Facility Hazard Analysis and Risk Assessment Subject Area

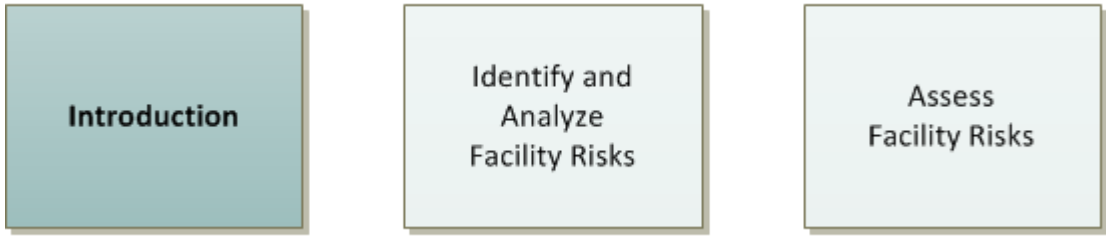
Effective Date: **May 13, 2016** (Rev 4.0)
Periodic Review Due: **May 13, 2019**

What you may need

Where to next

Contacts
SME: Wai Lin Ng, x7153

SBMS: x7267



Introduction

This subject area describes one of the processes used to identify and analyze hazards and risks for industrial, operational and experimental areas.

A hazard is defined as a condition or activity that, if left uncontrolled, can result in an injury or illness. A job hazard analysis is used to identify and control hazards while performing work, both scientific and operations. A facility hazard analysis evaluates hazards in the workplace and contains descriptions of the location, task, hazard, and controls. This subject area covers facility hazard analysis; job hazard analysis is covered in the Work Planning and Control for Experiments and Operations Subject Area.

A risk assessment evaluates the potential consequence of exposure to a hazard. The risk assessment process builds on the hazard analysis and determines risk based on severity of

the undesired consequence, likelihood of the consequence occurring, and the frequency of exposure.

This subject area meets the hazard analysis and risk assessment requirements for facilities in OHSAS 18001 Clause 4.3.1 Hazard Identification, Hazard Analysis and Risk Assessment and 10 CFR 851.21.

A facility risk assessment (FRA) is used in conjunction with a job risk assessment (JRA) (see the OHSAS 18001 Program Subject Area) to identify the hazards to be considered during work planning, following the Work Planning and Control for Experiments and Operations Subject Area. FRA addresses hazards that originate from conditions within a facility or operation; the JRA addresses hazards with respect to the work being performed.

This subject area does not apply to accelerator and nuclear facilities. Workplace hazards and risks associated with accelerators and nuclear facilities are described in the Safety Analysis Documents, and covered in the Accelerator Safety Subject Area. Radiological and nuclear materials are covered in the Facility Hazard Categorization and Nuclear/Criticality Safety Subject Areas.

This subject area does not cover hazards occurring during temporary operations, construction operations, or outdoor work.

Standards of Performance

Managers shall analyze work for hazards, authorize work to proceed, and ensure that work is performed within established controls.

All staff and users shall identify, evaluate, and control hazards in order to ensure that work is conducted safely and in a manner that protects the environment and the public.

All staff and users shall conduct work within the facility-specific operational boundaries specified in Facility Use Agreements.

All staff and guests shall promptly report accidents, incidents, injuries, ESS&H deficiencies, emergencies, and off-normal events in accordance with procedures.

Facility Hazard Analysis and Risk Assessment Subject Area

Effective Date: **May 13, 2016** (Rev 4.0)
Periodic Review Due: **May 13, 2019**

What you may need

Where to next

Contacts
SME: Wai Lin Ng, x7153

SBMS: x7267

Introduction | **Identify and Analyze Facility Risks** | Assess Facility Risks

Each organization is to conduct hazard analysis and risk assessment to identify the hazards and appropriate controls in their areas such as: experimental halls, accelerators, laboratories, shops, mechanical equipment rooms, sewage & water treatment plant, well houses, and warehouses.

Identify and Analyze Facility Risks

1. The line organization designates trained staff to use the Hazard Validation Tool (HVT) to identify the hazards in their facilities for HVT risk levels 2, 3, and 4.
   Note: For new facilities, obtain initial baseline information from the engineering designs (*see* the Engineering Design Subject Area) and facility readiness evaluations (*see* the Readiness Evaluations Subject Area) on operational safety limits and controls. Record the information in the work planning documents and the HVT.
2. Line organizations analyze identified hazards and ensure that hazard controls resulting from the analyses are applied using a graded approach in work planning documents as described in the Work Planning and Control for Experiments and Operations Subject Area.

Note: Links to the appropriate documentation may be found in the Facility Use Agreement (see the Facility Use Agreements home page [*Limited Access]).

3. When facility hazards are not adequately covered by basic hazard controls, line organizations apply supplemental technical hazard analyses (e.g., pressure safety analysis, cryogen safety analysis, fire hazard analysis, explosives, or energetic materials). Refer to the exhibit Facility Hazard Analysis and Review Matrix (HARM).

   Line organizations ensure that controls and boundary limits are documented, reviewed, and approved in work planning documents, Safety Analysis Reports/Documents, permits, and/or licenses for identified hazards.

4. Ensure that area-specific information is identified in the HVT for use on hazard information placards by workers and work planners.

Facility Hazard Analysis and Risk Assessment

Subject Area
Effective Date: **May 13, 2016** (Rev 4.0)
Periodic Review Due: **May 13, 2019**

What you may need

Where to next

Contacts
SME: Wai Lin Ng, x7153

SBMS: x7267

Introduction | Identify and Analyze Facility Risks | **Assess Facility Risks**

Assess Facility Risks

The Facility Risk Assessment (FRA) process identifies the hazards in an area, analyzes those hazards against risk, and assigns a risk level. Using the risk level, controls are established to reduce the risk to an acceptable level.

BNL site-level facility risk assessments (FRAs) are maintained in the Hazard Validation Tool (HVT). Line organizations may maintain more detailed FRAs as appropriate to the scope of their operations.

1. Line organization designees ensure that their areas are appropriately characterized by the predetermined risk assessments in the HVT or by their own line organization's FRAs.
2. If an area type is not assigned in the HVT, line organizations can

- Create a new risk assessment with input from the cognizant person for that space
  Or
- Add it to the HVT by contacting the Facility Hazard Analysis and Risk Assessment SME.

3. Line organization designee(s) update the hazard information for their areas in the HVT when operational activities are modified or changed:

- As part of the commissioning of new facilities or modifications to existing facilities that have not been previously assessed for risk;
- As requested by an Exit Readiness or Operational Readiness Review Team;
- When a review of an event, injury, illness, critique, or occurrence report determines that a revision to the Facility Risk Assessment (FRA) is needed;
- When previously unreviewed hazards are identified;
- When new controls are required by Federal, State or local laws, or requirements.

Guidance

FRAs can be used by work planners and job supervisors as a reference for hazards and hazard-controls in similar operational areas.

FRAs may assist management in prioritizing resources and funding needs to be directed to reduce the risk of injury in similar operational areas.

Facility Hazard Analysis and Risk Assessment Subject Area

Effective Date: **May 13, 2016** (Rev 4.0)
Periodic Review Due: **May 13, 2019**

What you may need

Where to next

Contacts
SME: Wai Lin Ng, x7153

SBMS: x7267

Reporting Obligations

None

External/Internal Requirements

BNL has to abide by all applicable Prime Contract clauses, DOE directives, industry standards, as well as Federal, state, and local laws. BNL develops its policies and procedures based on an evaluation of these external requirements. This Subject Area implements the following requirements:

Requirement Number	Requirement Title
10 CFR 830, Subpart A	Energy, Nuclear Safety Management, Quality Assurance Requirements
10 CFR 851	Worker Safety and Health Program
29 CFR 1910	Labor/Occupational Safety and Health Standards
DOE-STD-1066-99	Fire Protection Design Criteria
EO 12941	Seismic Safety of Existing Building
O 414.1D Admin Chg 1 (May 8, 2013)	Quality Assurance
O 420.1C (Dec 12, 2012)	Facility Safety

Facility Hazard Analysis and Risk Assessment Subject Area

Effective Date: **May 13, 2016** (Rev 4.0)
Periodic Review Due: **May 13, 2019**

What you may need

Where to next

Contacts
SME: Wai Lin Ng, x7153

SBMS: x7267

Training

JTA (HVT - Documenting Hazards & Risks Qualified - GE 121) was established for those who are assigned the task of maintaining data for facility hazards and risks in the Hazard Validation Tool (HVT). Responsible staff will be assigned the JTA by their line training coordinator.

The following courses are required training for GE-121:

- HVT - Documenting Hazards & Risks (TQ-HVT_HAZARDS)
- Hazard Validation Tool for Work Planning (TQ-HVT)

Definitions

Term	Definition
Facility Use Agreement (FUA)	A Facility Use Agreement is a contract between the Facilities & Operations Directorate (F&O), as represented by the Facility Complex Manager (FCM)and the facility occupants, which specifies the operational boundaries of the facility.
hazard	A condition or activity that, if left uncontrolled, can result in an injury or illness.
industrial facility	A facility with no radiological inventory exceeding process guidelines and no chemical inventory above Appendix A of 29 CFR 1910.119, *List of Highly Hazardous Chemicals, Toxics and Reactives.* An industrial facility may contain other routine hazards, such as electrical, pressure, and high temperature.
operational area	An area (inside or outside) or room with experimental equipment or support equipment, where there is current operational activity.
operational boundaries or safety limits	The limits and controls placed on personnel activities, processes, materials, and equipment. The limits and controls are typically defined by work planning documents, Standard Operating Procedures, Safety Analysis Reports/Documents, permits and/or licenses, and identified hazards.
radiological facility	A facility containing an area(s) defined as a Radiological Area in the Radiological Control Manual and having an inventory less than the Category 3 thresholds in Table A.1 of DOE-STD-1027-92, Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23 Nuclear Safety Analysis Report.
risk	The product of the occupancy, likelihood of occurrence, and severity of consequence.
risk level	Predetermined numerical value (0, 1, 2, 3, or 4) in the Hazard Validation Tool based on hazards in an area before mitigation is considered.
safety documentation	That body of written and retained material prepared by the user organization (or their agents), which identifies hazards, hazard controls, and operational boundaries commensurate with the overall risk, and required level of review and approval.

Forms/Exhibits

Title	Effective Date
Facility Hazard Analysis and Review Matrix (HARM)	05/13/2016
Guidance on Barrier Analysis	05/13/2016
Guidance on Change Analysis	05/13/2016
Guidance on Energy Trace and Barrier Analysis	05/13/2016
Guidance on Failure Modes and Effects Analysis	05/13/2016
Guidance on Fault Tree Analysis	05/13/2016
Guidance on Fire Hazard Analysis	05/13/2016
Guidance on Preliminary Hazard Analysis	05/13/2016
Guidance on What-If Analysis	05/13/2016
Risk Assessment Calculations for Facility/Area Assessments	05/13/2016

Facility Hazard Analysis and Review Matrix (HARM)

Effective Date: **May 13, 2016**

A preliminary Facility Hazard Analysis is the basic analysis necessary for all hazard types. Supplemental analysis may be necessary based on the following considerations: public perception, program down-time, and potential loss of high-value equipment. The Facility Hazard Analysis Subject Matter Expert should be consulted to make this determination.

See the following exhibits for information on the analyses:

- Guidance on Barrier Analysis,
- Guidance on Change Analysis,
- Guidance on Energy Trace and Barrier Analysis,
- Guidance on Fault Tree Analysis,
- Guidance on Failure Modes and Effects Analysis,
- Guidance on Preliminary Hazard Analysis,
- Guidance on What-If Analysis.

See the exhibit Job Safety Analysis in the Work Planning and Control for Experiments and Operations Subject Area for guidance on Job Safety Analysis. Refer to the ALARA and Radiological Work Subject Area for guidance on an ALARA Analysis.

