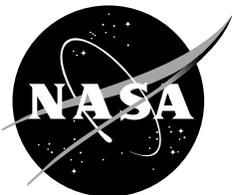


Preparing Hazard Analyses for JSC Ground Operations

Safety and Test Operations Division

Revision C

December 2001



National Aeronautics and
Space Administration

Lyndon B. Johnson Space Center
Houston, Texas

Foreword

This document provides you instructions for preparing hazard analyses on JSC ground equipment and operations. It contains basic instructions and references for several hazard analysis techniques. The techniques mentioned provide means to identify hazards and their controls in systems and their operations throughout the system life cycle. The document also includes instruction on doing Job Hazard Analysis.

The document is a “how-to” document, rather than a requirements document. It provided more detailed instructions for meeting Chapter 111 of JPG 1700.1, “JSC Safety and Health Handbook,” current version.

If you have any comments or suggestions for this document, please contact the Chief, Safety and Test Operations Division, mail code NS.

Approval:

Stacey T. Nakamura
Chief, Safety and Test
Operations Division

Contents

1	Who must follow this document?	1
2	What is a system?.....	1
3	What is a hazard analysis?	1
4	When must I do a hazard analysis?.....	1
5	Available techniques for hazard analysis.....	2
6	Which technique should I use?	2
7	Contents of a hazard analysis.....	3
8	Procedure for doing a hazard analysis	3
9	Tools to help you with a hazard analysis	4
10	Eliminating or controlling hazards found during your hazard analysis	4
11	Must I track the hazards until they are closed?.....	4
12	References to use while doing a hazard analysis	4
13	Reviewing and approving a hazard analysis	4
14	What must I do with the hazard analysis after I am through?.....	5
15	Format of a hazard analysis	5
16	Assessing the risk of a hazard.....	5
	Appendix A, Comparison of Hazard Analysis Techniques.....	7
	Appendix B, "What-If" Analysis.....	9
	Appendix C, "What-If/Checklist".....	11
	Appendix D, Hazard and Operability Study.....	16
	Appendix E, Failure Mode and Effects Analysis (FMEA).....	24
	Appendix F, Fault Tree Analysis.....	39
	Appendix G, Job Hazard Analysis (JHA)	47
	Appendix H, Some Other Analysis Techniques	54

NASA Mishaps

Ninety-one civil service and contractor personnel sent to hospital for exposure to nitrogen tetroxide due to unexpected leaking valve.

Fire and explosion occurred in 7500 kva power generating unit when unexpected arc occurred due to unforeseen wear of transformer insulation causing a phase to ground release.

1 Who must follow this document?

You must follow this document if you do hazard analyses of any kind for JSC ground operations.

2 What is a system?

A system is a group of any level of complexity that includes:

- Operations
- Support environment
- Personnel
- Materials
- Tools
- Equipment
- Facilities
- Software
- Procedures
- Personal protective devices

3 What is a hazard analysis?

A hazard analysis is an organized method to identify hazards at any point in the life cycle of the system and to ensure that the hazards are properly controlled to minimize or accept the level of risk. A “hazard” is any credible condition or exposure that could cause injury, damage to property, or loss of life, or mission failure.

4 When must I do a hazard analysis?

You must do a hazard analysis if:

- Your operation falls under the requirements of 29 CFR 1910.119, “Process Safety Management.”
- Your work involves hazardous operations, such as working with:
 - Hazardous chemicals
 - Explosives

- Extreme temperatures
- Lasers
- Cryogenic materials
- Vacuum chambers with or without test subjects
- Lifting devices and equipment
- Any other hazardous operations
- You are building a new facility, or modifying an existing one.
- You are planning to conduct a hazardous test.
- As required by Chapter 111 of JPG 1700.1 (current version), “JSC Safety and Health Handbook.”

You should start your hazard analysis in the early design stages and add to it as design and operational details are available. Designing in hazard controls is less expensive than adding controls after the system is built. You may still do a hazard analysis on an existing system if one hasn't been done before.

5 Available techniques for hazard analysis

There are several hazard analysis techniques. Here are some of the more common ones:

- What-If
- What-If/Checklist
- Hazard and Operability Study (HAZOP)
- Failure Mode and Effects Analysis (FMEA)
- Fault Tree Analysis
- Job Hazard Analysis (JHA)
- Integrated Hazard Analyses
- Any appropriate hazard analysis that will provide the same level of detail as those listed above
- Any combination of the above

6 Which technique should I use?

You may use any of the techniques listed above or use any other technique, as required by the complexity of your system. Consulting safety personnel on the decision of which technique to use will help you choose the most effective technique for your situation. Some techniques are better than others. For example, a FMEA or a JHA is not good for an entire building, but most of the others are. Conversely, a FMEA is excellent for analyzing what on the systems can fail as a single-point failure. However, a FMEA only considers hardware and not procedures. Many other techniques involve hardware, procedures, actions of people, and the environment that the system occupies as well.

Appendix A lists the advantages and disadvantages of the techniques covered in this document.

7 Contents of a hazard analysis

As a minimum, your hazard analysis must contain:

- The system name
- The location of the system
- The hazards associated with the system
- The consequences of each hazard, if it were to cause a mishap
- Existing engineering and administrative controls for each hazard
- Proposed engineering or administrative controls for each hazard, if the existing controls are inadequate
- The consequences of the engineering and administrative controls failing
- The human factors associated with the system
- A qualitative evaluation of the possible safety and health effects before and after the controls are in effect
- The names of the team members that did the hazard analysis
- The last time you looked at the system
- A qualitative of the risk before and after the hazard controls are in place

8 Procedure for doing a hazard analysis

The specific steps for doing a hazard analysis depends on the hazard analysis technique(s) you use. Some hazard analyses are done by a single safety analyst or engineers, while others are done by teams. Many times, a team approach is the best approach because of the synergy of the team in identifying hazards.

The general steps for doing a hazard analysis are:

- Determine whether or not to use the team approach. Ask yourself, “Do I form a team? If so, who should be on my team?” The team should include:
 - Designers
 - Maintenance personnel
 - Construction personnel
 - Operations personnel
 - Safety personnel
 - Any others who might have knowledge of the system
- Determine the best hazard analysis technique to use.
- Do the hazard analysis by:
 - Identifying hazards
 - Determining the worst credible mishap, if all controls failed
 - Determining the Risk Assessment Code (RAC) for the event with no controls
 - Determining what controls are in place
 - Determining the worst credible event with all the existing controls in place
 - Determining the RAC with all controls in place
 - Determining if any further work is required based on the RAC

- Determining what further work is required
- Writing the report

9 Tools to help you with a hazard analysis

Several tools for doing a hazard analyses are available, based on the technique you want to use. The Safety and Test Operations Division will provide advice, technical help, team facilitating, and software and other tools on request.

10 Eliminating or controlling hazards found during your hazard analysis

You must use at least one of the steps shown below to eliminate or control a hazard:

- Eliminate the hazard by design, if possible.
- Control the hazard by guards, procedures, or training. Include procedural controls in the actual procedures. Update training requirements to reflect the hazard controls as necessary.
- Accept the left over risk.

The steps are listed in order of preference. See chapter 105 of JPG 1700.1 (current version) for more information.

11 Must I track the hazards until they are closed?

Yes, you must track any open hazards until they are resolved as described in 10 above.

12 References to use while doing a hazard analysis

You may use any of the following for references:

- System drawings
- Other hazard analyses which have reviewed similar or like systems
- Functional and physical interfaces
- Previous history of the system or process
- OSHA – 29 CFR 1910 for general industry and 29CFR 1926 for construction
- Other appropriate standards
- NHB 1700.1 (V1-B), “NASA Safety Policy and Requirements Document”
- NHB 7320.1, NASA Facilities Engineering Handbook
- NASA Standard 8719.7, Facility System Safety Guidebook
- JPG 1700.1 (current version), “JSC Safety and Health Handbook”
- MIL-STD 882, Systems Safety Program Requirements

13 Reviewing and approving a hazard analysis

You must have at least the following people review your hazard analysis:

- The facility manager
- The contractor’s safety representative (if applicable)

- The branch chief and equivalent contractor management (if you are a contractor)
- The division chief and equivalent contractor management (if you are a contractor)
- NS Safety and Test Operations Division

Include comments in the hazard analysis, as necessary. The analysis must have approval signatures by the above personnel before you may start any hazardous activity.

14 What must I do with the hazard analysis after I am through?

You must keep the analysis and review it every time there is a change to the system, or every 5 years, whichever is less. You must also include the findings of the hazard analysis in the operational procedures to ensure that personnel performing the procedures are aware of the hazards and take appropriate actions.

For job hazard analyses, you must review them every year or whenever the job changes.

15 Format of a hazard analysis

The format of the hazard analysis can vary depending on the analysis technique used. However, it must contain the items called out in Paragraph 8 above. Examples of different hazard analysis techniques are in the Appendixes.

16 Assessing the risk of a hazard

Use the RAC matrix and descriptions in Chapter 111 of JPG 1700.1 (current version), which are shown on the following pages. To use the matrix:

- Find the “severity” or the worst-case outcome of a mishap from the hazard along the left side of the matrix.
- Find the “frequency” that you expect the mishap to occur across the top of the matrix.
- Find the RAC in the box where the “severity” and “frequency” cross.
- Use the table after the matrix to determine what action to take based on the RAC.

Note: Refer to the current version of JPG 1700.1, Chapter 111 for the current RAC matrix.

PROBABILITY ESTIMATE (FREQUENCY)

		A Frequent Likely to occur one or more times a year.	B Probable Likely to occur once in 1 - 2 years.	C Occasional May occur once in 2 - 5 years.	D Remote Unlikely to occur, but possible within 5 years to end of system life.
S E V E R E I T Y	I Catastrophic Death, several serious injuries or illnesses, or damage over \$1,000,000	1	1	2	3
	II Critical Serious injury or illness, several lost workdays, or Damage between \$250,000 - \$1,000,000	1	2	3	3
	III Marginal Lost workday, several minor injuries, or Damage between \$25,000 - \$250,000	2	3	4	4
	IV Negligible Minor injury or damage less than \$25,000	3	3	4	4

Appendix A Comparison of Hazard Analysis Techniques

The following table lists the hazard analysis techniques covered in this document along with the advantages and disadvantages.

<i>Technique. . .</i>	<i>Advantages . . .</i>	<i>Disadvantages . . .</i>	<i>See . . .</i>
What-If	<ul style="list-style-type: none"> • A very inexpensive tool to estimate the seriousness of some system concerns • Good when you don't have a lot of time to make decisions • Good for contingency planning 	<ul style="list-style-type: none"> • Not as formalized as the other safety tools • May give scenarios which are not realistic 	Appendix B
What-If/ Checklist	<ul style="list-style-type: none"> • Same as the What-If analysis 	<ul style="list-style-type: none"> • Same as the What-If analysis 	Appendix C
Hazard and Operability Study (HAZOP)	<ul style="list-style-type: none"> • Looks at process deviations • Uses a synergistic team approach • Breaks systems into manageable pieces • Also identifies operability, maintenance, and environmental hazards • Looks at most of the possibilities during the analysis and can limit the number of causes that are investigated further. • Good for systems that involve some kind of "flow" such as fluid flow through a pipe or electron flow through a wire 	<ul style="list-style-type: none"> • Requires a team of more than one person • May be time-consuming • Is expensive to perform • Requires good documentation 	Appendix D
Failure Mode and Effects Analysis (FMEA)	<ul style="list-style-type: none"> • Good for specific, critical or hazardous subsystems to tell you what can fail and what the result of the failure will be • Is very systematic approach • Looks at every component to determine failure effects 	<ul style="list-style-type: none"> • Only looks at hardware and not at operations • Too laborious and time-consuming to use on an entire building • Only looks at hazards associated with failures, not those associated with normal operations • Only looks at the hardware failures, not the interaction between personnel, equipment or environment • Does not identify all hazards associated with a system, even if it identifies all single point failures 	Appendix E

<i>Technique...</i>	<i>Advantages...</i>	<i>Disadvantages...</i>	<i>See...</i>
Fault Tree Analysis	<ul style="list-style-type: none"> • Finding the causes of catastrophic, top-level events such as death or system destruction in complex systems • Can use before a mishap or after a mishap • Can be tied to numerical solutions to determine the probability of occurrence • Can be one of the most thorough analyses performed if the information on the system is well defined. 	<ul style="list-style-type: none"> • Must know many of the hazards in order to define a catastrophic, top-level event • Requires knowledge of fault tree techniques • Is very costly and time consuming and may require a complex computer analysis • The major disadvantage of a FTA is that it is very labor intensive and very expensive to perform. It also requires good documentation of the system. 	Appendix F
Job hazard analysis	<ul style="list-style-type: none"> • Good for analyzing a specific task • Employees are involved in reviewing their jobs to see if they can do their jobs more safely. • Employees work with their supervisors to improve job safety. • Required for hazardous jobs. 	<ul style="list-style-type: none"> • Not good for analyzing large operations • Each task must be reviewed in great detail • Management must be prepared to make changes to job which may effect the cost of the operations • The analysis is expensive to perform. 	Appendix G
Other analyses such as:	<ul style="list-style-type: none"> • Good for specific applications when the normal analysis techniques indicate that further investigation is needed 	<ul style="list-style-type: none"> • These analyses are very focused 	Appendix H
<ul style="list-style-type: none"> • Event tree analysis • Common cause analysis • Sneak circuit analysis 			

Appendix B “What-If” Analysis

1 What is a “What-If” hazard analysis?

A “What-If” hazard analysis is probably the easiest and most inexpensive form of hazard analysis to perform. Basically, you start at the lowest level of component and ask the question “what if” the part fails? What will be the outcome? The purpose of a “What-If” hazard analysis is to consider the effects of unexpected events on the system.

