SBMS

Forms | Contact List | SBMS Instructions | Help Desk

Find Subject Areas: Index | Categories | Alpha

Show Side Menu

Search Subject Areas & Legacy Documents:

Contents: Hazard Analysis

Effective Date: **March 2001**
Point of Contact: Hazard Analysis Subject Matter Expert

Section	Overview of Content (see section for full process)
Introduction	
1. Determining the Hazard Rating	• Use BNL Hazard Identification Tool to evaluate industrial or radiological facilities. • Run report. • Verify and concur with results of hazard rating. • Determine if further analysis is required.
2. Determining the Type of Hazard Analysis	• Compile list of hazards. • Determine hazard analysis and obtain concurrence. • Determine and document schedule and level of authorization. • Review and obtain concurrence for Authorization Plan Memorandum. • Modify Authorization Plan Memorandum, if necessary. • Submit revised Authorization Plan Memorandum to DDO for concurrence.
3. Conducting and Documenting the Hazard Analysis	• Conduct analysis agreed to in Authorization Plan Memorandum. • Review completed analysis. • Address all comments. • Place analysis in change control system. • Retain analysis.
4. Developing Operational Safety Limits (OSLs)	• Determine OSLs. • Complete FUA Change Analysis Basis Document. • Review OSLs. • Schedule an ORE before authorization or startup of facility.
Definitions	

Exhibits

Forms

Training Requirements and Reporting Obligations

This subject area does not contain training requirements.

This subject area contains reporting obligations. See the section Determining the Type of Hazard Analysis for information.

References

29 CFR 1910.119, Process Safety Management of Highly Hazardous Chemicals

ALARA Program Subject Area

Bloodborne Pathogens Subject Area

BNL Emergency Services Website

BNL Hazard Identification Tool

Community Involvement in Laboratory Decision-Making Subject Area

Confined Spaces Subject Area

DOE-STD-1027-92, Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23 Nuclear Safety Analysis Report

DOE Fire Protection Website

ES&H Standard 1.4.0, Compressed Gas Cylinder Safety

ES&H Standard 1.4.1, Pressurized Systems for Experimental Use

ES&H Standard 1.4.2, Glass and Plastic Window Design for Pressure Vessels

ES&H Standard 1.5.0, Electrical Safety

ES&H Standard 1.5.1, Lockout/Tagout Requirements

ES&H Standard 1.5.2, Design Criteria for Electrical Equipment

ES&H Standard 1.5.3, Interlock Safety for Protection of Personnel

ES&H Standard 1.14.0, Identification of Piping Systems

ES&H Standard 2.3.2, RF and Microwaves

ES&H Standard 4.0.0, Fire Safety Program

ES&H Standard 4.1.2, Means-of-Egress (Exits)

ES&H Standard 4.10.2, Flammable Liquids: Storage, Use, & Disposal

ES&H Standard 4.11.0, Installation of Flammable Gas Systems (Experimental and Temporary Installations)

ES&H Standard 4.12.0, Special Precautions for Locations Containing Flammable Atmospheres

ES&H Standard 4.12.1, Refrigerators for Flammable Liquid Storage

ES&H Standard 5.1.0, Nonflammable Cryogenic Liquids

ES&H Standard 5.2.0, Flammable Cryogenic Liquids

Environmental Assessments Subject Area

Exhaust Ventilation Subject Area

Facility Authorization Basis Program Description

Facility Hazard Categorization Subject Area

Facility Use Agreements Subject Area

Laser Safety Subject Area

Lifting Safety Subject Area

National Environmental Policy Act (NEPA) and Cultural Resources Evaluations Subject Area

Operational Readiness Evaluation (ORE) Subject Area

Oxygen Deficiency Hazards (ODH), System Classification and Controls Subject Area

Process Assessment Subject Area

Radiological Control Manual Program Description

Records Management Subject Area

Respiratory Protection Subject Area

Sealed Radioactive Source Control Subject Area

Storage and Transfer of Hazardous and Nonhazardous Materials Subject Area

Traffic Safety Subject Area

Work Planning and Control for Experiments and Operations Subject Area

Working With Chemicals Subject Area

Standards of Performance

Managers shall manage work to control risks and hazards, ensure customer satisfaction, and provide a benefit to BNL.