HAZARD TYPE	RELEVANT SUBJECT AREAS AND LEGACY MANUALS	SUPPLEMENTAL RECOMMENDED ANALYSIS TECHNIQUE	CANDIDATE EXTERNAL REVIEWER(S)
Animal Subjects	Animal Research Subject Area	What-if Analysis	Subject Matter Expert (SME), Institutional Animal Care & Use Committee
Biological	Biosafety in Research Subject Area, Bloodborne Pathogens Subject Area, Emergency	What-if Analysis, Barrier Analysis, Change Analysis	SME, Institutional Biosafety Committee

	Preparedness Subject Area		
Chemical	Chemical Safety Subject Area, Compressed Gas Cylinders and Related Systems Subject Area, Emergency Preparedness Subject Area, Exhaust Ventilation Subject Area, Personal Protective Equipment and Respirators Subject Area	What-if Analysis, HAZOP, Barrier Analysis, Change Analysis	SME
Confined Space/ Oxygen Deficiency Hazard (ODH)	Oxygen Deficiency Hazards (ODH), System Classification and Controls Subject Area, Confined Spaces Subject Area	What-if Analysis, Barrier Analysis, Job Safety Analysis; See the following exhibits in the Oxygen Deficiency Hazards (ODH), System Classification and Controls Subject Area: Calculation of the Fatality Factor; Equipment Failure Rate Estimates; Fatality Rate Determination; and Oxygen Concentration in Ventilated Spaces.	SME, Laboratory Environmental Safety and Health Committee
Cryogenic	Cryogenics Safety Subject Area	Failure Modes and Effects Analysis, Fault Tree Analysis, Energy Trace Barrier Analysis; See the following exhibits in the Oxygen Deficiency Hazard (ODH) Subject Area: Calculation of the Fatality	SME, Laboratory Environmental Safety and Health Committee

		Factor; Equipment Failure Rate Estimates; Fatality Rate Determination; and Oxygen Concentration in Ventilated Spaces.	
Electrical	Electrical Safety Subject Area, Lockout/Tagout (LOTO) Subject Area	Failure Modes and Effect Analysis	SME, Laboratory Electrical Safety Committee
Explosives	Explosives Safety Subject Area	What-if Analysis, Barrier Analysis, Failure Modes and Effects Analysis	SME, Laboratory Environmental Safety and Health Committee
Fire and Life Safety	Fire Safety Subject Area	Fire Hazard Analysis, Life Safety Code, Change Analysis	SME, Laboratory Fire Safety Committee
Human Subjects	Human Subjects Research Subject Area	What-if Analysis	SME, Institutional Review Board, Radioactive Drug Review Board
Laser	Laser Safety Subject Area	Failure Modes and Effects Analysis (interlock)	SME, Laser Safety Committee, Laboratory Environment, Safety & Health Committee
Lead	Lead Subject Area	What-if Analysis, Barrier Analysis	SME
Magnetic Fields/ Microwave	Non-ionizing Radiation Safety Subject Area	What-if, Job Safety Analysis	SME
Radiological	Radiological Control Manual Program Description, ALARA, Dose Limits, and Administrative Controls (ACLs) Subject Area	Shielding Analysis, ALARA Analysis, Failure Modes and Effects Analysis (interlock), Fault Tree Analysis, Criticality Analysis, Change Analysis	SME, Laboratory Environment, Safety & Health Committee

Stored Energy/Lifting Equipment	Lifting Safety Subject Area	What-if Analysis, Barrier Analysis, Change Analysis	SME, Laboratory Environment, Safety & Health Committee
Stored Energy/ Mechanical Equipment/ Pressure/Vacuum	Compressed Gas Cylinders and Related Systems Subject Area, Pressure Safety Subject Area	What-if Analysis, Barrier Analysis Failure Modes and Effects Analysis, Change Analysis, Job Safety Analysis	SME
Thermal	Piping Systems, Identification of Subject Area	What-if Analysis, Barrier Analysis, Job Safety Analysis	SME
Transportation (Radiological or Hazardous Material On-site or Off-site)	Facility Hazard Categorization Subject Area, Sealed Radioactive Source Control Subject Area, Storage and Transfer of Hazardous and Nonhazardous Materials Subject Area, Traffic Safety Subject Area	What-if Analysis, Barrier Analysis	SME, Transportation Safety Officer, Traffic Safety Committee

This guidance is not intended to be all-inclusive. It is intended to give the user some basic information as to the purpose of the analysis, how it is applied, methods for conducting the analysis, necessary resources, and limitations. Where possible, examples pertinent to BNL operations were used to show typical contents and formats.

Barrier Analysis

Purpose:

A Barrier Analysis is a tool for evaluating controls or barriers to prevent the unwanted flow of (hazardous) energy to targets (personnel or equipment) to prevent an accident or incident from occurring.

Application:

Barrier Analysis is an excellent, simple qualitative tool for systems analysis, safety reviews, or after-the-fact accident analysis. The Department of Energy typically uses Barrier Analysis as an accident analysis tool associated with the broader systems safety approach called Management Oversight and Risk Tree (MORT). However, Barrier Analysis is also an excellent choice for identifying and controlling hazards before an accident or incident occurs.

Methodology:

In the Barrier Analysis, an accident is evaluated to determine what barriers failed or were inadequate to prevent the unwanted energy flow (e.g., toxic gas, electrical current, high pressure) to the "target" (e.g., people, equipment, or the environment) causing injury or damage. The barriers may then be modified or new barriers added to prevent recurrence. A review of the need for the particular energy source or the proximity of targets may be similarly reevaluated. Figure 1 shows the concept of Barrier Analysis.

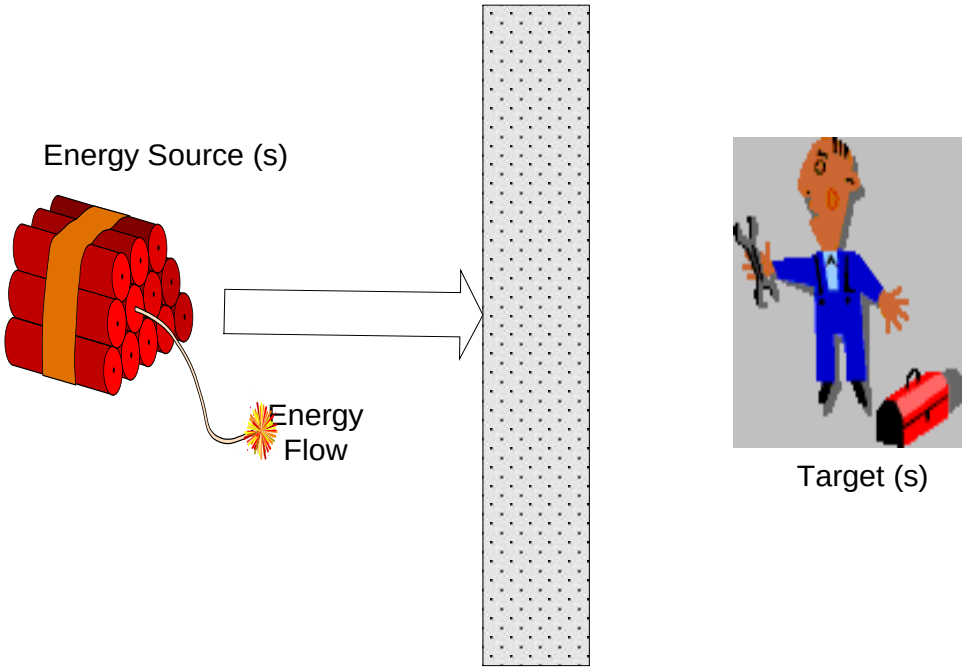


Figure 1.

The Barrier Analysis method is implemented by identifying energy flow(s) that may be hazardous and then identifying or developing the barriers that must be in place to prevent the energy flow from damaging equipment or injuring personnel.

For new operations, changes in existing operations, or periodic review of existing operations, a checklist of energy sources is typically used to identify the need for barriers; see Table 1. The Barrier Analysis method is used to identify needed engineering (design) and or administrative controls as barriers to the energy source in the earliest stages of design, as well as their adequacy, later in design, or as a check before start-up of a hazardous operation. Engineered safety features are considered the preferred type of barriers and should take precedence over the administrative controls, such as procedures, warning signs, and supervisory checks. Engineering barriers are more difficult to bypass than administrative barriers, and should be used first to control the energy sources. However, administrative barriers may be all that can be used in some situations; therefore, a combination of administrative barriers can be used to better ensure energy containment (defense-in-depth).

Table 1. Typical Examples of Energy Sources*

General Category	Energy Source
Acoustical Radiation	Equipment noise Ultrasonic cleaners Alarm devices and signal horns
Corrosive	Chemicals, acids, caustics Decon solutions "natural" chemicals (soil, air, water)
Electrical	Battery banks Diesel generators High lines Transformers Wiring Switchgear Buried wiring Cable runs Service outlets and fittings Pumps, motors, heaters Power tools and small equipment Capacitors
EMR and Particulate Radiation	LASERS, medical X-rays Radiography equipment and sources Welding equipment Electron beam Blacklight (e.g., Magnaflux) Radioactive sources, contamination, waste, and scrap Storage areas, plug storage Skyshine, Bremsstrahlung Activation products, neutrons
Explosive or Pyrophoric	Caps, primer cord, explosives Electrical squibs Powder metallurgy, dusts Hydrogen and other gases Nitrates, peroxides, perchlorates Carbides, superoxides Metal powders, plutonium, uranium Zirconium Enclosed flammable gases Power actuated tools
Flammables	Chemicals, oils, solvents, grease Hydrogen (battery banks), gases Spray paint, solvent vats Coolants, rags, plastics, foam Packing materials
Kinetic-Linear	Cars, trucks, railroad cars Dollies, surfaces, obstructions Crane loads in motion, shears Presses, Pv blowdown Power assisted driving tools
Kinetic-Rotational	Centrifuges, motors, pumps Flywheels, gears, fans Shop equipment (saws, grinders, drills, etc.) Cafeteria and laundry equipment

Mass, Gravity, Height	Human effort Stairs, lifts, cranes Sling, hoists, elevators, jacks Bucket and ladder Lift truck, pits, excavations Vessels, canals, elevator doors Crane cabs, scaffolds, and ladders
Nuclear	Vaults, temporary storage areas Casks, hot cells, reactor areas Criticality potential in process Laboratories, pilot plants Waste tanks and piping, basins, canals Sources and solutions, Skyshine Activation products, Bremsstrahlung
Pressure-volume/K-constant	Boilers, heated surge tanks Autoclaves Test loops and facilities Gas bottles, pressure vessels Coiled springs, stressed members Gas receivers
Thermal (except radiant)	Convection, furnaces Heavy metal weld preheat Gas heaters, lead melting pots Electrical wiring and equipment Exposed steam pipes and valves Steam exhausts
Thermal Radiation	Furnaces, boilers Steam lines Lab and pilot plant equipment Heaters Solar
Toxic Pathogenic	Toxic chemicals, check MSDS Exhaust gases Oxygen deficient atmosphere Sand blasting, metal plating Decon and cleaning solutions Bacteria, molds, fungi, and viruses Pesticides, herbicides, and insecticides Chemical wastes and residues

* The Work Planning and Control for Experiments and Operations Subject Area contains additional energy sources.

In addition to engineering or administrative barriers, barriers can be categorized by their function, their location, and their type, as shown in Table 2.

Table 2.

Barriers		
Functions	**Location**	**Type**
• Prevention • Control • Minimization	• On the energy source • Between the energy source and target • On target • Separation through time and space	• Physical Barriers • Equipment Design • Warning Devices • Procedures/work processes • Knowledge and skill • Supervision

Completeness:

Completeness of the Barrier Analysis is limited by the ability to identify all the energy sources, all the potential targets, and to consider all the available controls or "barriers," both engineering and administrative. This technique lends itself to the use of comprehensive checklists of energy sources to ensure a complete review of an operation or system.

Resources/Skills Required:

A basic understanding of the concept of energy flow in accident causation is essential in the use of this technique. Energy source checklists are very useful for novice and experienced analysts to carefully review a system for all energy sources. The intuitive, qualitative nature of this tool makes it immediately useful and easy to apply, whether doing simple occupational safety/health evaluations of new operations or more detailed evaluations of complex systems.

Limitations:

The method can be used to plan process safety procedures, verify safety configurations, identify a changing energy status, or evaluate a process. This method is simple to apply, use, and document. It is also good for quick, inexpensive reviews and analyses.

The Barrier Analysis Method is not comprehensive for the total analysis of a new design. It may miss critical human errors or hardware failures.

References:

"Barrier Analysis," DOE-76-45/29, SSDC-29, Safety Systems Development Center, EG&G Idaho, Inc., July 1985.