2 What are the advantages of a “What-If” analysis?

The “What-If” analysis is a very inexpensive tool for estimating the magnitude of certain facilities’ concerns. This analysis approach is good when you don’t have a lot of time for decision-making. It is also very good for contingency planning.

3 What are the disadvantages of a “What-If” analysis?

The “What-If” analysis is not as formalized as the other safety tools. It may give scenarios that are not realistic.

-

4 When would I do a “What-If” analysis and who should do it?

You do a “What-If” analysis if you want to examine the possible deviations from the design and operations of your process or activity.

This analysis is most effective if done by individuals who have a good understanding of the operation of the facility and the associated systems in the facility.

5 Steps to doing a “What-If” analysis

The same kind of information is required for a “What-If” analysis as for a HAZOP (See Appendix C). The basic steps are as follows:

- Define the objectives and scope of the analysis.
- Select the team to perform the analysis.
- Conduct the questioning.
- Document the results.
- Track the hazards until eliminated or controlled.

6 Where should I start?

You methodically go through each functional area defined by the analysis objectives. Start with one functional area or some other manageable area of the facility or system using a series of “What-If” scenarios. Like the HAZOP, you can use the process for selecting nodes and,

ultimately, your manageable groups. You may use information shown in Appendix C for guidance in considering the hazard areas.

7 Typical “What-If” questions to ask

Typical questions might sound like this:

- What happens if my brakes failed when I was driving down the highway at 70 mph?
- What happens if the building temperature rises above ambient?
- What procedures do the test personnel follow if the pressure in the system rises drastically?

8 Format for a “What-If” Analysis

A typical example of a “What-If” analysis is shown below:

“What-If” Hazard Analysis Question Examples

What would happen to my facility **if** I had a fire? I would sound the alarm and go to the assigned assembly point.

What would be the worst thing that could possibly happen **if** I had a fire in my facility? We would lose the facility and possibly a life.

What would I do **if** we had a fire in my office? Call x 33333, if I can safely do so and then exit the building.

What is the closest exit **if** there were a fire in my building? To the right, approximately 15 feet.

Appendix C “What-If/Checklist”

1 What is a “What-If/Checklist”?

A “What-If/Checklist” is a type of hazard analysis that is very similar to the “What-If” hazard analysis, except that it applies a specific set of questions to each specific area. These questions do not necessarily ask “What-If,” but may just list an area of potential concern.

2 What are the advantages of a “What-If/Checklist”?

Like the “What-If,” the “What-If/Checklist” analysis is a very inexpensive tool used to estimate the magnitude of facility concerns. This system is good when you do not have a lot of time for decision-making. It is also very good for contingency planning.

3 What are the disadvantages of a “What-If/Checklist”?

The “What-If/Checklist” analysis is not as formalized as the other safety tools. It may give scenarios that are not realistic and it may not look at all possible causes. It gives equal importance to all hazards and may cause unnecessary expense to correct problems that do not have much probability of occurrence.

4 When would I do a “What-If/Checklist” analysis and who should do it?

You do a “What-If/Checklist” analysis if you want to examine the possible deviations from the design and operations of a process or activity.

This analysis is best done by individuals who have a good understanding of the operation of the facility and the associated systems in the facility.

5 Steps for doing a “What-If/Checklist” analysis

The same kind of information is required for a “What-If/Checklist” as is for a HAZOP (See appendix C). The basic steps are as follows:

- Define the objectives and scope of the analysis.
- Select the team to perform the analysis.
- Conduct the questioning.
- Document the results.
- Track the hazards until eliminated or controlled.

6 Where should I start?

You methodically go through each functional area defined by the analysis objectives. You start with one functional area or some other manageable group of the facility or system using a series of “What-If/Checklist” scenarios. Like the HAZOP, you can use the process for picking nodes

and picking your manageable groups. You can use the information shown in appendix C for guidance to consider the hazard areas.

7 Typical “What-If/Checklist” questions to ask

Typical questions, might sound like this:

- What happens if my brakes failed as I was driving on the highway at 70 mph?
- What happens if the building temperature rises above ambient?
- What procedures do test personnel follow if the pressure in the system rises drastically?

8 Format for a “What-If/Checklist” analysis

A “What-If/Checklist” analysis may look like the one shown below:

“What-If/Checklist” Example

HAZARD ANALYSIS REPORT

Date: Wednesday, December 11, 1996
 Revision: New
 Hazard Analysis Of: SAFER II Pyrovalve Qualification Test (Vibration & Thermal Cycling only)
 Building: 352
 Prepared By: Test Manager
 Organization: EP6
 Telephone: x 38799

Prepared By: _____
 Preparer
 Concurrence: _____
 Test Group Leader
 Concurrence: _____
 NASA Facility Manager
 Approved By: _____
 NASA Safety Office
 Approved By: _____
 NASA ESTB Office

Note: The RAC code shown here is a 6 X 6 Matrix, not the 4 X 4 which is shown in this document.

13

<u>Risk Assessment Code (RAC)</u>	<u>Probability Estimate</u>			
Severity Class	A	B	C	D
I	1	1	2	2
II	1	2	3	3
III	2	3	4	4
IV	3	3	4	4

RAC 1's will be considered imminent danger and require immediate attention.
 RAC 2's are serious and will require priority attention.
 RAC 3-6's are nonserious, but will be corrected in RAC order.

Severity Classes:

- I Catastrophic - may cause death or major system destruction.
- II Critical - may cause severe injury, severe occupational illness, or major property damage.
- III Marginal - may cause minor occupational illness or property damage.
- IV Negligible - probably would not affect personnel safety or health, but is a violation of specific criteria.

Probability Codes:

- A Likely to occur immediately.
- B Probably will occur in time.
- C May occur in time.
- D Unlikely to occur.

Hazard Analysis for SAFER II Pyrovalve Qualification Test

Test Purpose:

The primary objective of this program is to perform qualification testing for the simplified aid for extravehicular activity rescue II (SAFER II) pyrovalve.

System Functional Description:

The test matrix for the SAFER II Pyrovalve qualification testing will include: vibration, thermal cycling, three ambient test firings with 8000 psig at the pyrovalve input, three +168°F test firings with 10 000 psig at the pyrovalve input, three -20°F test firings with 5,750 psig at the pyrovalve input, one 85% pyrovalve firing at -20°F with 5750 psig at the pyrovalve input, one 115% pyrovalve firing at +168°F with 10 000 psig at the pyrovalve input, and one lock shut pyrovalve test firing. This Hazard Analysis will cover the vibration and thermal cycling hazards only.

Hazard Analysis Summary:

The major hazards associated with the vibration and thermal cycling are: 1) electrical potential, 2) projectiles or blast wave overpressure due to unintentionally initiating initiator, 2) high-temperature environment due to intentionally heating the test article to +168°F, 3) low temperature environment due to intentionally cooling the test unit to -20°F, and 4) loud sound levels during 5-minute vibration. These hazards are controlled by training and procedures. Controls are verified by procedures review and signatures and certification review by the TRRB.

Name: Maureen Dutton

Documents Reviewed:

Drawings and Component Listings:

8Z011Q ICD

Procedures:

ESTA-T-8Z011Q

NASA Documents:

JSC 17773B, Instructions for Preparation of Hazard Analysis for JSC Ground Operations

JSC-ESTA General Operating Procedure

HAZARD (Hazardous Environment)	CAUSE	EFFECT	Sev./Prob /RAC	CONTROLS	VERIFICATION	DISPOSITION
Electrical Potential	115 VAC support equipment power	Electrical burns, respiratory and/or cardiac arrest due to electrical current flow through victim to ground potential	I C 2	Certified electrical technicians UL approved equipment	TRRB review of certifications TRRB inspection of setup	Controlled
Projectiles or Blast Wave Overpressure	Unintentional initiation of initiator	Death or serious injury	IC 2	Certified pyrotechnic handlers required. Shorting springs installed on initiators. Grounding strap worn when handling initiators Faraday caps installed Thermal chamber heat safety limit is set at 200°F	TRRB review of certifications. Step 3.3.8 in TTA-OC-2-30 Step 3.1.5 of TS9620142 Step 3.1.7 of TS9620142 Step 3.3.1 of TS9620142	Controlled
Ionizing Radiation (Gamma-Xray, Beta-electron, Alpha-proton, Neutron particle radiation)	None	N/A	N/A	N/A	N/A	N/A
High-Energy Electromagnetic Fields (Electric, Magnetic, Microwave, Laser)	None	N/A	N/A	N/A	N/A	N/A
Oxygen-Deficient Atmosphere	None	N/A	N/A	N/A	N/A	N/A
Toxic Atmosphere	None	N/A	N/A	N/A	N/A	N/A
High Temperature Environment or Surfaces	Intentionally heating test articles to +168°F	Severe burns	II C 3	Test articles will only be handled by personnel when the units are at ambient temperature	Warning statement at beginning of Thermal Cycling procedure in TS9620142	Controlled
Low Temperature Environment or Surfaces	Intentionally cooling test articles to -20°F	Freeze-burning of skin	II C 3	Test articles will only be handled by personnel when the units are at ambient temperature	Warning statement at beginning of Thermal Cycling procedure in TS9620142	Controlled
High Sound Levels	None	N/A	N/A	N/A	N/A	N/A
Sharp Edges or Points	None	N/A	N/A	N/A	N/A	N/A
Collisions With Animate or Inanimate Objects	None	N/A	N/A	N/A	N/A	N/A

Crushing Forces	None	N/A	N/A	N/A	N/A	N/A
-----------------	------	-----	-----	-----	-----	-----

Appendix D Hazard and Operability Study

1 What is a HAZOP?

A HAZOP is a systematic approach to identify hazards in a process or operation and the inefficiencies in a facility or system.

2 What are the advantages to performing a HAZOP?

A HAZOP:

- Looks at process deviations.
- Uses a synergistic team approach.
- Breaks even the most complex systems into manageable pieces.
- Not only looks at safety hazards, but can also identify operability, maintenance, and environmental hazards.
- Looks at most of the possibilities during the analysis and then, based on the objectives and scope of the analysis, can limit the number of causes that are investigated further.

3 What are the disadvantages of a HAZOP?

The disadvantages of performing a HAZOP are:

- It's expensive to perform due to the number of personnel involved on the teams.
- It requires good documentation.

4 When would I do a HAZOP and who should do it?

The HAZOP is an extremely useful tool for very complex systems. Although normally used for process flows in the process industry, it can be used for analyzing any fluid or electrical systems.

A team of 3 to 9 people should do the HAZOP. The team should include process engineers, operational personnel, safety personnel, maintenance personnel, and other subject matter experts. Use a core team for the whole process and bring in subject matter experts to help as needed.

The team should have a leader, a facilitator, and a recorder. The facilitator keeps the group focused on the analysis if the team gets hung up on discussion. The recorder must be able to support the team dynamics and not slow down the process.

5 What information do I need to do a HAZOP?

You need the following kind of information for the HAZOP:

- Process and instrument drawings
- Facility drawings and plant site maps
- Process flow diagrams
- Operation procedures
- Hazard analyses or other safety reports
- Past mishap and incident reports
- Interlock descriptions and classifications
- Operating parameters
- Instrumentation set parameters
- Equipment specifications (pressure vessel capacities, maximum design pressures, other design specifications, as applicable to the system being analyzed)
- Other HAZOPs of similar systems

6 Steps for doing a HAZOP

Follow these basic steps:

- Define the objectives and scope.
- Gather the information.
- Select the team to do the analysis.
- Conduct the HAZOP using the detailed steps in paragraphs 7 – 11 below.
- Document the results.
- Track the hazard control implementations.

7 Break down the system to be analyzed into manageable “nodes.”

A node is a location where the parameters of the system change. Interfaces of functional areas are good node breakpoints. Some examples of good node breakpoints are:

- The interface between the test fixture and the test article.
- The interface between the potable water system and the building.