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.

Management System

This subject area belongs to the **Facility Safety** management system.

Back to Top

1.8-082004-/standard/2m/2m00t011.htm

SBMS

Forms | Contact List | SBMS Instructions | Help Desk

Find Subject Areas: Index | Categories | Alpha

Show Side Menu

Search Subject Areas & Legacy Documents:

Introduction: Hazard Analysis

Effective Date: **March 2001**

Point of Contact: Hazard Analysis Subject Matter Expert

The purpose of this subject area is to ensure that facilities categorized as radiological or industrial have the appropriate authorization basis to perform their missions. See the Facility Hazard Categorization Subject Area for more information on hazard categorization, and see the Facility Authorization Basis Program Description for information on the Laboratory's overall program. Either the authorization basis is determined by a "technical hazard analysis," or the facility is deemed adequately covered by Laboratory standard hazard control programs that are designed to handle routine hazards. The Facility Use Agreement (FUA) becomes the vehicle for and documentation of the authorization basis. See the Facility Use Agreement Subject Area for more information. Refer to the Hazard Analysis Flowchart for an overview of this subject area.

Three important functions are covered within this subject area to support this purpose. First, the subject area provides a "hazard screening" process, which is applied to facilities and proposed modifications to determine the need for and extent of follow-on safety analysis. Second, this subject area assists the line management in choosing the proper and most efficient hazard analysis technique to use when the need is identified, and how to document that analysis appropriately. Third, based on the technical safety analysis, this subject area also identifies controls and/or safety limits that need to be included in the FUA. The FUA then becomes the authorization basis for the facility.

By using this graded approach, more detailed safety documentation can be prepared for the facilities and modifications that fall into relatively higher hazard groups. Likewise, a larger proportion of resources in the safety documentation area can be applied to the larger magnitude hazards. The routine hazards, covered under Laboratory standard hazard control programs, are also formally documented in the FUA as not needing additional technical hazard analysis.

Back to Top

1.0-032001/standard/2m/2m00i011.htm

Send a question or comment to the SBMS Help Desk
Disclaimer

Subject Area: ***Hazard Analysis***

1. Determining the Hazard Rating

Effective Date: **March 2001**
Point of Contact: Hazard Analysis Subject Matter Expert

Applicability

This information applies to staff evaluating a facility and modifications to determine the level of necessary safety analysis to ensure the proper authorization basis. It applies to those facilities designated as industrial or radiological.

Required Procedure

Department Chairs/Division Managers ensure that their facilities and modifications are properly evaluated to determine if the hazards involved require additional hazards analysis beyond that covered by the Laboratory's basic hazards control programs and/or the Work Planning and Control for Experiments and Operations Subject Area. Those facilities or modifications completely covered by the Laboratory's basic hazard control programs would be exempted from the requirements of the Hazard Analysis Subject Area. This subject area will help to screen those facilities that need additional hazards analysis due to a greater level of risk and provide guidance as to the type of hazards analysis recommended. Staff who plan work that could challenge the facility hazard category contact the Facility Hazard Category Subject Matter Expert and follow the Facility Hazard Categorization Subject Area.

Staff involved in facilities or modifications that involve either federal funding, or use of federal facilities, federal lands, or capital equipment must ensure that a National Environmental Policy Act (NEPA)/Cultural Resources review is conducted before starting work. For more information, see the National Environmental Policy Act (NEPA) and Cultural Resources Evaluations Subject Area.

Step 1	The Department Chair/Division Manager or designee determines if the project or facility (activity) is covered by an existing authorization basis of an accelerator or nuclear facility. For more information, refer to the Facility Hazard Categorization Subject Area. If so, further action is not required by this subject area. If not, proceed to the next step.
Step 2	The Department Chair/Division Manager or designee uses the BNL Hazard