Example/Format:

Example A;

Barrier Analysis

System/Operation:_____
Date:_____ **Revision:** _____

Hazard/Process: <u>Contractor performing a floor cleaning operation using Acetone as the solvent and an electric buffer. Potential Hazards include increasing Acetone Vapor Concentration above the OSHA PEL (1,000 ppm) and possible concentrations that could exceeded the Lower Explosive Limit (25,000 ppm)</u>

Target (s) <u>Contractor Foreman, Painter A and Painter B.</u>

Physical Barriers	Administrative Barriers	Management Barriers
Personal Protective Equipment (PPE) • BNL PPE specifications for chemicals are planned and approved for use. The Industrial Hygiene Group provides guidance on specific gloves, body protection, and respirator and cartridge types. (Note: Respirators are not a barrier above the IDLH level or lower explosive limit for Acetone. • Contractor and BNL (industrial hygiene) will agree on the proper PPE for using Acetone.	**Work Processes** • BNL evaluated the task using procedures for the Work Planning and Control for Experiments and Operations Subject Area, which identified the hazardous nature of the Acetone, hazards and control measures and rated this as a high hazard job. • A job safety analysis has been developed by BNL with input from the Contractor. • The JSA defined the job tasks, known and anticipated hazards, control measures to be used, and required approvals should there be a need to change the work plan, equipment, or chemicals used. • Job requires approximately 1 pint of Acetone per hour of buffing. Only a one-pint container will be allowed in the facility. Additional supply (one day's work) will be kept in the flammable storage cabinet in rm. 102.	**Training/Knowledge/Skills** • Training and experience at the Contractor Foreman and painter level was verified prior to initiating the contract. In addition to verification of experience with this type of application technique, the contractor was required to complete CVO, Hazcom and Basic Electrical Safety Courses at BNL. • The Contractor Foreman and painters were trained on the specific procedure for this job and the associated JSA.

Ventilation • Auxiliary ventilation for the chemicals planned and approved for use will be provided by BNL. • Contractor will be instructed in the proper use of the ventilation equipment. • Ventilation equipment must be class 1, division 1 approved and be running during the entire Acetone cleaning operation.	**Work Procedures** • The Contractor is required to obtain BNL approval prior to starting the job. • The procedure for the job has been approved by BNL. All subsequent changes must be approved by BNL and the procedure must remain at the job site with the JSA attached. • The Contractor Foreman is required to submit the Acetone MSDS to the Contractor's Safety Manager, and BNL, before using Acetone. • The LEL for the acetone will be monitored by Facility Support Personnel during the operation, any excursion >10% of the LEL will shut down the operation	**Line Management Oversight** • BNL will implement an effective contractor work control process to ensure the selection of qualified contractors and adequate job planning and hazard analysis. • BNL Project Manager is responsible for properly implementing the necessary project oversight to ensure the tasks are performed within the established controls.
Buffing Equipment • The floor buffer to be used must be class 1, division 1 approved for use with flammable vapors**.** This must be verified by the Project Manager prior to buffing operations. • The buffer must also be protected by a GFCI		

Example B. (post accident analysis, illustrates how the Barrier Analysis would be used to evaluate an accident where barriers failed and/or were circumvented)

Barrier Analysis
System/Operation:_____
Date:_____ **Revision:** _____

Hazard: <u>Increasing Acetone Vapor Concentration Above the OSHA PEL (1,000 ppm) that eventually exceeded the Lower Explosive Limit (25,000 ppm)</u>

Target (s) <u>Contractor Foreman, Painter A and Painter B.</u>

<table>
<tr><th>Physical Barriers</th><th>Administrative Barriers</th><th>Management Barriers</th></tr>
<tr>
<td>Personal Protective Equipment;
• BNL PPE specifications for chemicals planned and approved for use, was incomplete, i.e., it did not define specific gloves, body protection, and respirator and cartridge types.
• (Note: Respirators are not a barrier above the IDLH level or lower explosive limit for Acetone.
• Contractor did not define proper PPE for using Acetone.</td>
<td>Work Processes
• BNL's work planning was incomplete, which resulted in poor understanding of the tasks, hazards and control measures.
• A job safety analysis could have been developed if BNL and the Contractor had properly conducted work planning and a hazard analysis. The JSA or project hazard analysis would have defined the job tasks, known and anticipated hazards, control measures to be used, and required approvals should there be a need to change the work plan, equipment, or chemicals used.</td>
<td>Training/Knowledge/Skills
• Training and experience at the Contractor Foreman and painter level was not adequate to develop and implement appropriate controls for hazardous chemicals, including flammable liquids, and electrical equipment use.</td>
</tr>
<tr>
<td rowspan="2">Ventilation
• BNL did not specify the need for auxiliary ventilation for the chemicals planned and approved for use.
• Contractor did not provide adequate auxiliary ventilation</td>
<td>Hazard Identification
• OSHA standards require work area assessments to be conducted to identify physical and health hazards of chemicals. The independent BNL and Contractor hazard analyses for the chemicals planned to be used were inadequate, poorly documented, and not sufficiently comprehensive for defining appropriate controls (e.g., substituting a less hazardous material, limiting the quantity of Acetone used, providing adequate ventilation, eliminating ignition sources, providing continuous explosive vapor monitoring, defining spill response procedures) during floor preparation and painting.
• The floor buffer did not have sufficient labeling to warn the painters of the hazard associate with using the buffer in the presence of flammable vapors.</td>
<td rowspan="2">Line Management Oversight
• BNL did not implement an effective contractor work control process to ensure the selection of qualified contractors and adequate job planning and hazard analysis.
• BNL relied solely upon the BNL Project Manager to properly implement the necessary project oversight to ensure the tasks were performed within the established controls.
• The BNL Project Manager and Task Manager failed to identify all chemical hazards and develop specific control measures.</td>
</tr>
<tr>
<td>Work Procedures
• The Contractor did not obtain BNL approval prior to using Acetone, as required by the contract.
• The Contractor Foreman did not submit he Acetone MSDS to the Contractor's Safety Manager, nor discuss the Acetone MSDS with him, before using Acetone.</td>
</tr>
</table>

This guidance is not intended to be all inclusive. It is intended to give the user some basic information as to the purpose of the analysis, how it is applied, methods for conducting the analysis, necessary resources and limitations. Where possible, examples pertinent to BNL operations were used to show typical contents and formats.

Change Analysis

Purpose:

A Change Analysis examines the potential effects of modifications to a system or process from a starting point or baseline (hazards pre-analyzed) configuration. The Change Analysis systematically evaluates undesirable effects from each modification to that baseline.

Application:

Change Analysis can be applied to systems of all kinds ranging from simple to complex. It is well applied as a means of optimizing the selection of a preferred change from among several candidate changes, or in aiding the design of a needed change. The technique can be applied meaningfully only to a system for which baseline risk has been established (e.g., as a result of prior analysis).

Methodology:

Start with the existing, known system as a baseline. Examine the scope of all contemplated or real changes, and analyze the effect of each change (singly) and all changes (collectively) on the system. When evaluating the changes, look at the adverse or unacceptable consequences from that change. This technique often requires the use of a walk-down, to physically examine the system or facility to identify the current configuration.

Alternatively, a Change Analysis could be initiated on an existing facility by comparing "as designed" with the "as built" configurations. In order to accomplish this, there would first be a need to physically identify the differences from the "as designed" configuration.

In either case, a detailed evaluation of the modifications or changes would be made and tabulated. Then the individual likely worst-case effects of each of those changes from the baseline are postulated. Finally, the combined effects are additionally developed, the change in risk developed, and the overall results are reported. The process sequence is

1. Identify the system baseline
2. Identify changes - Walk-down
3. Examine each baseline change by postulating effects
4. Postulate collective/interactive effects
5. Conclude system risk or deviation from baseline risk
6. Report findings

Completeness:

Completeness is limited, by the level of depth/detail in performing the analysis. Completeness required to analyze a given change is governed by the extent of the change itself. Completeness cannot exceed that of prior analyses used in establishing the baseline risk.

Resources/Skills Required:

Understanding all of the physical principles governing the behavior of the system being changed is necessary, in order that the effects of the change can be determined with confidence. Assuming that the complexity of the changes does not appreciably exceed that of the system prior to alteration, mastery of the baseline analytical technique becomes sufficient. A key resource for the Change Analysis is experienced operational personnel who have long-term involvement in an operational process. These personnel can help define the change as it relates to the baseline.

Limitations:

The advantage of the Change Analysis is that it is fast and can be focused: i.e., only the effects of changes need be analyzed, rather than the system as a whole. In this advantage also lies the technique's major shortcoming, i.e., the presumption that the baseline analyses have been carried out adequately. Difficulty of application is determined largely by the extent to which the system has undergone (or will undergo) change, in combination with system baseline complexity.

References:

Bullock, M.G., "Change Control and Analysis," DOE 76-45/21, SSDC-21, Systems Safety Development Center, EG&G Idaho Inc., SSDC-21, March 1981.

Keppner, Charles H., and Tregoe, Benjamin B., "The Rational Manager," McGraw-Hill, 1965.

Secretary of the Air Force, "Air Force Pamphlet 91-215, Operational Risk Management Guidelines and Tools," September 1997.

Example/Format:

System/Process:_____
Date:_____
Revision: _____

Factors	Baseline	Change	Difference	Significance
What				
Objects				
Energy				
Defects				
Protective Devices				
Where				
On the Object				
In the process				
Place				
When				
In time				
In the process				
Who				
Operator				
Co-Worker				
Supervisor				
Others				
Tasks				
Goal				
Procedure				
Quality				
Working Conditions				
Environmental				
Overtime				
Schedule				
Delays				
Trigger Event				
Managerial Controls				
Control Chain				
Hazard Analysis				
Monitoring				
Risk Review				

To use the worksheet: The user starts at the top of the column and considers the current situation compared to a previous situation and identifies any change in any of the factors. The significance of detected changes can be evaluated intuitively or they can be subjected to what-if, logic diagram, or other specialized analyses.

This guidance is not intended to be all-inclusive. It is intended to give the user some basic information as to the purpose of the analysis, how it is applied, and methods for conducting the analysis, necessary resources, and limitations. Where possible, examples pertinent to BNL operations were used to show typical contents and formats.

Energy Trace and Barrier Analysis (ETBA)

Purpose:

The Energy Trace and Barrier Analysis (ETBA) is a system-based analysis process developed to assist in the identifying hazards by focusing in detail on the presence of energy in a system and the barriers for controlling that energy. It can produce a consistent, detailed understanding of the sources and nature of energy flows that can or did produce accidental harm. Results of the analysis support estimation of risk levels, and the identification and assessment of specific options for eliminating or controlling risks.

Application:

The ETBA methodology is applicable for simple or complex systems of all types. It is used to ensure disciplined, consistent, and efficient procedures for the discovery of hazards in a new system. It is also used to examine existing systems that have not been analyzed rigorously in the past. ETBA lends itself to overviews of energies in systems, and disciplines the search for specific hazards or risks that require more detailed analysis. The major strengths of ETBA are its ability to minimize oversights of hazards, its disciplining procedure, its thoroughness, and its compatibility with other system safety analysis methods. It is iterative when used properly, because it identified uncertainties during the energy flow-tracing steps. ETBA is also open-ended, with the theoretical capacity to analyze an unlimited number of energy flows and barrier behaviors to show their influence on process outcomes. The ETBA can be thought of as a more formal and detailed "Barrier Analysis." The ETBA can be used in place of the Barrier Analysis when greater detail is needed or it can be used to examine the impact of hazards developed using the Barrier Analysis in a much greater detail.

Methodology:

ETBA is based on the premise that accidental harm is produced by unwanted energy exchanges associated with energy flows through barriers into exposed "targets." Subsequent refinements have resulted in a simple but comprehensive analysis process using sequential logic that minimizes the chance of overlooking hazards during safety analyses. The ETBA process must begin with the definition of the system being analyzed.

The ETBA involves 5 basic steps as shown below; Step 1 is the identification of the types of energy found in the system. It often requires considerable expertise to detect the presence of the types of energy present. Step 2 is a trace step. Once identified as present, the point of origin of a particular type of energy must be determined and then the flow of that energy through the system must be traced. In Step 3, the barriers to the unwanted release of that energy must be analyzed. For example, electrical energy is usually moved in wires with an insulated covering. In Step 4, the risk of barrier failure and the unwanted release of energy are assessed. Finally, in Step 5, risk control options are considered and selected.

1. Identify the types of energy present in the system.
2. Locate energy origin and trace the flow.
3. Identify and evaluate barriers (mechanisms to confine the energy).
4. Determine the risk (the potential for hazardous energy to escape control and damage something significant).
5. Develop improved controls and implement as appropriate.