8 Choose the guidewords and modifiers to use for each node

Work down a list of guidewords and modifiers to determine which ones apply to the node.

Some of the guidewords you can use include, but are not limited to:

- Flow
- Pressure
- Temperature
- Signal

- Others, as dictated by the system being analyzed

Modifiers are words that modify the guidewords to further identify the hazards. These include, but are not limited to:

- No
- More
- Less
- As well as
- Part of
- Reverse
- Other than

9 Apply the guidewords and modifiers to each node

For each node:

- Apply each guideword with applicable modifiers to the node and determine all the causes for the condition as described by the guideword and modifier.
- Analyze each cause to determine what the consequences are from the condition, without any controls in place.
- Determine the effect of each consequence—does this condition affect safety, the environment, operability, maintenance, etc. If it does not affect any of these items, move on to the next cause. If it does, determine the severity and probability of occurrence without controls in place.

10 Why do we look at the consequences without controls, even if we have controls in place?

To determine the worst-case situation that could occur. If controls are already in place, then look at the situation where all or part of the controls fail (multiple failures commonly occur).

11 List all existing controls and determine what additional controls are necessary

To determine if additional controls are necessary:

- Determine the severity and probability of occurrence for the consequence with all the controls in place. If the controls do not affect the severity and probability of occurrence for the condition, then additional controls may be required, depending on the severity and probability without controls.
- If additional controls are required, then list them on the worksheet. (Don't try to engineer the controls at this time.)
- Assign actions to team members or others to determine how to provide the additional controls and report back to the team at a later time.
- Analyze the controls when they are reported back to determine how they affect the severity and probability of occurrence.

Hazard and Operability Study (HAZOP) Example

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left;">Node Information</th> <th style="text-align: left;">Date</th> <th style="text-align: left;">Time</th> </tr> <tr> <td>Cover : <input type="text" value="1"/></td> <td><input type="text" value="12/30/94"/></td> <td><input type="text" value="10:16 AM"/></td> </tr> <tr> <td>Node ID: <input type="text" value="01"/></td> <td colspan="2">PHA Type</td> </tr> </table> <p style="text-align: center;">© DiGraphics, Inc.</p> <p>Project</p> <p>Water Purification System for JSC</p> <hr/> <p>Node Description</p> <p>This node is the water coming into JSC, either from Clear Lake Water Authority, City of Houston, or from the 2 underground wells.</p> <hr/> <p>Design Intention</p> <p>The intention of this node is to provide safe potable water to JSC</p>	Node Information	Date	Time	Cover : <input type="text" value="1"/>	<input type="text" value="12/30/94"/>	<input type="text" value="10:16 AM"/>	Node ID: <input type="text" value="01"/>	PHA Type		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left;">Project Information</th> <th style="text-align: left;">Archived</th> </tr> <tr> <td>Project ID <input type="text" value="1"/></td> <td>Created <input type="text" value="11/26/96"/></td> </tr> <tr> <td colspan="2">Company <input type="text" value="NASA"/></td> </tr> <tr> <td colspan="2">Facility <input type="text" value="Building 322A"/></td> </tr> <tr> <td colspan="2">Unit <input type="text"/></td> </tr> </table> <hr/> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="3" style="text-align: left;">Project Drawings</th> </tr> <tr> <th style="text-align: left;">Drawing</th> <th style="text-align: left;">Revision</th> <th style="text-align: left;">Reference</th> </tr> <tr> <td><input type="text" value="M-322A-103, SR-M7"/></td> <td><input type="text" value="FOR #2"/></td> <td><input type="text" value="NAS-9-19413"/></td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> </table> <hr/> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="3" style="text-align: left;">PHA Team Members</th> </tr> <tr> <th style="text-align: left;">Name</th> <th style="text-align: left;">Phone</th> <th style="text-align: left;">Company</th> </tr> <tr> <td><input type="text" value="John Byard"/></td> <td><input type="text" value="36705"/></td> <td><input type="text" value="JCWS"/></td> </tr> <tr> <td><input type="text" value="Pat Kolkmeier"/></td> <td><input type="text" value="33131"/></td> <td><input type="text" value="NASA"/></td> </tr> <tr> <td><input type="text" value="Perry Piplani"/></td> <td><input type="text" value="33194"/></td> <td><input type="text" value="NASA"/></td> </tr> <tr> <td><input type="text" value="Howard Sloan"/></td> <td><input type="text" value="35325"/></td> <td><input type="text" value="HEI"/></td> </tr> <tr> <td><input type="text" value="Charis Pattison"/></td> <td><input type="text" value="35287"/></td> <td><input type="text" value="JCWS"/></td> </tr> <tr> <td><input type="text" value="Bob Seiwel"/></td> <td><input type="text" value="36348"/></td> <td><input type="text" value="HEI"/></td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> </table>	Project Information	Archived	Project ID <input type="text" value="1"/>	Created <input type="text" value="11/26/96"/>	Company <input type="text" value="NASA"/>		Facility <input type="text" value="Building 322A"/>		Unit <input type="text"/>		Project Drawings			Drawing	Revision	Reference	<input type="text" value="M-322A-103, SR-M7"/>	<input type="text" value="FOR #2"/>	<input type="text" value="NAS-9-19413"/>										PHA Team Members			Name	Phone	Company	<input type="text" value="John Byard"/>	<input type="text" value="36705"/>	<input type="text" value="JCWS"/>	<input type="text" value="Pat Kolkmeier"/>	<input type="text" value="33131"/>	<input type="text" value="NASA"/>	<input type="text" value="Perry Piplani"/>	<input type="text" value="33194"/>	<input type="text" value="NASA"/>	<input type="text" value="Howard Sloan"/>	<input type="text" value="35325"/>	<input type="text" value="HEI"/>	<input type="text" value="Charis Pattison"/>	<input type="text" value="35287"/>	<input type="text" value="JCWS"/>	<input type="text" value="Bob Seiwel"/>	<input type="text" value="36348"/>	<input type="text" value="HEI"/>									
Node Information	Date	Time																																																																					
Cover : <input type="text" value="1"/>	<input type="text" value="12/30/94"/>	<input type="text" value="10:16 AM"/>																																																																					
Node ID: <input type="text" value="01"/>	PHA Type																																																																						
Project Information	Archived																																																																						
Project ID <input type="text" value="1"/>	Created <input type="text" value="11/26/96"/>																																																																						
Company <input type="text" value="NASA"/>																																																																							
Facility <input type="text" value="Building 322A"/>																																																																							
Unit <input type="text"/>																																																																							
Project Drawings																																																																							
Drawing	Revision	Reference																																																																					
<input type="text" value="M-322A-103, SR-M7"/>	<input type="text" value="FOR #2"/>	<input type="text" value="NAS-9-19413"/>																																																																					
PHA Team Members																																																																							
Name	Phone	Company																																																																					
<input type="text" value="John Byard"/>	<input type="text" value="36705"/>	<input type="text" value="JCWS"/>																																																																					
<input type="text" value="Pat Kolkmeier"/>	<input type="text" value="33131"/>	<input type="text" value="NASA"/>																																																																					
<input type="text" value="Perry Piplani"/>	<input type="text" value="33194"/>	<input type="text" value="NASA"/>																																																																					
<input type="text" value="Howard Sloan"/>	<input type="text" value="35325"/>	<input type="text" value="HEI"/>																																																																					
<input type="text" value="Charis Pattison"/>	<input type="text" value="35287"/>	<input type="text" value="JCWS"/>																																																																					
<input type="text" value="Bob Seiwel"/>	<input type="text" value="36348"/>	<input type="text" value="HEI"/>																																																																					

4/23/98

Page 1

Rec.	Proj.	Session	Guideword	Causes
1	00194	001	No/Less Flow	No water to the 600 PSIG supply line.
2	00194	001	No/Less Flow	1 1/2" Valve between supply and throat closed
3	00194	001	No/Less Flow	All 4 supply flex lines disconnected
4	00194	001	No/Less Flow	1 1/2" valve between throat and return closed
5	00194	001	No/Less Flow	600 PSI supply not supplying enough water
6	00194	001	No/Less Flow	1 1/2" Valve between supply manifold and the throat partially closed
7	00194	001	No/Less Flow	Any of the 4 supply flex lines not connected or leaking.
8	00194	001	No/Less Flow	Any of the 4 return flex lines not connected or leaking
9	00194	001	No/Less Flow	1 1/2" Valve between throat and return manifold partially closed.
10	00194	001	No/Less Flow	Return manifold not flowing properly
11	00194	001	No/Less Flow	Any of the 4 each supply and return flex lines hooked up improperly
12	00194	001	No/Less Flow	Pressure greater than 600 PSI supplied to supply manifold.
13	00194	001	No/Less Flow	Water jacket not providing cooling water flow.
14	00194	001	No/Less Flow	Loss of cooling water to pond.
15	00194	001	No/Less Flow	All 4 return flex lines disconnected.
16	00194	001	No/Less Flow	No water to the 600 PSI supply line.
17	00194	001	No/Less Flow	3/4" Valve between supply and 7" Section closed
18	00194	001	No/Less Flow	Relief Valve open and flowing.
19	00194	001	No/Less Flow	Burst disc open and flowing
20	00194	001	No/Less Flow	All 6 flex lines between the supply and the 7" section not connected.
21	00194	001	No/Less Flow	All 6 flex lines between the 7" section and the return manifold not
22	00194	001	No/Less Flow	2.0" Valve between 7.0" section and return manifold closed.
23	00194	001	No/Less Flow	Return manifold not flowing.
24	00194	001	No/Less Flow	600 PSI supply not supplying enough water
25	00194	001	No/Less Flow	3/4" Valve between supply and 7.0" section partially closed.
26	00194	001	No/Less Flow	Any of the 6 supply flex lines not connected or leaking.
27	00194	001	No/Less Flow	Any of the 6 return flex lines not connected or leaking.
28	00194	001	No/Less Flow	Any of the 6 return flex lines not connected or leaking.
29	00194	001	No/Less Flow	2.0" Valve between 7.0" section and return manifold partially closed.
30	00194	001	No/Less Flow	Any of the 6 each supply and return flex lines hooked up improperly

Data Entry

Section / Node Throat section/node 1 is the coolant water thru the throat assembly designed to operate at full coolant		Mod Date 9/27/94	Session ID 001	Project ID 00194	Risk Before Safgrds C F R 2 2 2		
		Record 1	© DGraphics, Inc.			After Safgrds C F R 4 5 4	
Guide Word No/Less Flow	Condition / Status Startup	Other Factors Flooding	Type 3 Operability				
Possible Causes No water to the 600 PSIG supply line.	Consequences / Effects Loss of Nozzle, Arc Heater, and Test Article(s). Potential of high voltage into the control room thru instrumentation lines with risk of personnel injury or loss of life.	Safeguards PT 331A PDT 331 FE331 PT, FE 332 PT, FE 333 PT, FE 345 PT 301					
Other Considerations <ul style="list-style-type: none"> SOP 113.0, Coolant water System Emergency Procedures (per DTP) Closed circuit TV Test Team Members alert to testing operations 	Action No Action Required						

HazPro

Session Summary

Guideword	Causes	Consequences	Safeguards	Other Considerations	Action
<p>No/Less Flow</p> <p>Type</p> <p>S Operability</p> <p>RISK Ranking</p> <p>Before After</p> <p>F 2 4</p> <p>C 2 5</p> <p>R 2 4</p> <p>Rec. Ser ID</p> <p>1 001</p>	No water to the 600 PSIG supply line.	Loss of Nozzle, Arc Heater, and Test Article(s). Potential of high voltage into the control room instrumentation lines with risk of personnel injury or loss of life.	PT 331A BDT 331 FE 331 PT, FE 332 PT, FE 333 PT, FE 345 PT 301	<ul style="list-style-type: none"> SOP 113.0, Coolant water System Emergency Procedures (per OYP) Closed circuit TV Test Team Members alert to testing operations 	No Action Required

Appendix E

Failure Mode and Effects Analysis (FMEA)

1 What is a FMEA?

A FMEA is a reliability engineering tool that the system safety community and OSHA have adopted as a safety tool for analyzing system failures that could cause a hazard. To put it another way, a FMEA is an analytical tool to identify all the ways that a component can fail, and what are the effects of the failure on the system.

2 When should I use a FMEA?

Use it after other hazard analysis techniques have identified safety-critical systems that need further analysis.

FMEAs analyze systems at the lowest level to determine the hazard associated with component failure, and how the failures affect the overall mission performance of the safety critical system.

3 What are the advantages a FMEA?

A FMEA:

- Is a very systematic approach.
- Looks at every component to determine failure effects.