	Identification Tool, answering the questions as they relate to the facility being evaluated. **Note:** This tool is designed to assist the analyst in identifying the hazards associated with each activity to determine the level of hazard analysis required. The tool is used by answering seventeen sets of questions. If "No" is answered to the highest level question in a set, the more detailed questions will not appear; thus, there is no need to answer them.
Step 3	The Department Chair/Division Manager or designee runs the report at the end of the BNL Hazard Identification Tool. Based on answers to the questions, the tool calculates a "hazard rating" of 0, 1, 2, or 3. This rating relates to the potential severity of hazards (with 3 the highest) in an activity before quantities, likelihood, or particular circumstances are taken into account (unmitigated hazard level). If the result is a hazard rating of 0 or 1, no additional safety analysis is necessary. A hazard rating of 0 or 1 is adequately covered by the Laboratory's basic hazards control programs and is exempted from this subject area. **Note:** The Department/Division must document the results.
Step 4	The responsible Line Management, in conjunction with the Hazard Analysis Subject Matter Expert and/or Facility Support Representative, verify and concur with the results of the hazard rating. **Note:** If concurrence can not be obtained, the tool should be rerun, with additional input from the Hazard Analysis Subject Matter Expert and Facility Support Representative. The Department/Division must document the results.
Step 6	For a rating of 2 or 3, the Department Chair/Division Manager or designee contacts the Hazard Analysis Subject Matter Expert to verify the rating and collectively answer the additional risk screening questions in the exhibit on the Risk Screening Matrix Questions. **Note:** If the result is a hazard rating of 3, detailed safety analysis is required. **Note:** If the result is a hazard rating of 2, documented safety analysis may be necessary, depending on the results of the additional screening questions.
Step 7	For activities with a hazard rating of 2, the Hazard Analysis Subject Matter Expert, in conjunction with the Line Management, determine if further analysis is required based on the level of risk. **Note:** Should a rating of 2 be determined not to need further analysis, the Department/Division must document this fact.
Step 8	If the hazard identification tool results in a hazard rating of 3 or a 2 that was determined in step 7 to need further analysis, proceed to the section on Determining the Type of Hazard Analysis.

References

References

BNL Hazard Identification Tool

Facility Hazard Categorization Subject Area

National Environmental Policy Act (NEPA) and Cultural Resources Evaluations Subject Area

Work Planning and Control for Experiments and Operations Subject Area

| Continue to Next Page |

Back to Top

Subject Area: ***Hazard Analysis***

2. Determining the Type of Hazard Analysis

Effective Date: **March 2001**
Point of Contact: Hazard Analysis Subject Matter Expert

Applicability

This information applies to staff conducting a hazard analysis for a facility and modifications to support the authorization basis for the activity. It applies to those facilities designated as industrial or radiological.

Required Procedure

Department Chairs/Division Managers ensure that their facilities and modifications are properly evaluated using the appropriate hazard analysis techniques. This subject area provides guidance as to the types of hazard analysis techniques available and when they may be used for particular types of hazards.

Step 1	The Department Chair/Division Manager or designee uses the BNL Hazard Identification Tool to compile a list of hazards from the questions that were answered "yes" (See step 3 of the section on Determining the Hazard Rating.)
Step 2	The Department Chair/Division Manager or designee determines the appropriate hazard analysis and obtains concurrence from the Line Manager. See the exhibit on the Hazard Analysis and Review Matrix for more information.
Step 3	The Line Manager, in conjunction with the Hazard Analysis Subject Matter Expert, determines the schedule and level of authorization, and documents that in the Authorization Plan Memorandum.
Step 4	The Line Manager obtains concurrence of the Authorization Plan Memorandum from the appropriate Associate Laboratory Director (ALD).
Step 5	The responsible ALD submits the Authorization Plan Memorandum to the Deputy Director for Operations (DDO).
Step 6	The DDO concurs by signing the Authorization Plan Memorandum for all activities with a hazard rating of 3. For activities with a hazard rating of 2, the

	DDO may delegate that responsibility to the appropriate line management. If there is potential for off-site impact, as identified by the results from the risk questions in the section on Determining the Hazard Rating, Line Management follows the Community Involvement in Laboratory Decision-Making Subject Area using the exhibit Checklist for Identifying Issues/Decisions That May Require Community Involvement. The DDO forwards a copy of the Authorization Plan Memorandum to the Brookhaven Site Office (BHSO) for feedback and concurrence. **Note:** The DDO may require additional review for concurrence from Laboratory-level committees. The Laboratory Environment, Safety and Health Committee must then review and concur with the complete analysis.
Step 7	The BHSO forwards its comments on off-site impact to the DDO, who submits them to the Line Manager.
Step 8	The Line Manager forwards the comments to the Department Chair/Division Manager or designee, who modifies the Authorization Plan Memorandum, incorporating the comments, if any.
Step 9	The Department Chair/Division Manager or designee submits the revised Authorization Plan Memorandum to the DDO for concurrence.