The system must be defined in a way that enables the analyst to identify and trace energies from the time they enter the system until they leave the system or are converted into work. An adequate system definition would describe inputs, intended operation, outputs and control flows. The next step is to select a good checklist of energy types that might be in the system, to ensure that all energy sources are identified in the analysis. Figure 1 is an example of a comprehensive Energy Type Checklist. Using the checklist, make a list of all the energies that may require analysis. Then select one energy type at a time to trace through the system.

Figure 1. Energy Checklist (sample)

1. Electrical
AC or DC current flows
Stored electrical energy/discharges
Electromagnetic emissions/RF pulses
Induced voltages/currents
Control voltages/currents

2. Mass/gravity/height (mgh)
Trips and falls
Falling/dropped objects
Suspended objects

3. Rotational kinetic
Rotating machinery/gears/wheels
Moving fan/propeller blades

4. Pressure/volume/kinetic displacement (P/V/KD)
Overpressure ruptures/explosions
Vacuum growth
Liquid spill/blood/buoyancy
Expanding fluids/fluid jets
Uncoiling object
Ventilation air movement
Trenching/digging/earth moving

5. Linear kinetic
Projectiles, missiles/aircraft in flight
Rams, belts, moving parts
Shears, presses
Vehicle/equipment movement
Springs, stressed members

6. Noise/Vibration
Noise
Vibration

7. Moisture/humidity

8. Chemical (acute and chronic sources)
Anesthetic/asphyxiant
Corrosive
Dissolving/solvent/lubricating
Decomposable/degradable
Deposited materials/residues
Detonatable
Oxidizing/combustible/pyrophoric
Polymerizable
Toxic/carcinogenic/teratogenic
Waste/contaminating (air/land/water)

9. Thermal
Radiant/burning/molten
Conductive
Convective/turbulent evaporative/expansive heat/cool
Thermal cycling
Cryogenic

10. Etiologic agents
Viral
Bacterial
Fungal
Parasitic
Biological toxins

11. Radiation
Ionizing
Non-ionizing/lasers

12. Magnetic Fields

13. Living creatures or things
actions/interactions by people
actions by animals, other species
Actions by trees, shrubs etc.

14. **Terrestrial**
Earthquake
Floods/drowning
Landslide/avalanche
Subsidence
Compaction
Cave-ins
Underground water flows
Glacial
Volcanic

15. Atmospheric
Wind velocity, density, direction
Rain (warm/cold/freezing)
Snow/hail/sleet
Lightning/electrostatic
Particulate/dusts/aerosols/powders
Sunshine/solar
Acid rain, vapor/gas clouds
Air (warm/cold/freezing, inversion)

Each energy type present in the system is then analyzed by applying sequential logic to trace its flow, interaction with barriers, interaction between types, and intended work through the system. The energy type is analyzed from the time it first enters or occurs in the system, until it exits the system or is transformed into work, and perhaps another type of energy.

The next step is to identify the barriers controlling the energy flow along its flow path, including physical and procedural barriers of all kinds. At each step of the energy flow, "tests" for hazards are applied to the flow or conversion steps. The "tests" consist of posing a series of "What would happen if….:" shown in the ETBA Hazard Discovery Checklist, Figure 2, along the energy flow path.

Figure 2. ETBA Hazard Discovery Checklist

Energy Flow Changes	**Changes in Barriers**
1. Flow too much/too little/none at all	7. Barrier too strong/too weak
2. Flow too soon/too late/ not at all	8. Barrier designed wrong
3. Flow too fast/too slow	9. Barrier too soon/too late
4. Flow blocked/built up/release	10. Barrier degraded/failed completely
5. Wrong form/wrong type input of flow	11. Barrier impeded flow/enhanced flow
6. Cascading effects of release	12. Wrong barrier type selected

For each energy's flow path, identify the potential effects on each change in energy flows or barriers on the system. Wherever a potential unintended energy release or exchange is discovered, identify the "targets," people or objects, that are likely to be affected by the scenario, and define those effects. If the nature of scope of the effects poses an apparently significant risk of loss, record the scenario and an estimate of the associated risk level, to help set further analysis and control development priorities. The record provides a list of candidate risks for more detailed or alternative analyses. The scenarios pinpoint events that increase the risk. Once the energy or barrier risks are identified, they may be used as a starter list to develop risk control or elimination options, and life cycle monitoring needs. Each unwanted release or exchange is examined, to try to identify at least two changes that might be introduced to achieve desired risk reduction results. The findings are also used to guide the preparation of operating procedures, safety training plans and examples, and ongoing monitoring needs over the system life cycle.

Completeness:

ETBA is capable of producing highly disciplined, thoroughly detailed analyses of hazards in new or existing systems. By meticulously and logically tracking energy flows sequentially, into, within, and out of a system, ETBA compels a thorough analysis for each specific type of energy. Ultimately, the degree of thoroughness depends on the self-discipline and ability of the analyst to track logically the flows and barriers in the system.

Use of energy-related terminology and the logical presentation of the information enables viewers to determine quickly the thoroughness of the analysis, if they have a modest understanding of the intended system operation and the ETBA method.

Resources/Skills Required:

Individuals with engineering or science education can master ETBA most readily, with little additional training. Analysts must understand energy flow and work concepts, for which at least a rudimentary knowledge of the behaviors of each of the energy types in Figure 1 is necessary. Ability to logically identify energy sources and track flows in systems is an essential skill. Ability to visualize energy releases or energy exchange or transformation effects is another helpful skill. Mastery of ETBA can be enhanced by participation in accident investigations, and review of accident reports.

Limitations:

ETBA procedures are very simple. Though simple, the process is perceived as complex, and thus analysts unfamiliar with ETBA are reluctant to use it. Typical difficulties in applying ETBA are

1. The complexity of the system, energies, barriers, or exposures being analyzed.
2. Limits in analysts' knowledge about the behaviors of an energy flow in a given system.

Ill-defined systems introduce another kind of difficulty in that they must first be defined before ETBA, or any other predictive analyses, can be successfully performed. ETBA can aid the system design process by identifying uncertainties. In accidents, ETBA application may be handicapped by the cascading effects of the energy exchanges. Fire, for example, changes the interim states of system elements and energy flows over time so they cannot be identified reliably after the fact.

Users find that ETBA is probably the most powerful, efficient, and comprehensive system safety analysis process for the reliable discovery of new hazards in existing systems, or the discovery and analysis of risks in new systems. ETBA's sequentially structured procedures produce more consistent, logically reasoned, and less subjective judgments about hazards and controls than any other single safety analysis method available. When ETBA is performed after capabilities of other safety analyses methods have been exhausted, it invariably discloses

previously undefined hazards and risks. It also provides superior insights into changes that might be introduced to eliminate or control the hazards discovered.

References:

Bender, L., "Guide 7: A Guide for Using Energy Trace and Barrier Analysis with the STEP Investigation System," Events Analysis, Inc., Oakton, VA, 1985.

Haddon, W., "Energy Damage and the Ten Counter-measure Strategies," Human Factors Journal, August 1973.

Johnson, W., "MORT, The Management Oversight and Risk Tree, " SAN 821-2, U.S. Atomic Energy Commission, February 1973.

"Risk Assessment Techniques Manual," Transportation Safety Institute, U. S. Department of Transportation, Oklahoma City, OK, August 1986.

Secretary of the Air Force, "Air Force Pamphlet 91-215, Operational Risk Management Guidelines and Tools", September 1997.

Examples/Format: To be developed

This guidance is not intended to be all inclusive. It is intended to give the user some basic information as to the purpose of the analysis, how it is applied, and methods for conducting the analysis, necessary resources and limitations. Where possible, examples pertinent to BNL operations were used to show typical contents and formats.

Failure Modes and Effects Analysis (FMEA)

Purpose

Failure Modes and Effects Analysis (FMEA) is a method designed to:

- Identify and fully understand potential failure modes and their causes, and the effects of failures on the system or end users, for a given product, process or system.
- Assess the risk associated with the identified failure modes, effects and causes and prioritize issues for corrective/preventive actions.
- Identify and carry out corrective actions to address the most serious concerns.

Objective

FMEA is used to understand the causes of the failures in order to take actions to reduce the risk(s) to an acceptable level.

Types of FMEAs

The most common types of FMEAs are System FMEA, Design FMEA and Process FMEA.

System FMEA is the highest-level analysis of an entire system made up of various subsystems. The focus is on system-related deficiencies, including system safety, system integration or interfaces between subsystems or with other systems, interactions with the surrounding environment, human interaction, service and other issues that could cause the overall system not to work as intended. In Systems FMEAs, the focus is on functions and relationships that are *unique* to the system as a whole (i.e., do not exist at the lower levels). Included are failure modes associated with interfaces and interactions, in addition to considering single-point failures (where a single component can result in complete failure of the entire system). Some practitioners separate out human interaction and service into their own respective FMEAs.

Design FMEA focuses on product design, typically at the subsystem or component level. The focus is on design-related deficiencies, with emphasis on improving the design and ensuring product operation is safe and reliable during the useful life of the equipment. The scope of the Design FMEA includes the subsystem or component itself as well as the interfaces between adjacent components.

Process FMEA focuses on the manufacturing process or assembly process, emphasizing how the manufacturing process can be improved to ensure that a product is built to design requirements in a safe manner, with minimal downtime, scrap and rework. The scope can include manufacturing and assembly operations, shipping,

incoming parts, transporting of materials, storage, conveyors, tool maintenance and labeling. Process FMEAs most often assume the design is sound.

Application

The FMEA is a methodic examination of the components of a system, which is used to identify how a component can fail, how the system will react to the failure and will the failure result in a safety concern or risk. It can also serve as a tool to determine if the failure is detectable (which can assist in developing trouble-shooting and maintenance guides) and if redundant systems are warranted. The FMEA is a component-to-system oriented ("bottom-up") technique, which looks at one failure at a time. Therefore, it may not identify hazards from multiple failure situations.

Typically, FMEAs have been directed at the failure of parts in mechanical systems, but the tool is suitable for analyzing the failure of any component of any type system. At BNL, FMEAs have been used extensively in the RHIC cryogenic systems analysis *(see examples).*

The technique is universally applicable to systems, subsystems, components, procedures, and interfaces. The FMEA can be thought of as a more formal and detailed "What-If Analysis." The FMEA can be used in place of the What-If Analysis when greater detail is needed, or it can be used to examine the impact of hazards developed using the What-If Analysis in much greater detail.

Using a small inter-disciplinary team with system knowledge is usually the most effective approach.

Methodology

FMEA Roadmap for performing effective FMEA's at a high-level:

1. **Preparation**
    a. Determine the scope
    b. Visual Depiction (such as FMEA Block Diagram or Process Flow diagram)
    c. Assemble the Right Team (not done by one or two people)
    d. Establish Ground Rules and Assumptions
    e. Gather Information
2. **Conducting The Meeting**
    a. Identify and list all major components, their functions, and/or processes
    b. Determine the Failure Modes
    c. Identify Effects of Failure
    d. Assess the Severity of Effects (Severity)
    e. Identify Causes of Failure
    f. Identify Current Prevention Controls
    g. Assess Probability of Occurrence (Occurrence)
    h. Identify Current Detection Controls
    i. Assess the Probability of Detection (Detection)
    j. Calculate the Risk Priority Number (RPN= [Severity] X [Occurrence] X [Detection])
    k. Assess and Prioritize Risk
    l. Develop Corrective Actions (CAs)
    m. Calculate the Resultant-Final Risk Assessment (as a result of CA implementation) Risk Priority Number (RPN)
3. **Follow-up**
    a. Review High Risk and Actions with Management
    b. Implement Corrective Actions
    c. Audit FMEA CA Effectiveness
    d. Link FMEA to Test/Control/Maintenance Plans
    e. Update FMEA with Lessons Learned/ Operational Experience

Risk Priority Number (RPN) Limitations

RPN has a number of limitations and is not a perfect representation of the risk associated with a failure mode and associated cause. Practitioners who use RPN should be aware of the inherent limitations and take measures to be sure product and process risks are properly characterized and addressed. Examples of limitations to RPN include:

1. It is subjective, not objective
2. The potential values of RPN are not continuous
3. The Detection scale has its own limitations
4. There can be many duplicate RPN values, representing different combinations of severity, occurrence and detection rankings
5. The practice of using RPN thresholds is not advised.

When RPN is used, high severity must be considered regardless of RPN value.

