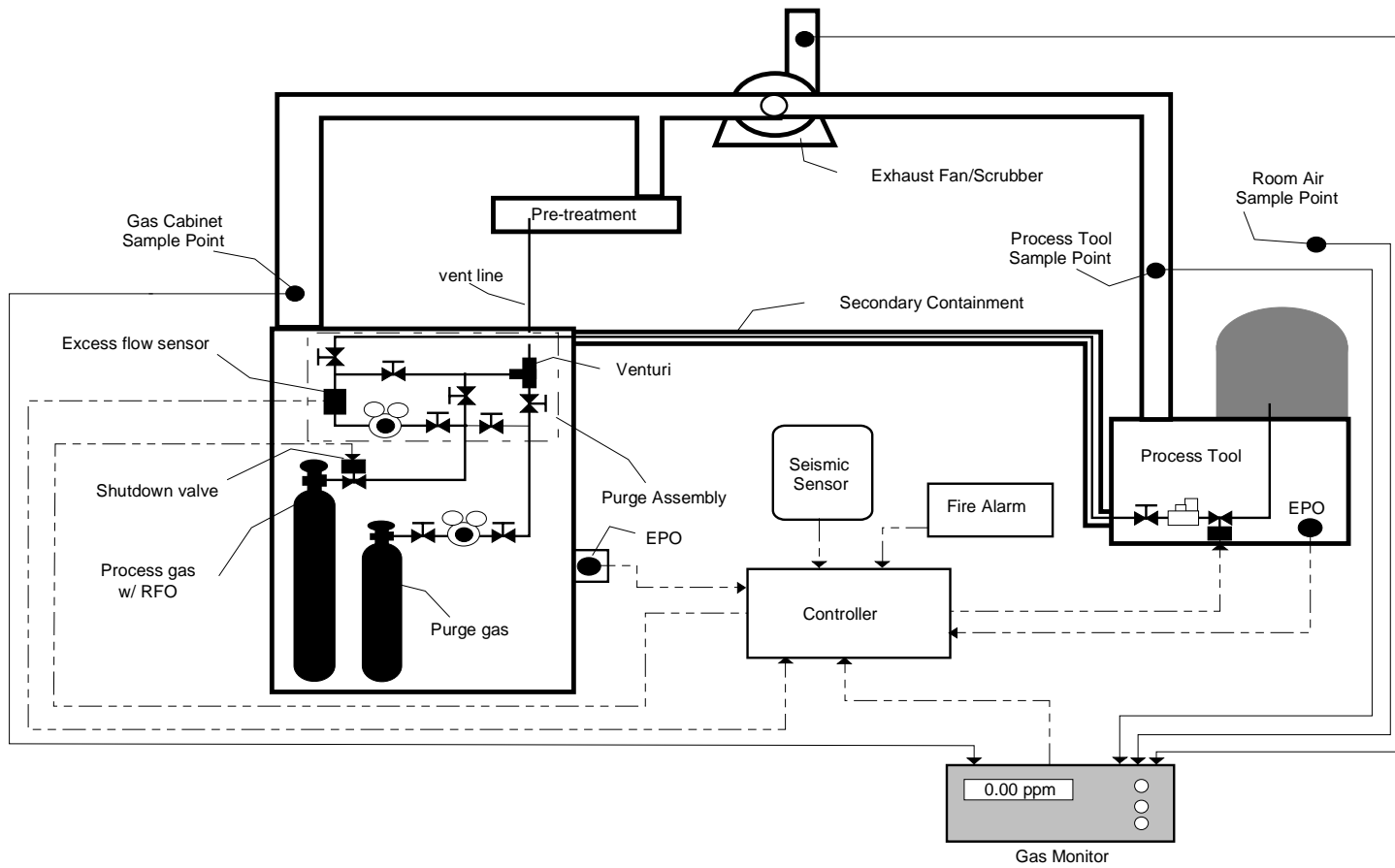


Figure 1 ACME Enterprises Super Tool System

4 REFERENCES

- Mahn, J.A et al., *Qualitative Methods for Assessing Risk*, Document Number SAND95-0320, Sandia National Laboratories (May 1995).
- Gertman, David I. and Blackman, Harold S., *Human Reliability and Safety Analysis Data Handbook*, John Wiley and Sons, Inc (1994).
- Stephans, Richard A and Talso, Warner W, editors, *System Safety Analysis Handbook*, System Safety Society (1996).
- Howard, Hillard H. et al., *Guidance for the Preparation of Safety Analysis Reports*, Document number LA-11661-MS, Los Alamos National Laboratory (June 1990).
- Parker, Richard and Foster, Mollie, *Design for ESH – Semiconductor Industry*, NSC (1999).
- Hazard Analysis and Risk Assessment*, Novellus Systems Incorporated ISO procedure SAF-2002b (April 1999).
- Department of Energy, DOE/EH-DRAFT, "Preliminary Guide for Conformance with OSHA's Rule for Process Safety Management of Highly Hazardous Chemicals," March 1993.
- Department of Energy, DOE/EH-DRAFT, *Guide for Chemical Process Hazardous Analysis*, March 1993.
- Department of Labor, 29 CFR 1910.119, *Process Safety Management*, July 1992.
- Guidelines for Hazardous Evaluation Procedures*, Center for Chemical Process Safety, AIChE, 1992.

**SEMATECH Technology Transfer
2706 Montopolis Drive
Austin, TX 78741**

**<http://www.sematech.org>
e-mail: info@sematech.org**