References

BNL Hazard Identification Tool

Community Involvement in Laboratory Decision-Making Subject Area

| Go to Previous Page | Continue to Next Page |

Back to Top

1.8-082004/standard/2m/2m02d011.htm

Subject Area: ***Hazard Analysis***

3. Conducting and Documenting the Hazard Analysis

Effective Date: **March 2001**

Point of Contact: Hazard Analysis Subject Matter Expert

Applicability

This information applies to staff conducting and documenting a hazard analysis for a facility and modifications to support the authorization basis for the activity. It applies to those facilities designated as industrial or radiological.

Required Procedure

Department Chairs/Division Managers ensure that their facilities are properly evaluated using the proper hazard analysis techniques. The analysis must be conducted by qualified staff and documented in accordance with this section.

Step 1	The Department Chair/Division Manager or designee conducts the analyses agreed to in the Authorization Plan Memorandum. **Note:** If necessary, contact the appropriate Subject Matter Experts for guidance and assistance in conducting the analysis.
Step 2	The Department Chair/Division Manager or designee ensures that appropriate subject matter experts review the completed analysis. The review may include off-site experts. See the exhibit on the Hazard Analysis and Review Matrix for more information.
Step 3	The Department Chair/Division Manager or designee sends an analysis with a hazard level of 3 to the designated Laboratory-Level Committee, such as the Electrical Safety Committee, and then to the Laboratory Environment, Safety & Health Committee for review, as agreed to in the Authorization Plan Memorandum.
Step 4	The Department Chair/Division Manager or designee addresses all comments from the designated committees.

	from the designated committees.
Step 5	The Department Chair/Division Manager or designee places the analysis in a Departmental/Divisional change control system.
Step 6	The Department Chair/Division Manager or designee ensures that the analysis is retained in accordance with the Records Management Subject Area.

References

Records Management Subject Area

| Go to Previous Page | Continue to Next Page |

Back to Top

1.5-042004/standard/2m/2m03d011.htm

Subject Area: ***Hazard Analysis***

4. Developing Operational Safety Limits (OSLs)

Effective Date: **March 2001**
Point of Contact: Hazard Analysis Subject Matter Expert

Applicability

This information applies to staff who develop Operational Safety Limits (OSLs) for a facility and modifications to support the authorization basis for the activity. It applies to those facilities designated as industrial or radiological.

Required Procedure

Operational Safety Limits (OSLs) are auditable boundaries of operation that are not to be exceeded during normal operations to ensure safety. The OSLs define the conditions, safe boundaries, and administrative controls necessary to ensure that a boundary of safe operation is established for the facility and modifications and that it is operated within those boundaries. Operations within the requirements of the OSL are intended to prevent unacceptable events, i.e., accidents, system failure, or exposure to radiation or toxic substances. These limits can range from very broad to specific and must be applied individually to facilities or operations.

Step 1	The Department Chair/Division Manager or designee reviews the hazard analysis to determine the appropriate Operational Safety Limits (OSLs), which includes three general areas: • **Design Features.** Design features are components, systems, or other engineered features (e.g., shielding), which are intended to maintain the facility within the boundaries established by the hazard analysis. A margin of safety is usually built in design features. This would be analogous to designing the burst pressure of a boiler to a 500 psi (a 5:1 margin of safety over the working pressure of 100 psi). Another example is the pressure relief valve installed on a boiler to ensure that pressures did not raise above a certain value. • **Safety Limits.** A safety limit is a parameter placed on observable and measurable variables that directly relates to performance and integrity of

<table>
<tr><td></td><td>
measurable variables that directly relates to performance and integrity of the operation. If the value of the variable were to reach this limit, no impact to the health and safety of personnel and no permanent damage to equipment would occur. However, operation above a safety limit would not be permitted since the margin of safety would be reduced to an unacceptable level. An example would be a safety limit of 120 psi for a boiler that normally operates at 100 psi.