Many organizations use alternatives to RPN, such as severity and occurrence. For example, FMECA (FMEA, with the added step of Criticality Analysis) uses severity and occurrence risk rankings as input to the criticality risk, without the use of a detection risk ranking. When severity and occurrence risk rankings are used by themselves, care must be taken to understand potential risk due to inability to detect failure modes and their causes, and properly characterize and address this risk.

Completeness

Completeness of the analysis is a function of the degree to which the

1. failure modes are identified and explored.
2. possible effects are identified for each failure mode.
3. effects of multiple, co-existent failure modes are analyzed.

FMEA Success Factors

1. Understanding the fundamentals and procedures of FMEAs, including the concepts and definitions.
2. Selecting the right FMEA projects
3. Selecting the right FMEA Team (small inter-disciplinary team with system knowledge)
4. Preparation steps for each FMEA project
5. Applying lessons learned and quality objectives
6. Providing effective facilitation
7. Implementing an effective company-wide FMEA Process *(see Figure 1 below)*

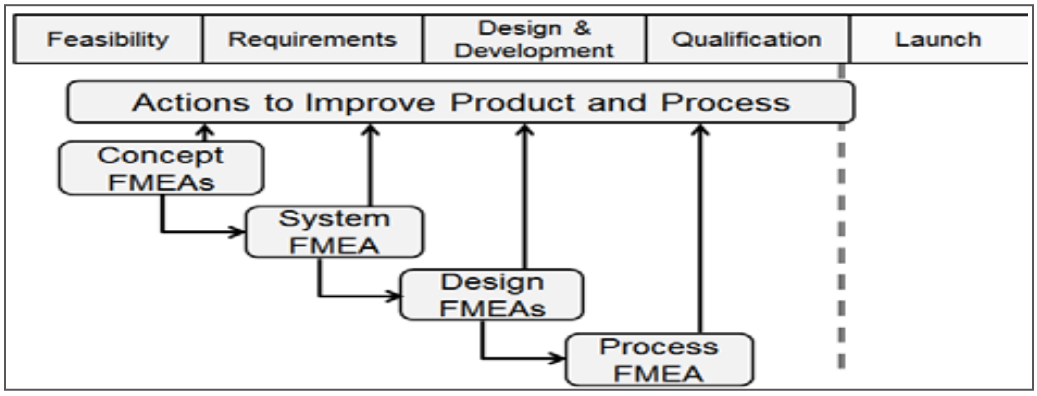


Figure 1. FMEA and Stage Gate Process - High Level

Implementing these FMEA success factors will help ensure FMEAs achieve safe, reliable and economical products and processes.

Limitations

The technique has been highly useful at BNL in evaluating complex cryogenic systems. It is, however, time consuming and requires a significant skill level. A Fault Tree Analysis is sometimes used in its place, although the FMEA technique has the advantage that no undesirable event needs to be predetermined to enable its use.

Advantages of the FMEA technique are
- It produces a comprehensive review
- It is good for complex systems
- It is an easy concept to grasp
- Computer software is available for assistance.

Disadvantages are
- Human errors may be missed
- It is time consuming, depending on the complexity of the system
- It can be expensive, depending on the complexity of the system
- It may not pick up multiple failures.

References

Department of Defense, Military Standard 756, "Reliability Prediction," 1985.

Department of Defense, Military Standard 1629A, "Procedures for Performing a Failure Mode, Effects and Criticality Analysis," November 1980.

Hammer, W., "Handbook of System and Product Safety," Prentice-Hall, Englewood Cliffs, NJ, 1972 (pp. 148-156).

Hammer, Willie, "Occupational Safety Management and Engineering," Prentice-Hall, 1981 (pp. 466-468).

Wallace, R.C., "A Step by Step Guide to FMECA," Reliability Review, Vol. 5 No. 2, June 1985.

Secretary of the Air Force, "Air Force Pamphlet 91-215, Operational Risk Management Guidelines and Tools," September 1997.

United States Military, 1949, Mil-P 1629 "Procedure for performing a failure mode effect and criticality analysis"

Fadlovich, Erik. Performing Failure Mode and Effect Analysis [Online] 2007 [cited 2010; Available from: http://www.embeddedtechmag.com/component/content/article/6134, Embedded Technology

Carl S. Carlson, Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes using Failure Mode and Effects Analysis, John Wiley & Sons, Wiley Series in Quality & Reliability Engineering, 2012

AIAG, Potential Failure Mode and Effects Analysis (FMEA) Reference Manual Fourth Edition [2008]; note, the scales in this tutorial have been re-formatted, abbreviated and/or shortened for readability

FMEA Standards

There are many standards and guidelines published that cover the scope and general procedure for doing FMEAs or FMECAs. Some of the more common and relevant are:

SAE J1739, Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) [2009]

AIAG, Potential Failure Mode and Effects Analysis (FMEA) Reference Manual Fourth Edition [2008]

MIL-STD-1629A, Procedures for Performing a Failure Mode Effects and Criticality Analysis (Cited for cancelation in1994, but still used in some military and other applications)

SAE ARP5580, Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile
Applications [2001]

IEC 60812, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA) [2006]

Examples of Scales

SEV - Severity Evaluation Criteria

Effect	Criteria: Severity of Effect	Rank
Hazardous/ Disaster	Complete loss of system or major sub-system and potential for hazard to life – e.g. vessel burn through/ radiation incident. Vacuum vessel or port implosion...etc Legal action possible	10
Disaster	Complete loss of entire system or sub-system – Slit and assembly. Customer completely dissatisfied.	9
Extreme	Complete loss of function. Critical component and assembly destroyed or put out of action for months. Customer extremely dissatisfied	8
Severe	Complete loss of primary function. Major work refitting and testing. Customer highly dissatisfied	7
High	Part loss or limitation of primary function and/or secondary function (e.g. can focus but only after long). Customer very dissatisfied	6
Moderate	Primary function intact (able to deliver focussed beam) but secondary function disabled or limited. E.g. beam steering limited/ beam drift with time and/or severe delay to completion. Customer dissatisfied	5
Low	Inconvenience or difficulty in achieving certain functions and/or very delayed project finish. Customer dissatisfied	4
Very Low	Certain inconveniences observed (possibly not covered by specification) but can be worked around =- e.g. cross-talk move on pitch affects bend, bender must be refocused after move. Customer mostly satisfied but problem noted	3
Minor	Inconveniences observed in certain operation (e.g. motions slightly too slow). Customer overall mostly satisfied	2
None	No Effect	1

OCC: Occurrence Evaluation Criteria

Rates	Criteria: Occurrence Rates	Rank
Extremely High	Failure almost inevitable > 1 in 2	10
Very High	Failure rate ~ 1in 3. Very high number of failures likely/	9
High	Failure rate > ~ 1in 8. High number of failures likely	8
Moderately High	Failure rate > ~ 1in 20. Frequent failure likely	7
Moderate	Failure rate > ~ 1in 80. Moderate number of failures	6
Moderate Low	Failure rate > ~1in 400. Only occassional, infrequent failures	5
Low	Failure rate > ~1in 1,000. Few failures ever expected	4
Very Low	Failure rate ~1in 10,000. Very few failures ever expected.	3
Exceptionally Low	100,000 to 1 in million). Very remote possibility of failure (within typical six – sigma criteria	2
None	Extremely low probability of occurrence <1 million	1

DET: Design and Test Detection Evaluation Criteria

Probability	Criteria: Probability of detecting failure	Rank
Absolute Uncertainty	Design control and test procedure cannot detect a potential mechanism and subsequent failure mode.	10
Very Remote	Very remote possibility that design control and test procedure can detect a potential mechanism and subsequent failure mode.	9
Remote	Remote possibility that design control and test procedure can detect a potential mechanism and subsequent failure mode.	8
Very Low	Very Low probability (<2%) that design control and test procedure can detect a potential mechanism and subsequent failure mode.	7
Low	Low probability (e.g.<10%) that design control and test procedure can detect a potential mechanism and subsequent failure mode.	6
Moderate	Moderate probability (e.g.> 50%) that design control and test procedure can detect a potential mechanism and subsequent failure mode.	5
Moderate High	Moderate high probability (e.g.> 85%) that design control and test procedure can detect a potential mechanism and subsequent failure mode.	4
High	Moderate high probability (e.g.95%) that design control and test procedure can detect a potential mechanism and subsequent failure mode.	3
Very High	Moderate high probability (e.g.> 99%) that design control and test procedure can detect a potential mechanism and subsequent failure mode.	2
Almost Certain	Design Controls have very high probability (99.99%)that potential cause/mechanisms and subsequent failure mode (Six –sigma) detected	1

Example of an Occurrence scale for Design FMEAs

Likelihood of Failure	Criteria: Occurrence of Cause	Criteria: Occurrence of Cause (Incidents per Item)	Rank
Very High	New technology/new design with no history	> 100 per thousand items > 1 in 10	10
	Failure inevitable with new design, new application, or change in operating conditions	50 per thousand items 1 in 20	9
High	Failure likely with new design, new application, or change in operating conditions	20 per thousand items 1 in 50	8
	Failure uncertain with new design, new application, or change in operating conditions	10 per thousand items 1 in 100	7
Moderate	Frequent failures associated with similar designs or in design testing	5 per thousand items 1 in 200	6
	Occasional failures associated with similar designs or in design testing	2 per thousand items 1 in 500	5
	Isolated failures associated with similar design or in design test	1 per thousand items 1 in 1,000	4
Low	Only isolated failures associated with almost identical design or in design testing	0.5 per thousand items 1 in 2,000	4
	No observed failures associated with almost identical design or in design testing	0.1 per thousand items 1 in 10,000	2
Very Low	Failure is eliminated through preventative control	< 0.01 per thousand items < 1 in 100,000	1

Example of an Occurrence scale for Process FMEAs

Likelihood of Failure	Criteria: Occurrence of Cause (Incidents per Item)	Rank
Very High	> 100 per thousand items > 1 in 10	10
	50 per thousand items 1 in 20	9
High	20 per thousand items 1 in 50	8
	10 per thousand items 1 in 100	7
Moderate	5 per thousand items 1 in 200	6
	2 per thousand items 1 in 500	5
	1 per thousand items 1 in 1,000	4
Low	0.5 per thousand items 1 in 2,000	4
	0.1 per thousand items 1 in 10,000	2
Very Low	< 0.01 per thousand items < 1 in 100,000	1

Example of Detection scale for Design FMEAs

Opportunity for Detection	Likelihood of Detection	Criteria: Likelihood of Detection by Design Control	Rank
No detection opportunity	Absolute Uncertainty	No current design control or cannot be detected	10
Not likely to detect at any stage	Very Remote	Design controls have a weak detection capability	9
Post Design Freeze and prior to launch	Remote	Product verification after design freeze and prior to launch with pass/fail testing	8
	Very Low	Product verification after design freeze and prior to launch with test to failure testing	7
	Low	Product verification after design freeze and prior to launch with degradation testing	6
Prior to Design Freeze	Moderately	Product validation prior to design freeze using pass/fail testing	5
	Moderately High	Product validation prior to design freeze using test to failure	4
	High	Product validation prior to design freeze using degradation testing	3
Virtual Analysis Correlated	Very High	Design controls have strong detection capability prior to design freeze	2
Detection N/A: Failure Prevention	Almost Certain	Failure cause or failure mode cannot occur because it is fully prevented	1

Example of a Detection scale for Process FMEAs

Opportunity for Detection	Likelihood of Detection	Criteria: Likelihood of Detection by Process Control	Rank
No detection opportunity	Absolute Impossible	No current process control; Cannot detect or is not analyzed	10
Not likely to detect at any stage	Very Remote	Failure Mode/Cause is not easily detected	9
Problem Detection Post Processing	Remote	Failure Mode detection post-processing by operator – visual/tactile/audible means	8
Problem Detection at Source	Very Low	Failure Mode detection in-station by operator – visual/tactile/audible means	7
Problem Detection Post Processing	Low	Failure Mode detection post-processing by operator – use of variable gauging	6
Problem Detection at Source	Moderate	Failure Mode detection in-station by operator; variable gauging or automated controls	5
Problem Detection Post Processing	Moderately High	Failure Mode detection post-processing by automated controls; lock part to prevent further processing	4
Problem Detection at Source	High	Failure Mode detection in-station by automated controls; automatically lock part in-station	3
Problem Prevention	Very High	Failure Mode detection in-station by automated controls; prevent discrepant part from being made	2
Detection N/A: Error Prevention	Almost Certain	Failure Mode/Cause prevention as a result of fixture design, machine design or part design	1