4 What are the disadvantages of a FMEA?

A FMEA:

- Only looks at hazards associated with failures, not those associated with normal operations.
- Only looks at the hardware failures, not the interaction between personnel, equipment or environment.
- Is very laborious to perform.
- Does not identify all hazards associated with a system, even if it identifies all single-point failures.

5 Steps for doing a FMEA

How well these steps are done determines the quality of the FMEA. The steps are as follows:

- Define the system and the scope and boundaries of the analysis. (What is the lowest level that I want to analyze? Do I consider the structural integrity of the tubing?, etc.)
- Construct a functional block diagram showing the relationship between the different system levels.
- Assess each functional block and determine if its failure would affect the rest of the system.
- Use a bottom-up type approach to determine the effects of failure of each component. List the modes or ways that the component can fail.

- For each failure mode determine the worst credible effect and determine a severity and probability of occurrence.
- Identify whether the failure is a single-point failure. (A single-point failure is a failure of a single component that could cause complete failure of the mission or loss of the system.)
- Determine corrective actions. (These can prevent the failure or mitigate the effects of the failure.)
- Document the failure on the worksheet.

FMEA Example Table of Contents

1. SUBJECT	26
2. PURPOSE	27
3. SCOPE.....	27
4. APPLICABLE DOCUMENTS	28
5. SUMMARY.....	28
6. COMPONENT FAILURE MODE	28
CHEMICAL ANALYSIS	30
<i>Tank Analysis</i>	30
<i>Secondary Containment #1</i>	31
<i>Secondary Containment #2</i>	<i>Not Shown</i>
<i>Secondary Containment #3</i>	<i>Not Shown</i>
ELECTRICAL ANALYSIS	32
<i>Master Control Panel</i>	32
<i>Control Panel Process Line #1</i>	35
<i>Control Panel Process Line #2</i>	<i>Not Shown</i>
<i>Control Panel Process Line #3</i>	<i>Not Shown</i>
<i>Control Panel Process Line #4</i>	<i>Not Shown</i>
<i>Control Panel Process Line #5</i>	<i>Not Shown</i>
<i>Control Panel Process Line #6</i>	<i>Not Shown</i>

1. SUBJECT

This report addresses the Failure Modes and Effects Analysis (FMEA) for the PLASFAB metal finishing system in Building 9 S, room 1020 (and 1024). This facility system will be used to facilitate the processing of mainly aluminum pieces with either anodized or chromate finish and the electro-polishing of stainless steel pieces.

The room enclosing the system has a chemical resistant subfloor for total secondary containment of chemistry. Structural support for working area is fiberglass I-beams and grating. Tanks are polypropylene and stainless steel. All heated metal tanks are insulated. The fluid handling lines are all hard piped constructed from PVC, CPVC, stainless steel, or black iron, and their mains are located beneath the grating. All electrical components are NEMA-rated for water and chemical resistance and UL-listed. All electrical wire runs are contained in PVC conduit. The air supply system is provided by a regenerative-style blower with filters and mufflers. The ventilation/ exhaust system is constructed of polypropylene and PVC; the exhaust plenums are mounted behind each tank and routed beneath the grating.

Failure modes are assigned a RAC (risk assessment code) before and after installation of countermeasures (uncontrolled and controlled.) The RAC is the third number of three; the first two being the matrix coordinate that determines the RAC number.

FMEA Example (continued)

Risk Assessment Code

Severity Classes:

- I Catastrophic - May cause death or major system damage.
- II Critical - May cause sever injury, sever occupational illness, or major property damage.
- III Marginal - May cause minor occupational illness or property damage.
- IV Negligible - Probably would not affect personnel safety or health, but is a violation of specific criteria.

Probability Codes:

- A Likely to occur immediately.
- B Probably will occur in time.
- C May occur in time.
- D Unlikely to occur.

RAC code:

Severity Class	Probability Estimate			
	A	B	C	D
I	1	1	2	3
II	1	2	3	3
III	2	3	4	4
IV	3	3	4	4

RAC 1's will be considered imminent danger and require immediate attention.

RAC 2's are serious and will require priority attention.

RAC 3 & 4's are nonserious but will be corrected in RAC order.

2. PURPOSE

The purpose of this FMEA is to evaluate the metal finishing system (PLASFAB-Metal Finishing Processing Line) and identify single-point component failure in the system that could result in injury to operating personnel and/or damage to tool or equipment.

3. SCOPE

Each credible single-point failure mode is considered. Operator error is not considered. Structural failures of non-dynamic items such as piping, valve bodies, mounting brackets, fasteners, frames, and electrical wiring runs are not considered except when these components are used in an environment where their failure is significantly more probable than in a more static environment. Systems which feed into the metal finishing area, such as utilities, are treated each as an input component.

**FMEA Example
(continued)**

4. APPLICABLE DOCUMENTS

DWG 100421-1, 100421-1, 100423, 100424, 100425, 100426, 100427, and 100428; PLASFAB.
DWG 500160 PLASFAB. (16 Sheets)
DWG A-9-3, E-9-27C, M-9-73A, & M-9-98A NASA Facility Drawings .
DWG 1, 1.1, 1.2, 1.3, & 2. SEASAFE FRP Structural.
PLASFAB “CLIN 0001-0003”

5. SUMMARY

This FMEA showed the following list of Critical Items. Critical Items are those failure modes that the criticality assessed as 1 or 2.

Rectifier delivery system.

Criticality I : An exposed buss system. Personnel contact with activated bare buss without proper PPE.

Steam Solenoid.

Criticality II: Fails to close or leaks internally, causing continuous heating/overheating.

6. COMPONENT FAILURE MODE

[N/O = Normal Open, N/C = Normal Closed]

The **Metal Finishing** system has been broken into **Line Operation** and **Utilities** supplying the system and the lines, which are factors relative to system operation. The **Line Operation** is subdivided to the **Tanks** and their chemistry. The **Tanks** are further subdivided to **component** level and control interface.

The system is to provide metal-finishing capabilities; a pre-clean Tank # 1-9 to be used prior to anodizing and Chemfilm processes, Class I (clear) anodizing, Class II (colored) anodizing, Chemfilm, and electropolish provided by six lines.

Line # 1 is tank # 1, 2, 3, 4, 5, and 6.

Line #1 is the pre-clean line with an alkaline cleaner (Oakite Inpro-Clean 3000) to remove light oils, grease, and ink with tandem cascade rinses; and an alkaline etch (Oakite 360L) to light etch to improve the adhesion of subsequent coatings. This line is controlled by the master control panel activation, located at entrance and operation of control panel line #1 located at the end of the line just above tank #6.

“Pre-clean” also includes tanks # 7, # 8, and # 9 of line # 2, an acidic deoxidizer (Oakite Deoxidizer LNC) and its cascade rinse.

**FMEA Example
(continued)**

Line # 2 is tank # 7, 8, 9, 10, 11, and 12.

Line #2 is the deoxidizer (Oakite Deoxidizer LNC) and cascade rinses of the Pre-clean and the Type II, Class I anodizing tanks (MIL-A-8625). The anodizing sealer tank (#13) for Class I is located on Line #3.

Line #3 is tank # 13, 14, 15, 16, and 17.

Line #3 is the sealer tank for Type II, Class I anodizing and the Alodine tanks; Tank # 14 is the Alodine 600S, Tank # 15 is a DI water drag-out and tanks # 16 and # 17 are a cascade rinse.

Line # 4 is Tank # 18 and 19.

Line #4 is the blue (Type II, Class II, and Blue) anodizing pigment and rinse. The sealer and rinse for this process is tank # 22, and # 23 of line # 5.

Line # 5 is Tank # 20, 21, 22, and 23.

Line # 5 is the black (Type II, Class II, and Black) anodizing pigment, rinse, sealer (nickel acetate) and rinse.

Line # 6 is tank # 24, 25, 26, 27, 28, and 29.

Line # 6 is the electropolish with a heated alkaline cleaner, an ambient cascade rinse, heated "Electrogleam 55," an ambient single rinse, and a sealer tank for another process (tank 29 will not be used).

**FMEA Example
(continued)**

Chemical Analysis Tank Analysis

Tank #1	Cleaner Oakite INPRO-Clean 3000 OSHA Hazard Class: B2 (Without air sparge; B1 with air sparge.) Caustic Amine Ethoxylate <5% Nonionic Surfactant <5% Sodium Silicate <5%	Tank Temperature: 170 F VAPOR: SG: 1.131; D 9.44 #/Gal. (Soap) 0073138279 0060828786 0001344098	Ph sol	Ph Conc
	Haz. Eye Irritant Skin Irritant Inhalation Irritant Ingestion Irritant		12.7	13.8
Tanks # 2 and 3	Cascade Rinse DI Water OSHA Hazard Class: D4 Rinse Air Sparger	Tank Temperature: Ambient. 750 Conductivity controller	Ph sol	Ph Conc
Tank # 4	Etch Oakite Etch 360L OSHA Hazard Class: B3 (Without air sparge; B1 with air sparge.) Caustic Sodium Hydroxide 40-50%bw	Tank Temperature: 120 F VAPOR:<18 mm/Hg @20C SG: 1.505; D 12.5 #/Gal. 4 % solution 0001310732	Ph sol	Ph Conc
	Haz. Eye Irritant Skin Irritant Inhalation Irritant Ingestion Irritant		13.1	
Tanks # 5 and 6	Cascade Rinse DI Water OSHA Hazard Class: D4 Rinse Air Sparger	Tank Temperature: Ambient 750 Conductivity controller	Ph sol	Ph Conc

FMEA Example

(continued)

Secondary Containment #1

Tank 1	Amine Ethoxylate <5%
	Nonionic Surfactant <5%
	Sodium Silicate <5%
Tank 4	Sodium Hydroxide 40-50% bw
Tank 7	TSR 30-40 % by wt. Nitric Acid 11% (15-25%/wt) Stainless Steel Tank / MSDS Air Sparger
Tank 10	Sulfuric Acid 10 % Air Sparger

**FMEA Example
(continued)**

Electrical Analysis Master Control Panel

COMPONENT: “FU” Main Fuse, 40 A

Condition: Limits electrical current to maximum allowable for the 6-line control panels.

Failure: Component fails to operate and exceeds current limitations.

Effect: Electrical components are protected by line fusing and control circuit fusing to keep components from being overdriven to malfunction or burn out.

RAC: Uncontrolled: III / C / 4 Controlled: IV / C / 4

Remarks & controls: Each line and control circuit is fused for individual load capacity.

Condition: Limits electrical current to maximum allowable for the 6-line control panels.

Failure: Component operates prior to reaching allowable current limit.

Effect: Premature shutdown of lines.

RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4

Remarks & controls: This failure would be corrected via troubleshooting and maintenance routines.

COMPONENT: “AFU” Controller Fuse, 1A

Condition: Limits electrical current to maximum allowable for control circuitry.

Failure: Component fails to operate and exceeds current limitations.

Effect: Electrical components may be overdriven to malfunction or burn out.

RAC: Uncontrolled: III / C / 4 Controlled: IV / C / 4

Remarks & controls: Components and wire gauge are designed to limit overload.

Condition: Limits electrical current to maximum allowable for control circuitry.

Failure: Component operates prior to reaching allowable current limit.

Effect: Premature shutdown of lines.

RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4

Remarks & controls: This failure would be corrected via troubleshooting and maintenance routines.

COMPONENT: “1PB” “Power On” Push Button

Condition: Provides momentary lockup path for Master Control Relay (MCR).

Failure: Fails to provide initial path for MCR lockup.

Effect: Each line will not be powered.

**FMEA Example
(continued)**

Condition: Provides momentary lockup path for MCR.
Failure: Fails to disengage when released.
Effect: Continuous power to MCR. Each line controller will not shut off.
RAC: Uncontrolled: III / C / 4 Controlled: IV / C / 4
Remarks & controls: Continuous operator monitoring and problem identification at shutdown. Supplied power must be shut off and component replaced.

COMPONENT: “2PB” E-Stop Push Button

Condition: Breaks the path to and de-energize the MCR.
Failure: Fails to break path to MCR.
Effect: Power is applied to line controllers.
RAC: Uncontrolled: III / C / 4 Controlled: IV / C / 4
Remarks & controls: Continuous operator monitoring and problem identification at shutdown. Individual lines may be shut down individually and remove main power. Supplied power must be shut off and component replaced.

COMPONENT: “MCR” Master Control Relay

Condition: Provides power for relay lockup and primary power for line controllers.
Failure: Contacts fail to provide relay lockup.
Effect: Lines will not power up.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Green light will not be sustained, relay will not lock up, and line buss will not be powered. No system function will operate. Requires component replacement.

Condition: Provides power for relay lockup and primary power for line controllers.
Failure: Contacts fail to provide power to the line buss.
Effect: Green light and relay will lock up, but power will not be applied to line buss.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Master “on” light will indicate power to lines, but none of the lines will have power. Component replacement required.