Typically, there would also be a set point below the safety limit where normal operations would take place. This set point provides sufficient margin for alarms and for corrective action by automatic protective action controls, before the safety limit is reached. For example, this set point can be accomplished with the thermostatic control for a boiler.

• Administrative Controls. Administrative controls are used in addition to design features and safety limits to augment the control of the hazard. Typically, these are additional requirements imposed by the facility to ensure that the operation is maintained within the conditions of the hazard analysis. These may also include
 ○ Minimum staffing requirements,
 ○ Minimum training requirements, and
 ○ Verification program for status and configurations of critical components and systems.

Caution must be exercised when defining the scope of the limits so that operations are not unnecessarily constrained and that OSLs are not exceeded.
</td></tr>
<tr><td>Step 2</td><td>
The Department Chair/Division Manager or designee, in conjunction with the appropriate Department/Division Building Manager, completes an FUA Change Analysis Basis Document to incorporate or link the OSLs into the appropriate FUA. Refer to the Facility Use Agreements Subject Area for information on change control of FUAs.

Note: For facilities without an existing FUA, the DDO approves the OSLs by memo.

Note: Before permission to operate, the OSLs must be incorporated in the FUA.
</td></tr>
<tr><td>Step 3</td><td>
The Department Chair/Division Manager or designee reviews OSLs when significant changes that affect the OSLs are planned, and/or periodically, not exceeding 3 years, and if appropriate, modifies the hazard analysis. The results of this review must be documented by the Department/Division.
</td></tr>
<tr><td>Step 4</td><td>
The Department Chair/Division Manager or designee schedules an Occupational Readiness Evaluation (ORE) before authorization or startup of the facility or modifications. See the Operational Readiness Evaluation (ORE) Subject Area for information on conducting an ORE.
</td></tr>
</table>

References

Facility Use Agreements Subject Area

Operational Readiness Evaluation (ORE) Subject Area

| Go to Previous Page |

Back to Top

1.0-032001/standard/2m/2m04d011.htm

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.