Examples/Format

Example 1. (FMECA-excerpt)

System:_____ Date:_____

Sub-System _____ Sheet ____ of _____

Reference Dwg: _____ Compiled by: _____

Approved by:_____

Item/ Component Number	Function	Failure Mode	Failure Effect	Probability of Occurrence	Criticality or Hazard Category/ Risk	Action to Reduce Failure Rate or Effects
Valve xyz	Controls flow of Liquid Hydrogen to target	Valve fails open	Excessive amount of Hydrogen in target >LEL, possible fire/explosion	0.0025	Critical	LEL monitor wired into ventilation system start up

Example 2. FMEA RHIC Beam Stop System

Component #	Nomenclature	Function	Failure Position Risk	Failure Effect	Redundancy Comments
D08-02	Pressure Regulator Filter Comb	Provides clean pneumatic pressure to operate beam stops.	Closed	No reduction of air pressure, solenoid valve jammed in the as is position	NO
			Low Risk		High contaminate levels could cause all stops to lock open.
D08-02	Pressure Regulator Filter Comb	Provides clean pneumatic pressure to operate beam stops	Open	Contaminants may cause solenoid valves to jam in the as is position	NO
			Low Risk		High contaminate levels could cause all stops to lock open
G12-bsx.2	Yellow Beam Stop	Provides mechanical obstruction of beam tube in counter-clockwise direction.	Gate Jammed	Foreign object causes gate to hang	Yes
			Low Risk		Stops should be cycled from MCR after each closure with beam.
G12-bsx.2	Yellow Beam Stop	Provides mechanical obstruction of beam tube in counter-clockwise direction.	Welded Gate	Stray Beam or high beam wake electrical field's causes gate welding.	Yes
			Low Risk		Stops should be cycled from MCR after each closure with beam.
G12-bsx.1	Blue Beam Stop	Provides mechanical obstruction of beam tube in clockwise direction.	Gate Jammed	Foreign object causes gate to hang	Yes
			Low Risk		Stops should be cycled from MCR after each closure with beam
G12-bsx.1	Blue Beam Stop	Provides mechanical obstruction of beam tube in clockwise direction.	Welded Gate	Stray Beam or high beam wake electrical fields causing gate welding	Yes
			Low Risk		Stops should be cycled from MCR after each closure with beam.
K58	Yellow BS Relay	Energized Yellow Beam Stop relay's solenoid allowing gate to open.	Contact Closed	Beam Stop open. Power to solenoid not removed with permission signal is lost.	Yes
			Low Risk		

Component #	Nomenclature	Function	Failure Position	Failure Effect	Redundancy
			Risk		**Comments**
D08-02	Pressure Regulator Filter Combo	Provides clean pneumatic pressure to operate beam stops.	Closed	Insufficient air flow to open valve. Spring pressure only must close valve.	NO
			Routine Risk		High contaminate levels could cause all stops to lock open.
D08-02	Pressure Regulator Filter Comb	Provides clean pneumatic pressure to operate beam stops.	Clogged	Insufficient air flow to open valve. Spring pressure only must close valve.	NO
			Routine Risk		High contaminate levels could cause all stops to lock open
PCB18-U2	Opto 22 Power Module Isolating Transistors	Provides ground to K36 when P13 Div B BS request signal allows beam	Open	Associated control relay losses ground shutting beam stop when control station request is open	Yes
			Routine Risk		
K58	Opto 22 Power Module Isolating Transistors	Provides ground for K36 when P13 Div B BS request signal allows beam	Short	Associated control relay grounded when permission is removed	Yes
			Routine Risk		
	Yellow BS Relay	Energizes	Open	Beam Stop shuts. Power to solenoid removed.	Yes
			Routine Risk		

FMEA Template

Assembly/Component: Drawing Ref:				FAILURE MODES and EFFECTS Analysis Design and System FMEA							FMEA No: Prepared By:		Rev. 0					
Item	**Function**	**Potential Failure Mode**	**Potential Effect(s) of Failure**	**SEV**	**Potential Cause(s) of Failure**	**OCC**	**Current Design Controls (Prevention)**	**Current Design Controls (Detection)**	**DET**	**RPN**	**Recommended Action(s)**	**Actions Taken**	**Responsible Person**	**Completion Date**	**SEV**	**OCC**	**DET**	**RPN**

This guidance is not intended to be all-inclusive. It is intended to give the user some basic information as to the purpose of the analysis, how it is applied, and methods for conducting the analysis, necessary resources, and limitations. Where possible, examples pertinent to BNL operations were used to show typical contents and formats.

Fault Tree Analysis

Purpose:

The purpose of a Fault Tree Analysis (FTA) is to assess a system or sub-system by identifying a postulated undesirable end event and examining the range of potential events that could lead to that end event using a "logic tree." The FTA is developed through deductive logic from an undesired event to all sub-events that must occur to cause the undesired event. The FTA can be applied at any point in the life of a facility. The FTA can be used to support the Preliminary Hazard Analysis (PHA) during facility design.

Application:

The technique is universally applicable to systems of all kinds, however, the following must be taken into consideration:

1. The undesirable system events, which are to be analyzed/abated, and their contributors, must be foreseen.

2. Each of those undesirable system events must be analyzed individually.

Because of its relative complexity and detail, it is normally not cost-effective to use the FTA for low risk applications. The FTA would typically only be used for those hazards that have been screened to the category 3 level using the hazard screening tool.

Methodology:

The Fault Tree Analysis (FTA) can model the failure of a single event or multiple failures which lead to a single system failure. The FTA is a top-down analysis. The method identifies an undesirable event and the contributing elements (faults/conditions) that would lead to it. The contributors are interconnected with the undesirable event, using network paths through Boolean logic gates. Some of the symbols used in FTA are shown in Figure 1.

The following basic steps are used to conduct fault tree analysis:

1. Define the top undesired event.

2. Define the physical and analytical boundaries of the system.

3. Construct the tree structure.

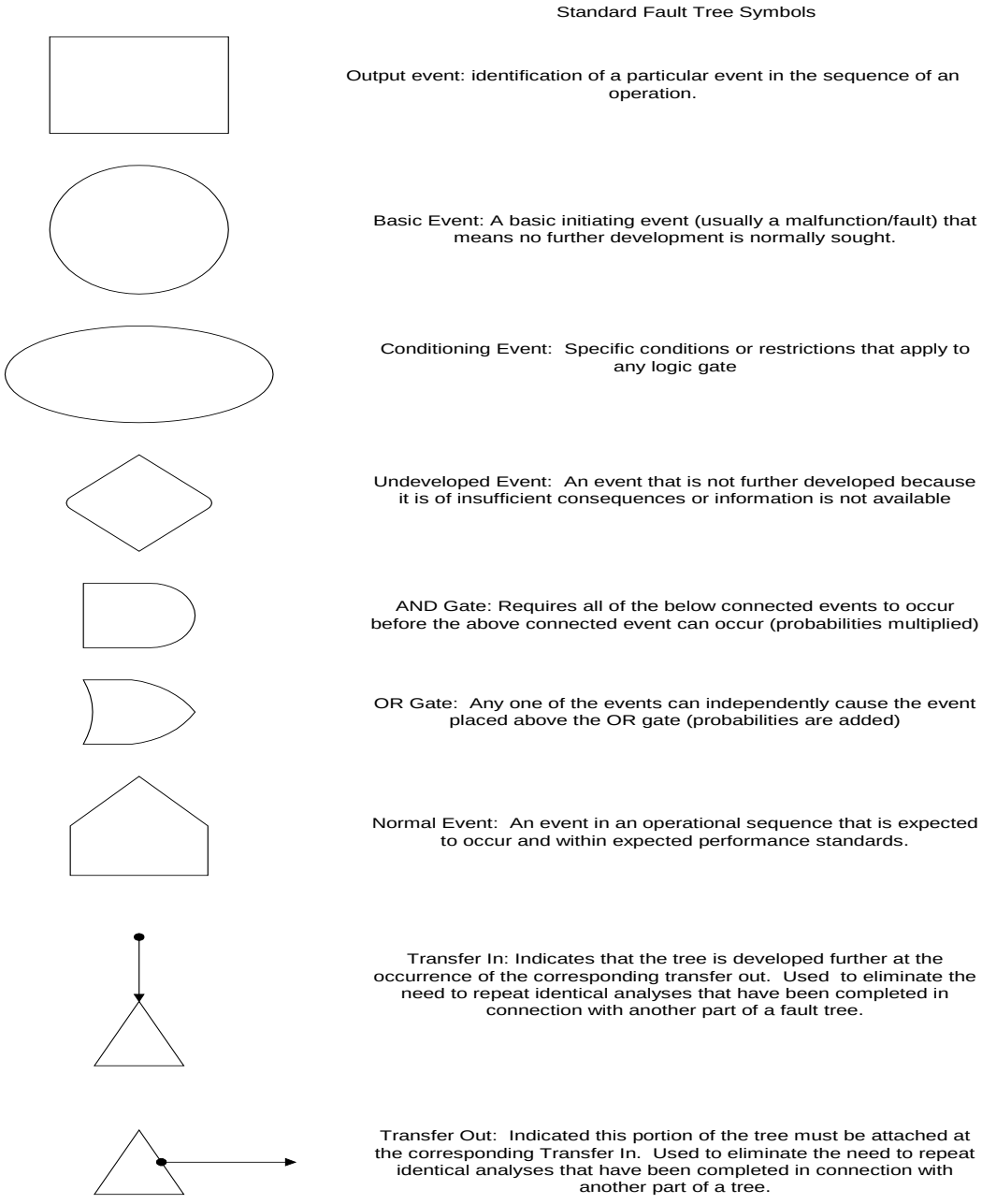
4. Develop the path of failures for each branch to the logical initiating failure.

5. Evaluate fault tree probability.

6. Analyze the results.

Once the fault trees have been developed to the desired degree of detail, the various paths can be evaluated to arrive at a probability occurrence. Cut sets are combinations of failures of components causing system failure (i.e., causing the top event of the tree). Minimal cut sets are the smallest combinations causing system failure. Identifying the minimal cut sets will help determine the controls needed to prevent that event.

Figure 1.


Standard Fault Tree Symbols
Output event: identification of a particular event in the sequence of an operation.
Basic Event: A basic initiating event (usually a malfunction/fault) that means no further development is normally sought.
Conditioning Event: Specific conditions or restrictions that apply to any logic gate
Undeveloped Event: An event that is not further developed because it is of insufficient consequences or information is not available
AND Gate: Requires all of the below connected events to occur before the above connected event can occur (probabilities multiplied)
OR Gate: Any one of the events can independently cause the event placed above the OR gate (probabilities are added)
Normal Event: An event in an operational sequence that is expected to occur and within expected performance standards.
Transfer In: Indicates that the tree is developed further at the occurrence of the corresponding transfer out. Used to eliminate the need to repeat identical analyses that have been completed in connection with another part of a fault tree.
Transfer Out: Indicated this portion of the tree must be attached at the corresponding Transfer In. Used to eliminate the need to repeat identical analyses that have been completed in connection with another part of a tree.

Completeness:

The completeness of the analysis is limited by the presumption that the

1. relevant undesirable events have been identified

2. contributing factors have been adequately identified and explored in sufficient depth.

Apart from these limitations, the technique as usually practiced is regarded as among the most thorough of those commonly used for general system application.

Resources/Skills Required:

Significant training and experience is necessary to use this technique properly. Skills for the uninitiated require from 8 to 40 (or more) hours of study and some practical experience. Prior knowledge of Boolean algebra and /or the use of logic gates is helpful.

Limitations:

Application, though time-consuming, is not difficult once the technique has been mastered. Computer aids are available. Unlike Failure Modes and Effects Analysis, the technique explores only those faults and conditions leading to unacceptable losses.

FTA has several strengths. The procedures are well defined and focus on failures. The top-down approach requires analysis completeness at each level before proceeding. It cannot guarantee identification of all failures but the systematic approach enhances the likelihood of completeness. The FTA addresses effects of multiple failures by identifying inter-relationships between components and identifying minimal failure combinations that cause the system to fail (minimal cut sets). The method addresses the effects of design, operation, and maintenance.

The FTA can handle complex systems. It provides a graphical representation that aids in understanding these complex operations and inter-relationships between subsystems and components. The FTA provides both qualitative and quantitative (probabilistic) information. Probabilities may be assigned to each sub-event and aggregated to determine an overall probability for the top event.