Condition: Provides power for relay lockup and primary power for line controllers.
Relay is disengaged, contacts stick.
Failure: Contacts fail to disengage to release relay lockup.
Effect: MCR remains engaged with green light. Power to line buss is applied.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Individual lines and main power will have to be removed.
Component replacement required.

**FMEA Example
(continued)**

Condition: Provides power for relay lockup and primary power for line controllers.
Relay is disengaged, contacts stick.
Failure: Contacts fail to disengage power to the line buss.
Effect: Relay disengages, green light extinguishes, but line buss is powered.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Procedural shutdown of each line prior to shutdown of master power is off.

COMPONENT: “1LT” Light, Green, Power On

Condition: Lit light indicates MCR lockup through relay contacts.
Failure: Bulb burns out.
Effect: MCR will not lock up, and power is not applied to lines.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Design. Bulb is in parallel with relay and is indication only.

COMPONENT: “2LT” Light, Red, Power Off (E-Stop)

Condition: Supplied voltage when E-Stop is pushed. E-Stop pushed, and MCR de-energized.
Failure: Bulb burns out.
Effect: No indication of MCR shutdown.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Design. Bulb is in parallel with relay, lockup contacts, and the green light and is indication only.

COMPONENT: “1FU” Fuse, Line #1 Main Fuse, 20A

Condition: Limits electrical current to maximum allowable for the line control panel.
Failure: Component fails to operate and exceeds current limitations.
Effect: Electrical components may be overdriven to malfunction or burn out.
RAC: Uncontrolled: III / C / 4 Controlled: IV / C / 4
Remarks & controls: Line and control circuit is fused for individual load capacity. Electrical components are protected by main fusing (40A) and control circuit fusing (1A). All fuses are double/triple fused.

Condition: Limits electrical current to maximum allowable for the 6-line control panels.
Failure: Component operates prior to reaching allowable current limit.
Effect: Premature shutdown of lines.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: This failure would be corrected via troubleshooting and maintenance routines.

**FMEA Example
(continued)**

Control Panel Process Line #1

COMPONENT: "1CFU" Fuse, 1A

Condition: Limits electrical current to maximum allowable for the line#1 control panel and components.

Failure: Component fails to operate and exceeds current limitations.

Effect: Electrical components may be overdriven to malfunction or burn out.

RAC: Uncontrolled: III / C / 4 Controlled: III / C / 4

Remarks & controls:

COMPONENT: "101PB" Power On Push Button

Condition: Provides momentary lockup path for "1ESR" (Emergency Stop Relay).

Failure: Fails to provide initial path for 1ESR lockup.

Effect: The line will not be powered.

RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4

Remarks & controls: Maintenance required.

COMPONENT: "102PB" Power Off (E-Stop) Push Button

Condition: Breaks the path to and de-energize the 1ESR relay.

Failure: Fails to break path to 1ESR

Effect: Power is applied to the line components.

RAC: Uncontrolled: III / C / 4 Controlled: IV / C / 4

Remarks & controls: Continuous operator monitoring and problem identification at shutdown. (green light will remain on) Individual components may be shut down and remove power. Supplied power must be shut off and component replaced.

COMPONENT: "1ESR" Relay E-Stop

Condition: Provides power for relay lockup and primary power for line components.

Failure: Contacts fail to provide relay lockup.

Effect: Lines will not power up.

RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4

Remarks & controls: Green light will not be sustained, relay will not lock up, and component buss will not be powered. No line component will operate. Requires component replacement.

**FMEA Example
(continued)**

Condition: Provides power for relay lockup and primary power for line components.
Failure: Contacts fail to provide power to the component buss.
Effect: Green light and relay will lock up, but power will not be applied to line buss.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Power “on” light (**101LT**) will indicate power to line, but no power will be applied to component buss. Component replacement required.

Condition: Provides power for relay lockup and primary power for line components. Relay is disengaged , contacts stick.
Failure: Contacts fail to disengage to release relay lockup.
Effect: **1ESR** remains engaged with green light. Power to line buss is applied.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Individual components will have to be powered off with selector switch and main power removed. Component replacement required.

Condition: Provides power for relay lockup and primary power for line components. Relay is disengaged , contacts stick.
Failure: Contacts fail to disengage power to the line buss.
Effect: Relay disengages, green light extinguishes, but component buss is powered.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Procedural shutdown of each line prior to shutdown of master power is off.

COMPONENT: “101TC” Temperature Control for Tank #1

Condition: Controls **101SV** to provide heat to tank.
Failure: Fails to provide signal to **101SV** to open solenoid valve.
Effect: Tank temperature falls to ambient.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Procedural control by monitoring process.

Condition: Controls **101SV** to provide heat to tank.
Failure: Fails to provide signal to **101SV** to close solenoid valve.
Effect: Tank temperature rises.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Procedural control by monitoring process.

COMPONENT: “101SV” Steam (Heating) Solenoid (elec.) for Tank #1

Condition: Electrical motor operating spring loaded (NC) steam valve.
Failure: Fails to operate steam valve upon demand.
Effect: Tank temperature falls to ambient.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Procedural control by monitoring process.

**FMEA Example
(continued)**

COMPONENT: **“102TC” Temperature Control for Tank #4**

Response is like “101TC”

COMPONENT: **“102SV” Steam (Heating) Solenoid (elec.) for Tank #4**

Response is like “101SV”

COMPONENT: **“103CC” Conductivity Controller for Tank #2 (2/3)**

Condition: Provides signal to water inlet solenoid to open to flush tanks 2 & 3.

Failure: Fails to provide signal when contamination is present.

Effect: Rinse water becomes contaminated.

RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4

Remarks & controls: Procedural control by visually monitoring process.

COMPONENT: **“103SV” Water Inlet Sparge Solenoid, Tank #3 (2/3)**

Condition: Electrical motor operating spring loaded (NC) water valve.

Failure: Fails to operate water valve upon demand.

Effect: Rinse water becomes contaminated.

RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4

Remarks & controls: Procedural control by monitoring process.

COMPONENT: **“104CC” Conductivity Controller for Tank #5 (5/6)**

Response is like “103CC”

COMPONENT: **“104SV” Water Inlet Sparge Solenoid, Tank #6 (5/6)**

Response is like “103SV”

COMPONENT: **“105ALT” Light White**

Condition: Indicates power is selected to for liquid level controller boards.

Failure: Light fails to illuminate. Bulb failure.

Effect: Light is indication only, it is parallel with boards.

RAC: Uncontrolled

Remarks & controls: Bulb replacement required.

COMPONENT: **#1 Circuit Board, Line #1 Controller Panel, Tank #1
(Controls Autofill Solenoid)**

Condition: *Input:* medium probe, *Output:* Water fill OFF

Failure: Water delivery fails to halt when level reaches medium probe.

Effect: Tank continues to fill.

RAC: Uncontrolled: III / C / 4 Controlled: III / C / 4

Remarks & controls: Procedural control by visually monitoring process. And hi-level alarm.

**FMEA Example
(continued)**

Condition: *Input:* Long probe, *Output:* Water fill ON.
Failure: Water delivery is not initiated when level reaches long probes.
Effect: Tank level is maintained or continues to recede.
RAC: Uncontrolled: III / C / 4 Controlled: III / C / 4
Remarks & controls: Procedural control by visually monitoring process.

COMPONENT: “105SV” Solenoid Autofill Tank #1
Response is like “103SV”

COMPONENT: #2 Circuit Board, Line #1 Controller Panel, Tank #1.
(Controls Liquid-Level & High-Level Delay Timer/Alarm/Horn)
Condition: *Input:* Shortest probe, *Output:* Initiate high-level alarm sequence.
Failure: Fails to initiate high level alarm.
Effect: Tank continues to fill.
RAC: Uncontrolled: III / C / 4 Controlled: III / C / 4
Remarks & controls: Procedural control by visually monitoring process.

COMPONENT: “105BLT” Light, Red, High-Level Alarm Light Tank #1
Condition: Indicates power is selected to for high level alarm.
Failure: Light fails to illuminate. Bulb failure.
Effect: Light is indication only, it is parallel with **105TR** and **1AH**
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Bulb replacement required.

COMPONENT: “105TR” Relay, Delayed Timer, High-Level Alarm Tank #1
Condition: Delay timer to turn on **105BLT** and **1AH**.
Failure: Fails to operate light or alarm.
Effect: Tank continues to fill.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Procedural control by visually monitoring process.

COMPONENT: “1AH” Alarm Horn, High-Level Tank #1 and/or #4 of Line #1
Condition: Alarm sounds when **106TR** or **105TR** supplies alarm signal.
Failure: Fails to sound alarm.
Effect: Tank continues to fill.
RAC: Uncontrolled: IV / C / 4 Controlled: IV / C / 4
Remarks & controls: Procedural control by visually monitoring process.

Appendix F Fault Tree Analysis

9 What is a Fault Tree Analysis (FTA)?

A fault tree analysis is a method to look at specific undesired events and then use a logic tree approach to determine what causes the undesired events to occur.

10 What are the advantages to using a FTA?

You can use FTA before a mishap or after a mishap. It can be tied to numerical solutions to determine the probability of occurrence. This provides a detailed review of a system and can be one of the most thorough analyses performed if the information on the system is well defined.

11 What are the disadvantages of using a FTA?

The major disadvantage of a FTA is that it is very labor intensive and very expensive to do. It also requires good documentation of the system.

12 Steps for doing a FTA

You do an FTA as follows:

- Determine the undesired event (For example: explosion, fire, structural failure, loss of stability, etc.)
- List the event at the top of the tree. It becomes the “top event” or “fault”
- Determine the “input events” or “faults” that can cause the undesired event to occur
- Determine the “type of event” for each event listed (see Paragraph 5)
- Connect these events to the “top event(s)” using logic gates (see Paragraph 6) Do this by determining whether the events can occur independently (“And” or “Or” gates) or conditionally (“Exclusive Or,” “Priority Or,” or “Inhibit”). Also determine the type of input event. (“Basic,” “Conditioning,” “Undeveloped,” “External,” or “Intermediate)
- Work downward to the next level of “input events and connect them to the preceding input events using logic gates
- Continue this process until you reach the “Basic Event,” “Conditional Event,” “Undeveloped Event,” or “External Event” (see Paragraph 5)

13 Types of events for a Fault Tree

An event is the reason that the fault occurs. It can take on the forms as shown below:

- The “Basic Event” - A basic initiating fault requiring no further development
- The “Conditional Event” - Specific conditions or restrictions that apply to any logic gate. Use this event with the “Priority And” and the “Exclusive Or” gates listed in Paragraph 6.
- The “Undeveloped Event” - An event which you don’t develop further , either because it’s consequence is negligible or because information is unavailable
- The “External Event” - An event which is normally expected to occur
- The “Intermediate Event” - A fault event that occurs because of one or more preceding causal events acting through logic gates

14 Logic gates for a Fault Tree

A logic gate can be one of several types of logic symbols. They include:

- The “And” gate - Output fault occurs if all input conditions are met.
- The “Or” gate - Output fault occurs if any input conditions or combination of input conditions are met.
- The “Exclusive Or” - Output fault occurs if exactly one of the input conditions occurs.
- The “Priority And” - Output fault occurs if all of the input faults occur in a specific sequence.
- The “Inhibit” - Output fault occurs if any single input fault occurs in the presence of an enabling condition.