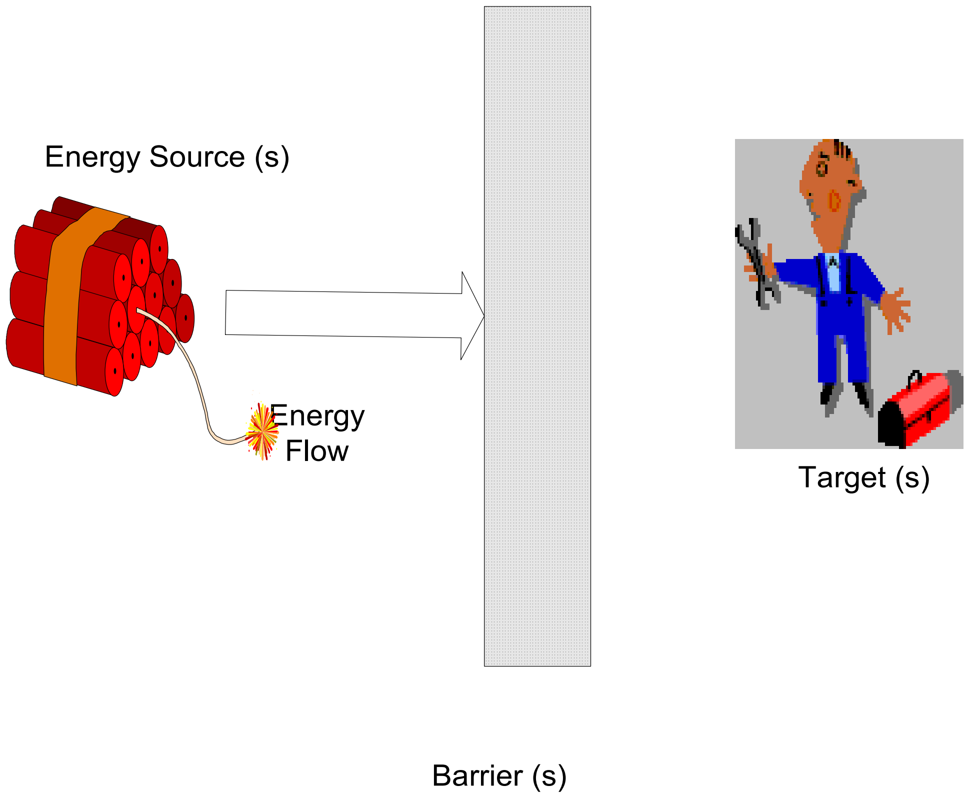


Figure 1.

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: **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)**

Target (s) **Contractor Foreman, Painter A and Painter B.**

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.

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.

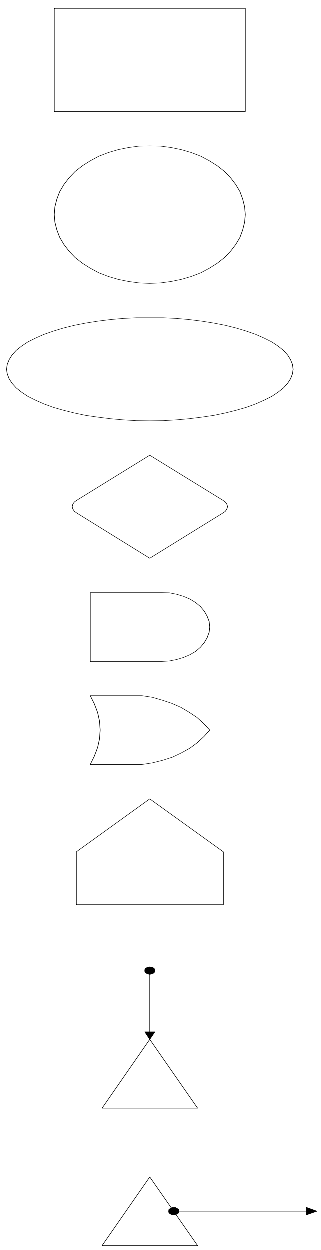
5. Evaluate fault tree probability.

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).