The method is capable of producing numerical statements of the probability of occurrence of undesirable events, given probabilities of contributing factors. That capability leads to a common abuse: much effort can be expended in producing "refined" numerical statements of probability, based on contributing factors whose individual probabilities are poorly known and to which broad confidence limits should be attached. The technique can be expensive and very time consuming.

The method identifies minimum sets of contributing factors, which, if they occur, will invariably precipitate the undesirable event. Common causes and human operator paths to events are also identified by use of the method.

References:

Briscoe, G.J., "Risk Management Guide," EG&G Idaho, Inc., SSDC-11, June 1977 (pp. 18-20).

Bullock, M. G., "Change Control and Analysis," EG&G Idaho, Inc., SSDC-21, March 981 (pp.208-211).

Crosetti, P. A., "Reliability and Fault Tree Analysis Guide," EG&G Idaho, Inc., SSDC-22. February 1982.

Department of Defense, Military Standard 882C, "System Safety Program Requirements," January 1993.

Hammer, W., "Handbook of System and Product Safety," Prentice-Hall, Englewood Cliffs, NJ, 1972 (pp. 238-246).

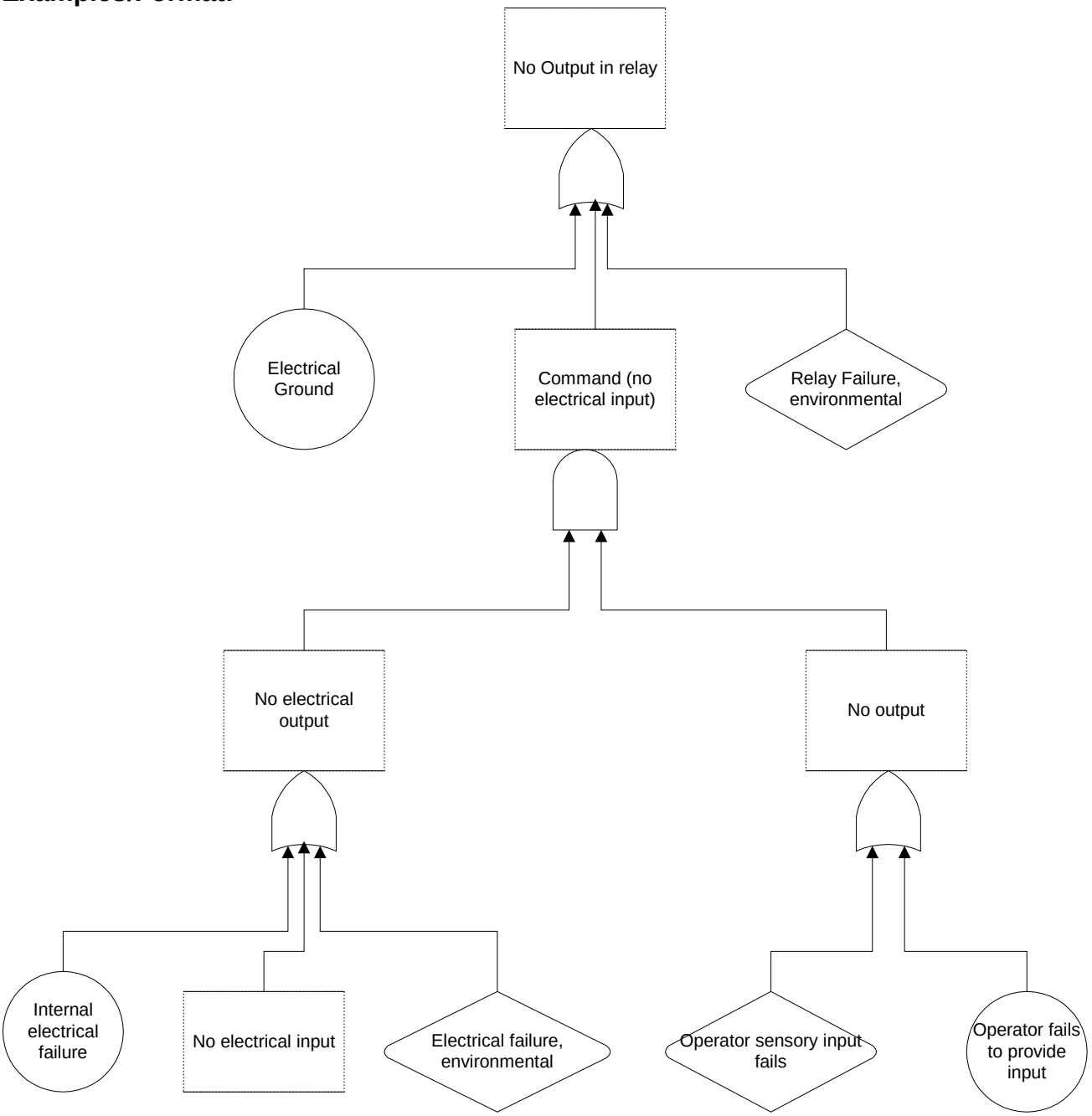
Hammer, Willie, "Occupational Safety Management and Engineering," Prentice-Hall, 1981 (pp.468-475).

Vesely, W.E. et al, "Fault Tree Handbook: NUREG-0492," U.S. Government Printing Office, January 1981.

Roland, Harold and Moriarty Brian, "System Safety Engineering and Management", John Wiley & Sons, 1983.

Secretary of the Air Force, "Air Force Pamphlet 91-215, Operational Risk Management Guidelines and Tools," September 1997.

Examples/Format:



Guidance on Fire Hazard Analysis

Effective Date: **May 13, 2016**

Fire is one of the predominant hazards. Its potential is present in almost all facilities and operations. How severe the hazard is and how fire impacts the facility operations is dependent on the specific configuration of the facilities. A Fire Hazard Analysis (FHA) is a specific document, required by the DOE/BSA contract. It is one of the documents that fulfill the requirement for a determination of a facility's fire risk (see DOE O 420.1C, *Facility Safety).*

Refer to the Fire Safety Subject Area regarding Fire Hazard Analysis.

This guidance is not intended to be all-inclusive. It is intended to give the user some basic information as to the purpose of the analysis, how it is applied, and methods for conducting the analysis, necessary resources and limitations. Where possible, examples pertinent to BNL operations were used to show typical contents and formats.

Preliminary Hazard Analysis (PHA)

Purpose:

The Preliminary Hazard Analysis (PHA) technique is used in the early stages of system design, saving resources (time, money, and personnel) which may have been required for a redesign if the hazards were discovered at a later date. The PHA provides an initial overview of the hazards present in the overall flow of the operation. It provides a hazard assessment that is broad, but usually not detailed. The key idea of the PHA is to at least briefly consider risk in every aspect of an operation. The PHA helps overcome the strong tendency in traditional, intuitive risk management to focus immediately on risking one aspect of an operation. This often leads to overlooking more serious issues hidden in other aspects of the operation. The PHA will often serve as the total hazard ID process when risk is low or routine (activities with a hazard rate of 2). In higher risk operations (activities with a hazard rate of 3), it serves to focus and prioritize follow-on hazard analyses by displaying the full range of risk issues.

Application:

Preliminary Hazard Analyses may be applied to all systems, subsystems, components, procedures. It must be performed first, i.e., prior to or as an initial step of design, shakedown, operation, maintenance, and refurbishment to be effective.

Methodology:

The PHA is a broad brushed, initial study, to identify apparent hazards, and the methods to effectively control them. To do this analysis, checklists are often used. A team approach is frequently used, which consists of personnel proficient in the type of activity in question meeting and listing all the hazards that have been experienced in the past. At least one

person on the team should be proficient in the body of regulations, standards, technical orders, and operations instructions that may be available/applicable.

An alternative method would be to apply any hazard analysis techniques (i.e., Failure Modes and Effects Analysis, Fault Tree Analysis, What-If, Fire Hazard Analysis), singly or in combination, early in system life cycle, preferably during formulation of design concept.

The steps in conducting a PHA are as follows:

- Ensure participants have a thorough knowledge of the anticipated flow of the operation.
- Collect all relevant design criteria, drawings, system operations, manuals
- Visualize the expected flow of events in time sequence from beginning to end of the operation.
- Consider human factor events as well as design/mechanical failures.
- Use a PHA matrix (see example/format) to identify and document the potential hazards, initiators, consequences, barriers and frequency. Note: there are many existing formats for PHAs which may be modified to better fit the system being evaluated.
- Identify those hazards with unacceptable consequences and frequencies and further develop the controls and/or utilize another Analysis technique, e.g., "What-If Analysis," Fire Hazards Analysis, etc.
- To document analysis
  - -Briefly describe the operation
  - -Describe the facility/operation safety features
  - -Further expand on those hazards that had an unacceptable consequences and probability of occurrence.
  - -Include the PHA matrix

Completeness:

Completeness depends upon the technique(s) used and the depth to which they are employed as well as the design information available at the time of the analysis.

Resources/Skills Required:

Requires experience and understanding of the subject. Competence is dependent upon the technique(s) selected with which to perform the Preliminary Hazard Analysis. (See General Comments below).

Limitations:

The Preliminary Hazard Analysis (PHA) is not strictly speaking, a discrete technique. It may be as simple as listing all the problems encountered on the last project of this type (Preliminary Hazards List). It may be the application of any technique, or any group of them, performed preliminarily, i.e., in the initial stages of design. For example, the PHA is often prepared and submitted as part of the Preliminary or Conceptual Design Review, as was done with the proposal for the installation of a 70 MeV accelerator at Building 801.

The PHA is based on any and all data available at the early design stages. This in itself poses some limitations from having only basic or incomplete information. However, the PHA is usually a "living document" that is updated and reviewed throughout the development cycle.

The evolution of the PHA, used within the DOE system and at BNL, generally incorporated some background on the process/system/facility, including known design criteria, inventories of hazardous materials, and facility safety features.

References:

Department of Defense, Military Standard 882C, "System Safety Program Requirements," January 1993.

Hammer, Willie, "Occupational Safety Management and Engineering," Prentice-Hall, 1981 (pg. 464-466).

Secretary of the Air Force, "Air Force Pamphlet 91-215, Operational Risk Management Guidelines and Tools," September 1997.

Roland, Harold and Moriarty Brian, "System Safety Engineering and Management", John Wiley & Sons, 1983.

Secretary of the Air Force, "Air Force Pamphlet 91-215, Operational Risk Management Guidelines and Tools," September 1997.

Examples/Format:

Generic Format for PHA

Nomenclature or Part or Subsystem affected	**Operating Mode**	**Hazard Description/ Potential Hazard**	**Failure Mode/ Initiator**	**Hazard Effects/ Consequences**	**Recommended Control/Barrier**	**Estimated Probability/Frequency**	**Comments**
The formal name of the part of subsystem, the drawing number, or procedure number. The part or procedure described is the one at which the hazardous condition will originate, the part affected.	The mode during which the hazard occurs. The operation mode may identify different hazards for the same part, subsystem, or procedure.	Brief description of the hazard. The hazard is the result of malfunction or failure that causes personnel injury, death or property damage.	Briefly describe the mode of failure of the part or procedure that allows the hazard to develop. More than one failure mode may be cited for each part or procedure and each hazard.	This describes the effects of the hazard on the system/ personnel. Multiple effects can be described.	Describes the countermeasure that will effectively control the hazard. Typically results in a reduction in the severity or probability of occurrence.	Typically defined in qualitative terms, Frequent = likely to occur repeatedly during life cycle of system (test/activity/operation) Reasonably Probable = likely to occur several times in a life cycle of a system Occasional = likely to occur sometime in the life cycle of the system. Remote = Not likely to occur in the life cycle of system, but possible Extremely Remote = probability of occurrence cannot be distinguished from zero. Impossible = physically impossible to occur.	May pertain to the hazard severity, the operation, operating mode or anything that will influence the hazard.