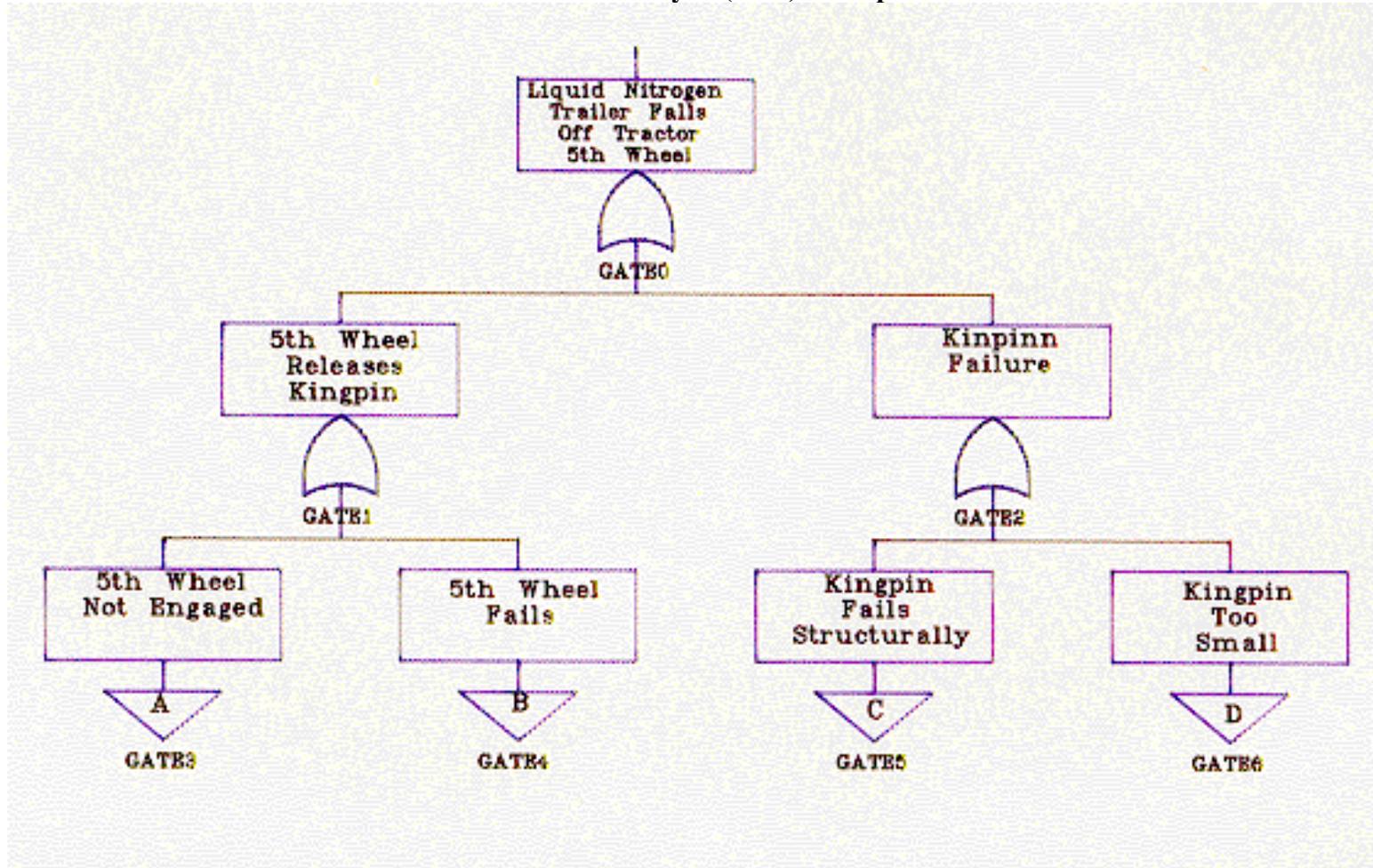
15 Other symbols to use

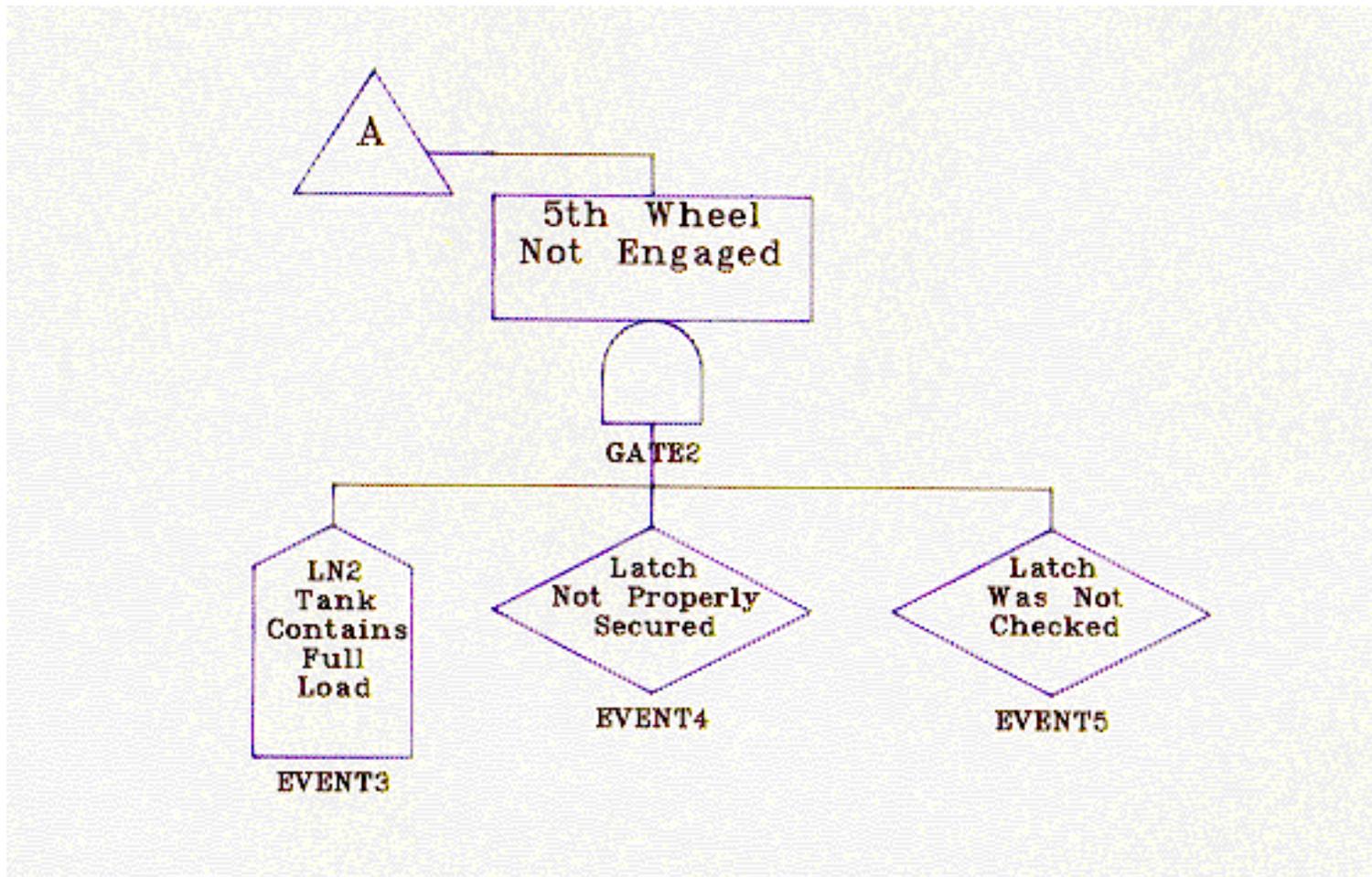
Two other commonly used symbols are:

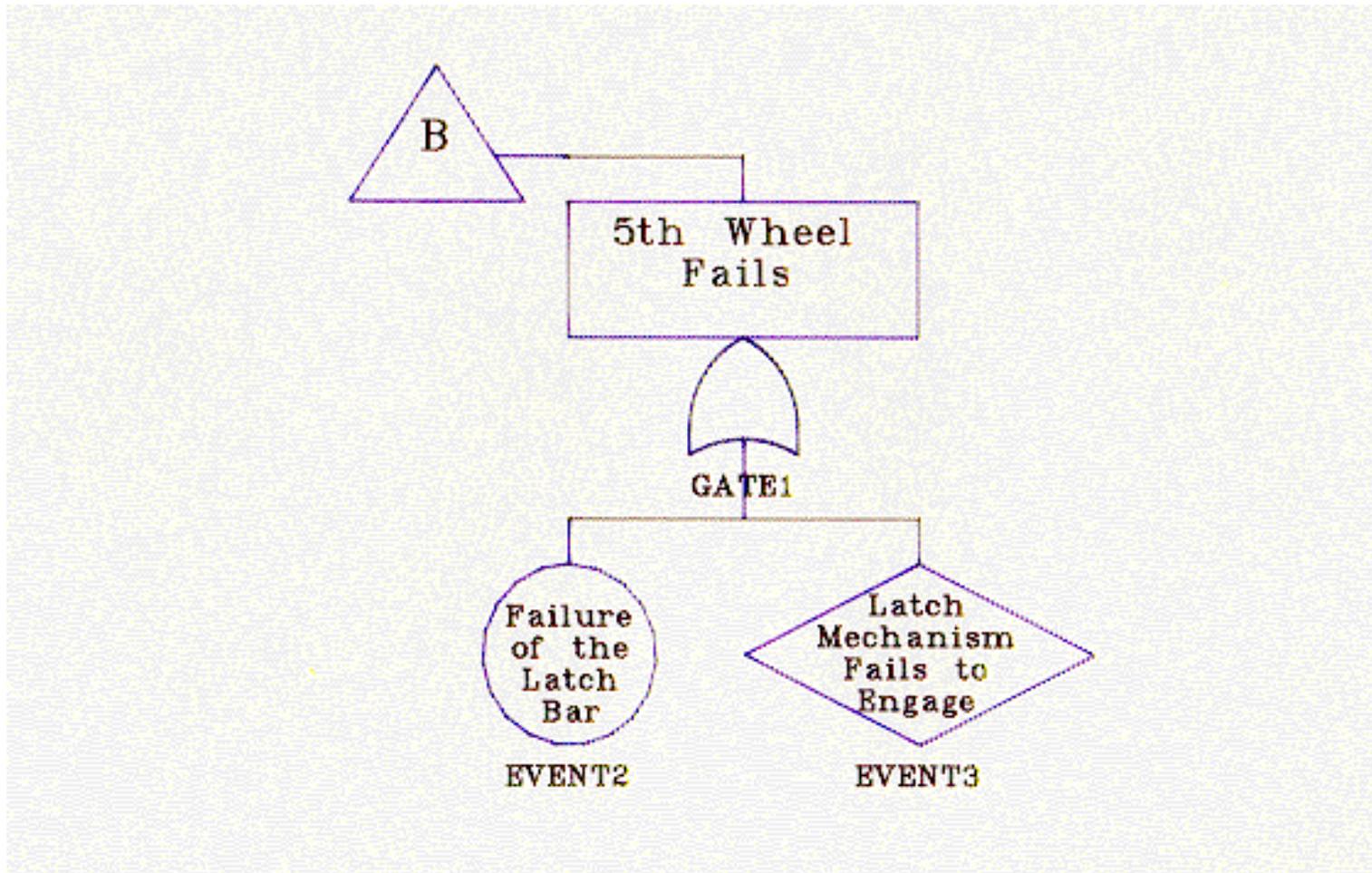
- The “Transfer In” - Indicates that the tree is developed further at the corresponding “Transfer Out” at another location or page
- The “Transfer Out” - Indicates that this portion of the tree must be attached at the corresponding “Transfer In”

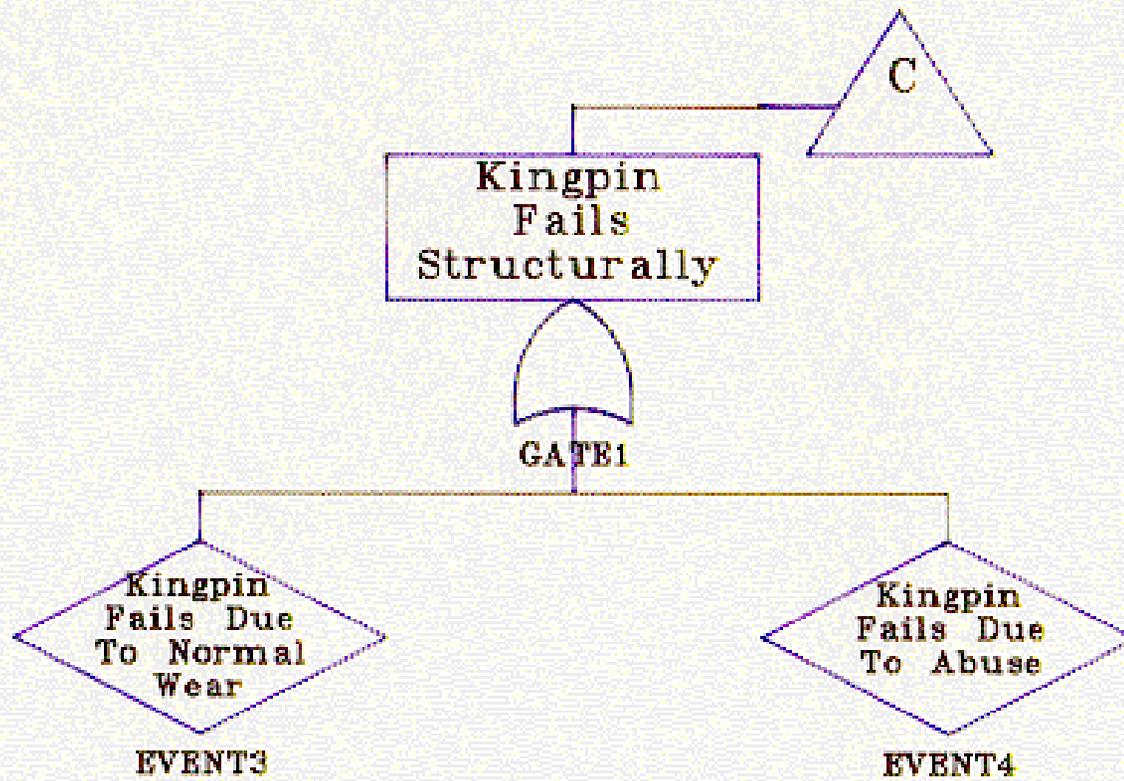
Note: This is a very brief description of how do a Fault Tree Analysis. For a more detailed description, see the Fault Tree Handbook,

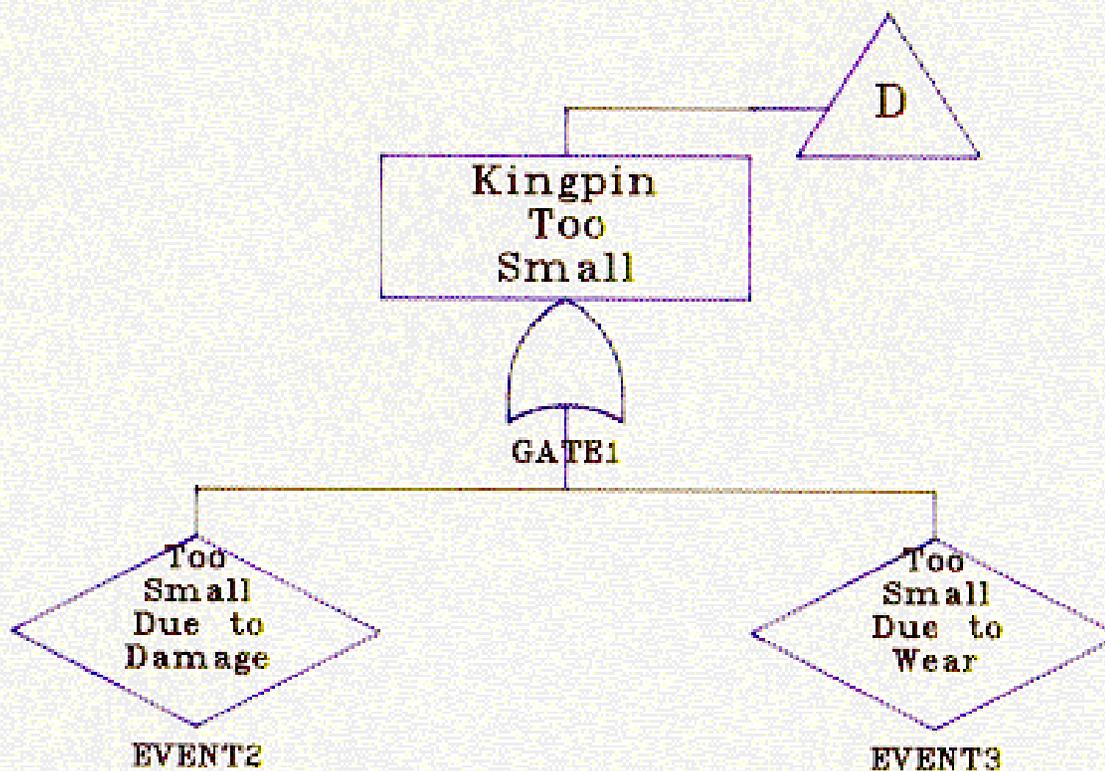
Fault Tree Analysis (FTA) Example

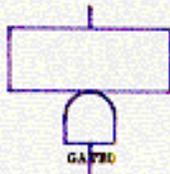








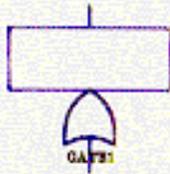




And Gate - All Events Must Occur to Cause Outcome



Right Transfer - A Transfer In From Another Page



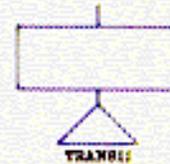
Or Gate - Any Event Can Occur to Cause Outcome



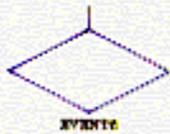
Left Transfer - A Left Transfer in From Another Page



Basic Event - The Lowest Basic Event Which Can Cause the Outcome At the Next Higher Level



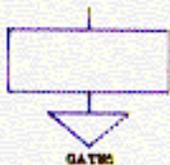
Transfer In - A Transfer From Another Page and Restated



Undeveloped Event - The Lowest Level of Analysis



House - A Normal Event. This Event is Naturally Occuring



Transfer Out - This is a Transfer Off the Page to Another Page

Appendix G Job Hazard Analysis (JHA)

1 What is a JHA?

A job hazard analysis is a method of performing a hazard analysis on each specific task performed in the workplace. This appendix follows the format and methodology of OSHA pamphlet 3071, "Job Hazard Analysis."

2 What are the advantages of a JHA?

The big advantage of a JHA is that the employees are involved from the beginning in reviewing their jobs to see if they can do their jobs more safely. Employees can also work with their supervisors to improve their job safety. JHAs are required for hazardous jobs at JSC.

3 What are the disadvantages of a JHA?

The disadvantage to a JHA is that you must review each task you do in great detail, to adequately do the analysis. Management must be prepared to make changes to job that may affect the cost of the operations. Although this technique is one way of doing a hazard analysis, it is very expensive if used on large-scale operations or facilities.

4 Get employees involved in doing JHAs

Employees must be involved in the JHA. Not only does this show that the supervisor is interested in the employee's safety, the employee has the most intimate knowledge of the job being analyzed.

5 Where should I start?

You start a JHA by asking the following questions:

- What job has the highest injury or illness rates?
- What job has the highest close call rates?
- Is the job a new job that has never been done before?
- Has the job changed?
- Have I looked at the job and the general conditions that might affect how the job is being done?
- Have I developed a checklist for the job?

After you have answered these questions, follow the steps in paragraphs 6 – 10.

6 Begin by asking questions

Ask questions such as:

- Are there materials on the floor that could trip a worker?
- Is lighting adequate?
- Are there any live electrical hazards at the job site?
- Are there any explosive hazards associated with the job or are they likely to develop?
- Do tools, including hand tools, machines, and equipment, need repair?
- Does excessive noise in the work area hinder worker communication and increase the risk of hearing loss?
- Is fire protection equipment readily accessible and have employees been trained to use it?
- Are emergency exits clearly marked?
- Are trucks or motorized vehicles properly equipped with brakes, overhead guards, backup signals, horns, steering gear and identification, as necessary?
- Are all employees operating vehicles and equipment properly trained and authorized?
- Are employees wearing proper personal protective equipment (PPE) for the jobs they are doing?
- Have any employees complained of headaches, breathing problems, dizziness, or strong odors?
- Is ventilation adequate?
- Does the job involve entry into a confined space?
- Have there been any tests for oxygen deficiency and toxic fumes?
- Are there systems that require lockout/tagout procedures?
- Does this job require special handling procedures for chemicals or pyrotechnics?
- Are there any other questions that might be appropriate?

7 Break down the job into specific steps that are required to do the job.

List each step of the job in order of occurrence as you watch the employee doing the job. Make sure that you record enough information about the task to be able to analyze the task properly, but not in too much detail.

Identify hazards associated with each job task

Ask questions such as:

- Is the worker wearing clothing or jewelry that could get caught in the machinery?
- Are there fixed objects that may cause injury, such as sharp machine edges?
- Can the worker get caught in or between machine parts?
- Can the worker be injured by reaching over moving machinery parts or materials?
- Is the worker off-balance at any time?
- Is the worker positioned at the machine in a way that is potentially dangerous?

- Is the worker required to make movements that could cause hand or foot injuries, repetitive motion injuries, or strain from lifting?
- Can the worker be struck by, lean against, or strike a machine part or object?
- Do suspended loads or potential energy pose a hazard?
- Can the worker fall from one level to another?
- Can the worker be injured from lifting objects, or from carrying heavy objects?
- Do environmental hazards, such as, dust, chemicals, radiation, welding rays, heat or excess noise, result from the performance of the job?

Repeat the job observations as often as necessary until you have identified all hazards.

8 Evaluate the hazard that you have identified.

Remember to look at possible events that could cause an injury or illness from each of the hazards identified. Some typical questions you might use to evaluate the hazards are:

- Is the worker wearing protective clothing and equipment, including safety belts or harnesses that are appropriate for the job?
- Does it fit properly?
- Has the worker been trained to use appropriate PPE?
- Are work positions, machinery, pits or holes, and hazardous operations adequately guarded?
- Are lockout procedures used to deactivate machinery during maintenance procedures?
- Is the flow of work improperly organized?
- How are dusts and chemicals dispersed in the air?
- What are the sources of noise, radiation and heat?
- What causes a worker to contact sharp surfaces?
- Why would a worker be tempted to reach into moving machine parts?

9 Recommend controls for each hazard

Use the most reliable controls possible.

Review the controls with the employee doing the job to determine whether the job could be done differently to eliminate the hazards, or whether training is needed to recognize hazards.

If safer and better job steps can be used, list each new step.

List exactly what the worker needs to know to do the job using the new methods.

If hazards are still present, try to reduce the necessity for doing the job or the frequency of doing the job.

10 What do I do after I complete a Job Hazard Analysis?

Review the JHA each year or when any conditions or operations change.

Job Hazard Analysis Worksheet

Job: Plasma Etching with Technics RIE -85 Plasma Etcher	Facility: RITF	Date 10/22/97
PPE: None required, ventilation of pump exhaust recommended	Analysis by: Nicole K. Dailey	Reviewed by:

Sequence of Basic Job Steps	Potential Hazards	Recommended Safe Job Procedure
<u>Installation</u>	<ul style="list-style-type: none"> • Electrical hazards, missing guards, chemical hazards, unstable mounting 	<ul style="list-style-type: none"> • Proper warning signs in place • Etcher placed securely on cart sufficiently large to hold all equipment • Toxic gases are not to be used for etching
<u>Normal Operation</u> 1. Checkout <ul style="list-style-type: none"> • Check system for proper connections (power, vacuum pump, compressed gases) • Check O-ring for damage and wear 	<ul style="list-style-type: none"> • Inadequate training and instruction • Lack of operating procedure addressing hazards, warnings • Exposure to vacuum pump exhaust 	<ul style="list-style-type: none"> • Only trained operators will operate plasma etcher • Procedure for plasma etcher (EL-011a) notes hazard warnings, cautions, emergency procedures • Pre-operation inspection addresses ensuring vacuum pump properly set-up and vented to lab hood. • Pre-operation inspection addresses ensuring that the system is properly grounded prior to use

Sequence of Basic Job Steps	Potential Hazards	Recommended Safe Job Procedure
<p>2. Activation and use</p> <ul style="list-style-type: none"> • Activate power for unit and cooling system • Select LEVEL adjustments for RF and gasses • Select OPEN for vacuum switch, pump down system • Select settings for each gas channel • Switch ON RF power and set desired power level • Switch OFF gases and RF power, system pumps down 	<ul style="list-style-type: none"> • Electrical hazards • Exposure to toxic gases • Unintentional release of stored energy in compressed gas cylinders or release of compressed gas causing asphyxiation • Improper operation of plasma etcher • Explosion • Inadvertent exposure to RF energy 	<ul style="list-style-type: none"> • Use of toxic materials prohibited • Bottles must be secured, regulators set, hoses connected, and valves closed on unused cylinders. Cylinders used in well-ventilated areas. • Only trained operator allowed to use plasma etcher • Use of non-reactive oil in vacuum • Procedural warnings against defeating interlocks; pre-inspection of cables; deactivation of RF generator when equipment is not in use
<p>3. Sample Introduction, removal</p> <ul style="list-style-type: none"> • Load parts in chamber on driven electrode • Close chamber cover, open vacuum valve, allow system to pump down • Switch on gases, all chamber to stabilize, switch ON RF power • Switch OFF RF power and gases, allow system to pump down • Close vacuum valve and open VENT valve • Wait 5 seconds, open chamber, remove sample, close vent valve 	<ul style="list-style-type: none"> • Inadvertent exposure to hazardous materials/use of incompatible sample material • Inadvertent exposure to RF energy 	<ul style="list-style-type: none"> • Procedural warnings against using toxic gases for etching • Procedural warning against using materials which could decompose into hazardous materials • MSDS sheets available in lab • Personal protective equipment used as required • Vacuum pump exhausted into fume hood • Procedural warnings against defeating interlocks; pre-inspection of cables; deactivation of RF generator when equipment is not in use
<p><u>Shutdown</u></p>	<ul style="list-style-type: none"> • Plasma etcher left activated, unauthorized use 	<ul style="list-style-type: none"> • Procedure EL-011a address shutdown procedures

Sequence of Basic Job Steps	Potential Hazards	Recommended Safe Job Procedure
<p><u>Maintenance, changes or repair</u></p>	<ul style="list-style-type: none"> • Shock, safety features defeated and not returned to normal • Exposure to hazardous chemicals • Explosion caused by using improper pump oil 	<ul style="list-style-type: none"> • Only authorized service personnel will perform repairs • Procedure to address daily maintenance limited to replacing vacuum pump oil, flushing lines with hydrogen peroxide, and minor adjustments. • Procedure addresses disconnecting power cord before performing adjustments • MSDS available for hydrogen peroxide and fomblin oil, use of PPE • Procedure addresses using only FOMBLIN (non-reactive) oil in vacuum pump

Appendix H

Some Other Analysis Techniques

1 What are some of the other types of hazard analysis?

Some of the other types of hazard analyses, include, but are not limited to:

- Common Cause Analysis
- Sneak Circuit Analysis
- Failure Mode and Criticality Effects Analysis (FMCEA)
- Event Tree Analysis
- Software Safety Analysis
- Preliminary Hazard Analysis (PHA)
- Subsystem Hazard Analysis (SSHA)
- System Hazard Analysis (SHA)
- Operating and Support Hazard Analysis (O&SHA)
- Energy Trace Barrier Analysis

2 When would I use one of the other hazard analysis techniques?

You would use one of the other hazard analysis techniques, if the normal hazard analyses techniques, as shown in the other appendices, indicate that the specific area needs further investigation or if you need special emphasis in a specific area. In some cases the techniques shown in paragraph 1 of this appendix are subsets of the other hazard analyses techniques and may or may not give more information.