Figure 1, Example PHA summary for the "Whole Body Neutron Irradiation Facility"

Potential Hazard	Initiator	Consequences	Barrier	Frequency	Comments
Source(s) Stuck in up position (above floor level)	-mechanical - electrical	Increased exposure by <15 mrem	- source position indicators - alarm on door - manual motor override - radiation monitor	Reasonably probable	Failure of a fuse is used because this failure mode has occurred.
Source(s) Stuck in down position (below the floor level)	- mechanical - electrical	- None (radiological) - program delay	- Source position indicators. - Alarm on door - Manual motor override. - Radiation monitor.	Reasonably probable	Should one or more of the sources not raise for a patient irradiation, the operation would make the decision to continue or terminate. The patients dose would be adjusted accordingly.
Power failure	-supply interrupted	Would be the same as with the source stuck up, if the source was down during the power failure there would be no consequences	- Backup emergency generator would supply power in less than 2 seconds. - Manual motor override to lower sources to storage location. - Emergency lighting is provided for egress.	Remote	The emergency power was verified by testing 8/10/94.
Fire in vault source in down position (below floor level)	- Electrical	- None to sources - Program delays	- Automatic fire suppression system. - 24 hr video camera surveillance by security - Fire Department Response in < 4 minutes. - Combustibles held to minimum, no flammable liquids.	Remote	
Fire in vault, source in up position (above floor level)	- Electrical	- Release of Radioactivity to room environment	- Source encapsulated in stainless steel. - Source contained in stainless steel source holder inside steel and aluminum guide/storage tubes. - Sources further protected by being in-side non-combustible cell. - Automatic fire suppression system. - 24-hr video camera surveillance by security. - Fire Department response < 4 minutes. - Combustibles held to a minimum, no flammable liquids.	Remote	
Release of radioactivity to room environment	-Fire -Mechanical damage to source	Airborne radioactive contamination -Low to moderate worker exposure. -Room contamination.	- Sources contained in stainless steel jacket and source holder. - Sources stored in tubes 10' underground surrounded by a steel and aluminum tube embedded in sand.	Extremely Remote	

Potential Hazard	**Initiator**	**Consequences**	**Barrier**	**Frequency**	**Comments**
Unplanned exposure to radiation	-source stuck in up position (one or more)	-Minimal exposure <15 mrem based on source closest to operator being stuck and <25 seconds for patient evacuation.	-Source position indicators. -Alarm on door. -Radiation monitor. -Manual motor override	Reasonably Probable	
Flooding of source tubes	-Fire Suppression system activated. -Natural Phenomena Event.	-Source Tubes below floor fill with water. -Source containers and holders subject to future corrosion.	-Fire Suppression system alarmed into the Fire Department. Response times less than 4 minutes. -Early storm warning though NEXRAD weather tracking radar onsite.	Remote	Should the sources get wet they would be removed, dried and inspected.
Collapse of Building	Natural Phenomenon Event (Hurricane, Tornado or earthquake.	-Inability to retrieve sources from source tube storage	- Early storm warning from NEXRAD weather radar located on site.	Remote	Sources would be in the storage position should there be a possibility of a NPH event.
Cable break	-Mechanical binding of source or counter weight. -Defective cable connector.	-No immediate hazards. -Radiation dose to repair personnel.	-None	Remote	Original cables were replaced due to failure, new more reliable cables were installed.
Leaking sources	Encapsulation failure due to corrosion, weld failure, or mechanical damage.	Possible minor exposure to occupants -contamination of guide tube	-Stainless Steel encapsulated. -Secondary stainless steel source holder. -torque clutches -sources remotely handled -Sources are smear checked for detection leaks semi annually.	Remote	Records of semi-annual leak checks indicate the no source leakage has taken place. Should a source start to leak it would be picked up by this check before the leak became severe.

This guidance is not intended to be all inclusive. It is intended to give the user some basic information as to the purpose of the analysis, how it is applied, methods for conducting the analysis, necessary resources, and limitations. Where possible, examples pertinent to BNL operations were used to show typical contents and formats.

What-If Analysis

Purpose:

The purpose of the What-If Analysis methodology is to identify hazards, hazardous situations, or specific accident events that could produce an undesirable consequence. The What-If Analysis is especially effective in capturing hazard data about failure modes. It is somewhat more structured and rigorous than the Preliminary Hazard Analysis (PHA), and thus is a logical follow-up analysis to the PHA. Because of its ease of use, it is probably the single most practical and effective tool for use by operational personnel.

Application:

The What-If Analysis can be applied to almost any operation or system process. It is also useful in contingency planning and accident analysis.

Methodology:

The What-If Analysis technique is a brainstorming approach in which a group of experienced individuals familiar with a process ask questions or voice concerns about possible undesired events in the process. The What-If Analysis concept encourages an analysis team to think of questions that begin with "what-if." Through this questioning process, the team identifies possible accident situations, their consequences, and existing safeguards, then suggests alternatives for risk reduction. The potential accidents identified are neither ranked nor given quantitative implications.

The analysis team reviews the process from the conceptual stage through operations. At each step they ask "what-if" questions dealing with procedural errors, hardware failures, and software errors. The technique may simply generate a list of questions and answers about the process. However, it usually results in a tabular listing of hazardous situations, their consequences, safeguards, and possible options for risk reduction.

A classic use of the What-If Analysis is as the first tool used after the Preliminary Hazard Analysis (PHA). For example, the PHA reveals an area of hazard that needs additional investigation. Probably the best single tool to further investigate that area will be the What-If Analysis.

Method Guidelines:

- Ensure participants have a thorough knowledge of the anticipated flow of the operation.
- Visualize the expected flow of events in time sequence from beginning to end of the operation.
- Select a segment of the operation on which to focus.
- Visualize the selected segment with "Murphy" injected. Make a conscious effort to visualize failures. Ask "what if various failures occurred or problems arose?"
- Add potential failures and their causes to your hazard list and assess them based on probability and severity.
- The "What-If" Analysis can be expanded to further explore the hazards in an operation by using scenario thinking. To use scenario thinking, develop short scenarios, which reflect the worst credible outcome from compound effects of multiple hazards in the operation.
- Follow the guidelines below in writing scenarios:
  - Target length is 5 or 6 sentences, 60 words,
  - Do not dwell on grammatical details,
  - Include elements of man, machine, media, and management,
  - Start with history but sanitize,
  - Encourage imagination and intuition,
  - Carry the scenario to the worst credible outcome,
  - Use a single person or group to edit.

Completeness:

The degree of completeness in the application of the What-If Analysis methodology is directly dependent upon team make-up and the exhaustive nature of the "what-if" questions asked.

Resources/Skills Required:

The analysis must include at least one person experienced and knowledgeable in the process, and one knowledgeable in the analysis method. For simple processes, two or three people may be assigned to perform the analysis. However, larger teams may be required for more complex processes. The What-If Analysis is specifically designed to be used by personnel actually involved in an operation. Therefore, the most critical "What-If" resource is the involvement of operators and their first line supervisors.

Limitations:

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

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

A small interdisciplinary team is usually more effective.

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

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

References:

Department of Energy, DOE-HDBK-1101-96, "Process Safety Management for Highly Hazardous Chemicals," February 1996.

Department of Energy, DOE-HDBK-1100-96, "Chemical Process Hazard Analysis," 1996.

Department of Labor, 29 CFR 1910.119, "Process Safety Management," July 1992.

"Guidelines for Hazard Evaluation Procedures," Center for Chemical Process Safety, AIChE, 1992.

Secretary of the Air Force, "Air Force Pamphlet 91-215, Operational Risk Management Guidelines and Tools," September 1997.

Example/Format:

Example 1 (Extract):

System/Activity: HF system distribution Date:_____

WHAT IF	CONSEQUENCES	PROTECTION	SCENARIO	COMMENTS
…the HF cylinder corrodes through?	Cylinder leak, HF release to atmosphere, possible worker exposure via inhalation and skin, possibly fatal.	None	1	Check with supplier regarding cylinder inspection practices.
…the dock and the equipment is involved in a fire?	HF releases to atmosphere via vent OR cylinder rupture, with possible worker exposure via inhalation and skin, possibly fatal.	None Relief valves, rupture disks.	2a 2b	Consider sprinkler or deluge system.
….the hot water jacket on the HF corrodes through?	Large heat of solution, HF releases via vent, possible worker exposure via inhalation and skin, possibly fatal.	None. Relief valves, rupture disks	3a 3b	
….mositure is introduced into the HF cylinder via the N2 supply?	Heat of solution, HF release via vent, possible worker exposure via inhalation and skin, possibly fatal. HF solution attacks carbon steel, corrosion, leak or rupture, possible worker exposure via inhalation and skin, possibly fatal.	None	4a 4b	Prevention is procedure for monitoring N2 supply

Example 2:

System/Activity: Cooling Water Chlorinating System Date: _____

WHAT IF	CONSEQUENCES	PROTECTION	SCENARIO	COMMENTS
…the system is involved in a fire?	High pressure in chlorine cylinder, fusible plugs melt, chlorine releases into fire….	Ignition source control	1	Verify that the area is free from unnecessary fuel.
…the wrong material is received in the cylinder and hooked up?	Water contaminated, not sterilized	None	2	Prevention: supplier's procedures
…the cylinder's fusible plugs prematurely fail?	Chlorine release.	None	3	Purchase and train personnel in the use of a CL2 cylinder leak capping kit
…the pressure check valve fails open ()both pass chlorine gas?	Built-in relief valve opens, releasing chlorine to atmosphere.	None	4	
…the basin corrodes through?	Chlorinated water release.	Periodic inspection	5	
…the recirculation pump fails OR power is lost?	Eventually low chlorine in water, biological growth. Release of undissolved chlorine to atmosphere if pressure check valve fails.	None. Pressure check valve.	6a 6b	
…the chlorine cylinder is run dry and not replaced?	Eventually low chlorine in water, biological growth.	None.	7	

Facility/Area Risk Assessment Description

Facility Risk Assessments (FRAs) are conducted for specific areas where organizations operate equipment, either experimental or support equipment. These operational areas are considered "facilities." These area assessments can be used by workers, planners and job supervisors as a source of information on facility hazards and controls during work planning. FRAs may assist management in prioritizing resources and funding to reduce the hazards associated with their facilities.

The facility risk assessment incorporates the following information:

- Hazards associated with each facility or location;
- Hazards inside and outside of the building (e.g., confined spaces);
- Controls in place for hazards;
- Stressors that increase one or more of the components of risk;
- Estimate of the Occupancy of Use of the area or facility;
- Estimate of the potential severity of an accident associated with each hazard;
- Estimate of the likelihood of an accident or injury occurring for each hazard.

Risk Scoring System for Facility/Area Assessment

1. The associated point value for Parameters A, B, C is determined based on the following chart:

Point Value → Parameter ↓	1	2	3	4	5
Occupancy or Use	≤once/ year	≤once/ month	≤once/ week	≤once/ shift	>once/ shift
Severity	First Aid Only	Medical Treatment	Lost Time	Partial Disability	Death or Permanent Disability
Likelihood	Very Unlikely	Unlikely	Possible	Probable	Multiple

Note: A = Occupancy: the frequency of people being in the facility or area.
B = Severity: the consequence of the injury/illness if the event occurs.
C = Likelihood: the potential of the negative consequence occurring.

The values are based on experience with similar equipment, data from past events, lessons learned and the best judgment of the analysts.

2. The Risk score is determined by multiplying:

Occupancy (A) x Severity (B) x Likelihood (C) = Risk Score

3. The Facility Hazard risk level is calculated with no controls in place, the mitigated risk is recalculated with the existing controls in place.

4. The HVT provides a generic risk rank of each area based on the type of operational activity in that area (e.g., chemical laboratory, machine shop/technical shop, electronic fabrication) and typical hazards in that area. The risk scoring is based on three main broad categories of hazards (chemical, biological, physical) and is determined without established risk mitigating controls. The highest score represents the risk rank for that area (0 to 4 scale).

Facility/Area Risk Assessment Description

Facility Hazard Analysis Rating –Based on Pre-Control Risk

Risk*	0 to 20	21 to 40	41-60	61 to 80	81 or greater
Action/ Rank	**0**	**1**	**2**	**3**	**4**
HVT input	not required	not required	required	required	required

Mitigated Risk based on Post Control:

Risk**	0 to 20	21 to 40	41-60	61 to 80	81 or greater
	Negligible	Acceptable	Moderate	Substantial	Intolerable

4. The Hazard Validation Tool output consists of the following risk assessment matrix.
(Example: sample data is filled in)

Area Hazard Name:

Hazard(s)	Without Controls				With Controls			
	Occupancy A	**Severity B**	**Likelihood C**	**Risk* AxBxC**	**Occupancy A**	**Severity B**	**Likelihood C**	**Risk** AxBxC**
Chemical	5	4	4	80	5	3	2	30
Biological	4	1	2	4	4	1	1	4
Physical	4	3	3	36	4	3	2	24