3 Where can I go to get information about these other techniques?

Many of the other techniques are in:

- MIL-STD 882, Systems Safety.
- Any good systems safety textbook.
- The class notes for the NASA Safety Training Center documentation.

Space Administration
Lyndon B. Johnson Space Center
Houston, Texas

(Preliminary) Hazard Analysis Report

Date:3/18/98
Revision:0
Hazard Analysis of: **METAL FINISHING AREA,**
(PLASFAB).

Approved By: *Signature = **Herbert K. Mitchell***
Branch Chief

Building/Room: 9S / 1020, A, B, & C.

Approved By: *Signature = **John W. Murray***
Division Safety Officer

Approved By: *Signature = **Robert S. Seiwel***
NASA JSC Safety Officer

Prepared By: John Murray

Concurrence: *Signature = **Thomas A. Hall***
Facility Manager

Organization: EM, Manufacturing, Materials, and Process Technology Division
Telephone: 281-483-1302

Severity Classes:

- I Catastrophic - May cause death or major system damage.
- II Critical - May cause sever injury, sever occupational illness, or major property damage.
- III Marginal - May cause minor occupational illness or property damage.
- IV Negligible - Probably would not affect personnel safety or health, but is a violation of specific criteria.

Probability Codes:

- A Likely to occur immediately.
- B Probably will occur in time.
- C May occur in time.
- D Unlikely to occur.

RAC code:

Severity Class	Probability Estimate			
	A	B	C	D
I	1	1	2	3
II	1	2	3	3
III	2	3	4	4
IV	3	3	4	4

RAC 1's will be considered imminent danger and require immediate attention.

RAC 2's are serious and will require priority attention.

RAC 3 & 4's are non-serious but will be corrected in RAC order.

Note:

FUNCTION STATEMENT

1.0 Introduction

Construction and startup of Metal Finishing Area (Building 9S, Room 1020, A, B, & C) with dye, alodyne, anodize, etch, dye and electro-polish capabilities.

2.0 Purpose

This analysis was performed to describe hazards, their cause and effect, the controls for these hazards, how the controls are verified, and the RAC code of each hazard intrinsically and with controls affected for the Metal Finishing Area.

3.0 Scope

The hazard analysis covers the Metal Finishing Area and the facility interfaces.

4.0 Applicable Documents⁶

JPG 1700.1 G ; JSC Requirements Handbook for Safety, Health and Environmental Protection

EA-557; Major Facility and Test Buildup Project Management Process

EA-574; Facility Maintenance Procedure

5.0 Summary

The Hazard Analysis performed for normal and emergency operation of the Metal Finish Area and shows that there no open category I or II RACs for the area analyzed.

Each process should have a hazard analysis performed before documentation of the procedure.

All PPE shall be designated and referenced to MSDS data or the ANSI standard where applicable in procedural hazard analysis performed for each procedure utilized.

(An explicit call out for PPE referencing minimum requirements is met by vender/manufacturer item)

Hazard Analysis - Metal Finishing Area (PLASFAB)

Nr.	Hazard	Cause	Effect	Un-controlled RAC C/F/R	Controls	Verification	Disposition Controlled or eliminated RAC C/F/R
1.	Chemical NOTE: MSDS and tank chemical solution identified with attachment. Vapor	- Diluted Exposure to or contact with chemical agents: - Concentrate Splashback -Tank chemical emissions - Scrubber failure	-Skin irritation or rash. (Limited direct contact mild effect) -Skin burns, or irritation -Irritated eyes/ respiratory (Smell will be obvious)	III/C/4 II/C/3 III/B/2	-Procedures for normal and emergency operation. -Proper PPE-Goggles, apron, long gloves, shoes. -Eyewash & shower available. -Training -Scrubber -Shutdown for equipment repair	-Continuous inspection by supervisor and coworkers -Safety inspections and walkdowns -Recertification Training -Negative air flow. -Smell	CONTROLLED III/D/4 CONTROLLED III/C/4 CONTROLLED III/C/4
2	Hazardous Chemical Tank # 1 Oakite Cleaner 3000 Non-Haz. Ingr.>80%, Amine Ethoxylate <5%, Nonionic Surfactant <5%, Sodium Silicate < 5% TSR <5%.	- Diluted Exposure to or contact with chemical agents: - Concentrate Splashback	-Skin irritation or rash. (Limited direct contact mild effect) -Skin burns, or irritation	III/C/4 II/C/3	-Procedures for normal and emergency operation. -Proper PPE-Goggles, apron, long gloves, shoes. -Eyewash & shower available. -Training	-Continuous inspection by supervisor and coworkers -Safety inspections and walkdowns -Rectification Training	CONTROLLED III/D/4 CONTROLLED III/C/4
3	Hazardous Chemical Tank # 4 Oakite Etch 360L Sodium hydroxide40-50% NHI_bal.	- Diluted Exposure to or contact with chemical agents: - Concentrate Splashback	-Skin irritation or rash. (Limited direct contact mild effect) -Skin burns, or irritation	III/C/4 II/C/3	-Procedures for normal and emergency operation. -Proper PPE-Goggles, apron, long gloves, shoes. -Eyewash & shower available. -Training	-Continuous inspection by supervisor and coworkers -Safety inspections and walkdowns -Recertification Training	CONTROLLED III/D/4 CONTROLLED III/C/4

Nr.	Hazard	Cause	Effect	Un-controlled RAC C/F/R	Controls	Verification	Disposition Controlled or eliminated RAC C/F/R
4	Hazardous Chemical Tank # 10 Sulfuric Acid = 10%	- Diluted Exposure to or contact with chemical agents: - Concentrate Splashback	-Skin irritation or rash. (Limited direct contact mild effect) -Skin burns, or irritation	III/C/4 II/C/3	-Procedures for normal and emergency operation. -Proper PPE-Goggles, apron, long gloves, shoes. -Eyewash & shower available. -Training	-Continuous inspection by supervisor and coworkers -Safety inspections and walkdowns -Recertification Training	CONTROLLED III/D/4 CONTROLLED III/C/4
5	Hazardous Chemical Tank # 14, Alodine 12003 Chromic Acid 50-60% Sodium Fluoride 1-10%, Potassium Ferricyanide 10-30%, Potassium Fluoborate 10-30%, Potassium Fluozirconate 1-10%	- Diluted Exposure to or contact with chemical agents: - Concentrate Splashback	-Skin irritation or rash. (Limited direct contact mild effect) -Skin burns, or irritation	III/C/4 II/C/3	-Procedures for normal and emergency operation. -Proper PPE-Goggles, apron, long gloves, shoes. -Eyewash & shower available. -Training	-Continuous inspection by supervisor and coworkers -Safety inspections and walkdowns -Recertification Training	CONTROLLED III/D/4 CONTROLLED III/C/4
6	Dye chemicals Tanks # 18 & 20 Chromium (combined) < 3% Chromium III < 3%	- Diluted Exposure to or contact with chemical agents: - Concentrate Splashback	-Skin irritation or rash. (Limited direct contact mild effect) -Skin burns, or irritation	III/C/4 II/C/3	-Procedures for normal and emergency operation. -Proper PPE-Goggles, apron, long gloves, shoes. -Eyewash & shower available. -Training	-Continuous inspection by supervisor and coworkers -Safety inspections and walkdowns -Recertification Training	CONTROLLED III/D/4 CONTROLLED III/C/4
7	Hazardous Chemical Tank # 22Anodal liquid seal: Nickel acetate 10-15% Nickel(combined) 4.5-5.5% Nickel compound 10-15%	- Diluted Exposure to or contact with chemical agents: - Concentrate Splashback	-Skin irritation or rash. (Limited direct contact mild effect) -Skin burns, or irritation	III/C/4 II/C/3	-Procedures for normal and emergency operation. -Proper PPE-Goggles, apron, long gloves, shoes. -Eyewash & shower available.	-Continuous inspection by supervisor and coworkers -Safety inspections and walkdowns -Recertification Training	CONTROLLED III/D/4 CONTROLLED III/C/4

Nr.	Hazard	Cause	Effect	Un-controlled RAC C/F/R	Controls	Verification	Disposition Controlled or eliminated RAC C/F/R
					-Training		
8	Hazardous Chemical Tank # 27 Phosphoric Acid 40-50% Sulfuric acid 30-50%	NOT USED					
9	Hazardous Chemical Tank # 29 Metalphoto liquid seal. Nickel acetate Tetrahydrate <10% NHI -bal	- Diluted Exposure to or contact with chemical agents: - Concentrate Splashback	-Skin irritation or rash. (Limited direct contact mild effect) -Skin Burns, or irritation	III/C/4 II/C/3	-Procedures for normal and emergency operation. -Proper PPE-Goggles, apron, long gloves, shoes. -Eyewash & shower available. -Training	-Continuous inspection by supervisor and coworkers -Safety inspections and walkdowns -Recertification Training	CONTROLLED III/D/4 CONTROLLED III/C/4
10	Chemical potential	-Tank (multiple tank) leak/rupture, overflow. -Quantity disposal. - Spills	Personnel & equipment contact, irritation / corrosive	II/C/3	-Design configured with multiple containment (Tank, containment shell for tanks, grate level pan, and Treated acid resistance brick floor.) -PPE -HazMat Training. -Disposal procedure.	-Procedural checklist -Equipment and safety inspection. -Disposal agents surveillance.	CONTROLLED III/C/4
11	Tank overflow	-Control system failed to stop filling tank(s). -Procedural identification or manual shutoff failure.	-Skin contact could cause burns or rash -Secondary containment utilized.	III/C/4	-Procedural training. -Operational awareness. -Design for multiple control and manual safeguards	-Rectification -Continuous inspection of work area by supervisor and workers.	CONTROLLED IV/C/4

Nr.	Hazard	Cause	Effect	Un-controlled RAC C/F/R	Controls	Verification	Disposition Controlled or eliminated RAC C/F/R
12	Thermal (Heat)	-Steam heat line (or integrity loss of closed system steam) -Conducted heat of tank or liquid. -Tank #13,22, & 27 fluid contents (160-210)	-Personnel injury by contact with heated item, gas. -Skin burns from contact with liquid or uninsulated glove	III/B/3	-ASME Design of piping and tanks -PPE -Procedure -Training	-Coworker and supervisor observation	CONTROLLED II/C/3
13	Thermal Evaporation	-Boil off of liquid and no replenish liquid	Exposed steam heater coils	III/C/4	-Procedural training. -Operational awareness. -Design for multiple control and manual safeguards	-Rectification -Continuous inspection of work area by supervisor and workers.	CONTROLLED III/D/4
14	Pressure	-Steam pressure line release. - Regulator Valve (15#) operated by site facility prior to interface point.	Personnel injury from projectile.	II/C3	-Main steam manifold has an relief valve above operating pressure and below upper limit of the system (18#)	-Relief valve has a Recertification req. -Regulator valve monitored constantly.	CONTROLLED III/C/4
15	Electrical Rectifier	-Contact with exposed wiring or shorted equipment Low voltage contact from bus bar.	Personnel injury or death.	I/C/2 II/C/3	-Electrical design and component enclosure. All 110V lines e enclosed in conduit and J-boxes have gasket seals and GFI breakers. -Single point emergency electrical shutoff control system. -Operational procedures. -Proper PPE	-Equipment/Safety Inspections -Configuration control. -Periodic procedural review. -Physical barrier.	CONTROLLED III/D/4 CONTROLLED III/C/4