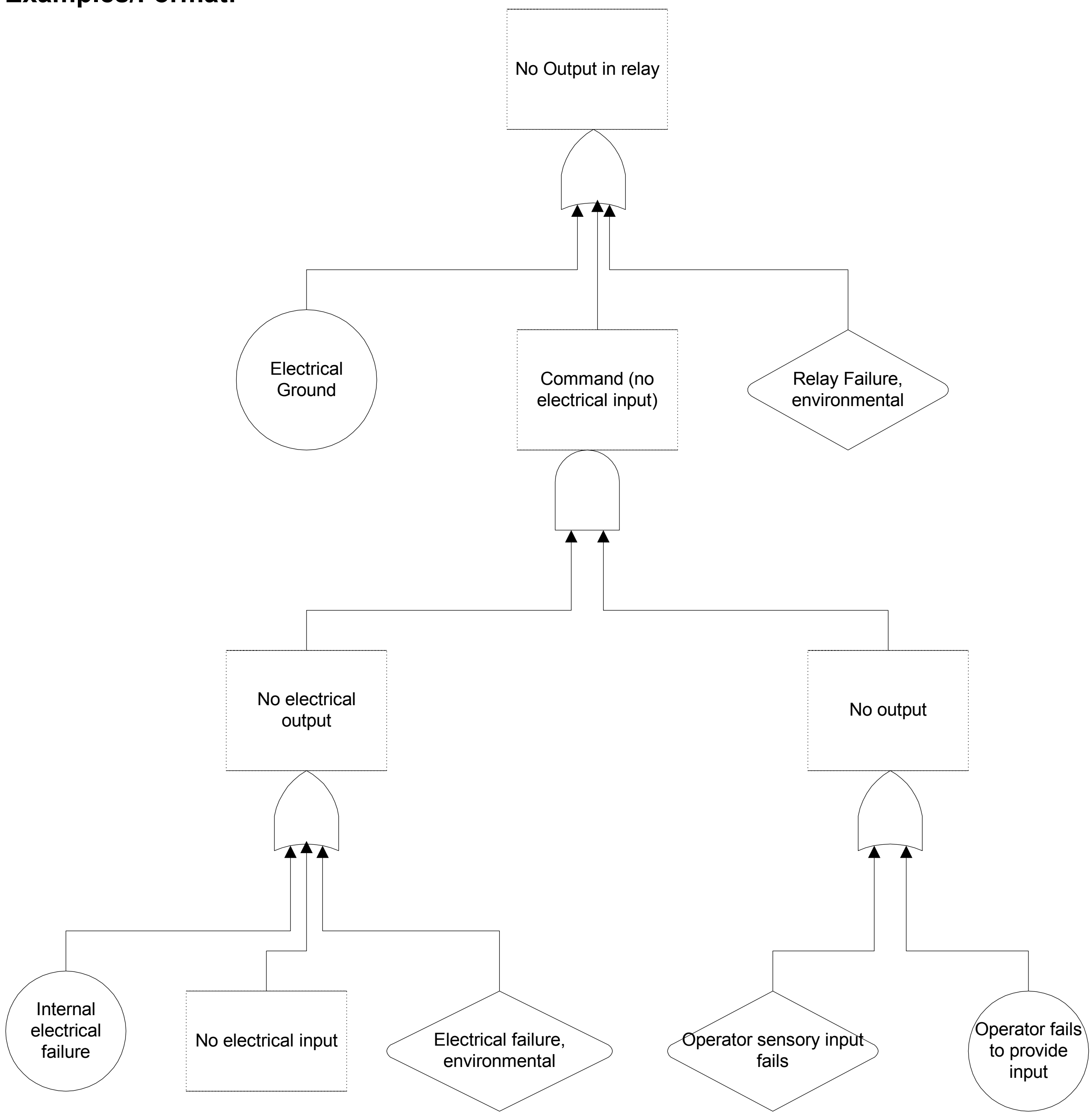
Hammer, Willie, "Occupational Safety Management and Engineering," Prentice-Hall, 1981 (pp.468-475).

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:



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.

Failure Modes and Effects Analysis (FMEA)

Purpose:

The purpose of the Failure Modes and Effects Analysis (FMEA) is to determine the results or effects of all sub-element failures on a system operation and to classify each potential failure according to its severity.

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:

To conduct a FMEA first examine the system, element by element. Identify modes in which each element can fail. Determine the effect(s) upon the system of each failure mode, taken both singly and in combination with others. The following steps should be performed:

1. Identify all major components, functions, and processes.
2. Determine the consequences of failure that would be unacceptable.
3. Determine the location, maintenance, and transportation mechanisms of all hazardous materials.
4. Determine the potential failure modes (that would result in the unacceptable consequences).
5. Specify the effects (impact) of the failures of the system.
6. Identify provisions to control hazards and failures.
7. Identify detection methods for failures.
8. Establish importance of each event, i.e., "insignificant" to "catastrophic." A quantitative expression, such as [P(probability)] x [C(consequences)] = R (risk) may be used.

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.

Resources/Skills Required:

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

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. However, over the FTA, 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 hardware 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.

Examples/Format:

Example 1. (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:	Failure Effect:	Redundancy:
			Risk:		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 fields 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.

Component #:	Nomenclature:	Function:	Failure Position:	Failure Effect:	Redundancy:
			Risk:		Comments:
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		
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		

Subject Area: ***Hazard Analysis***

Guidance on Fire Hazard Analysis

Effective Date: **March 2001**
Point of Contact: Hazard Analysis Subject Matter Expert

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 fulfills the requirement for a determination of a facility's fire risk.

In the applicable DOE Order (DOE Order 420.1), the FHA is required for all nuclear facilities, significant new facilities, and facilities that represent unique or significant fire safety risks. Furthermore, the FHA must be developed using a graded approach; the conclusions are incorporated in the Safety Analysis Report (SAR) or Safety Analysis Document (SAD) accident analysis sections. The logical extension is that the criteria are then integrated into design basis and beyond design basis accident conditions.

See the DOE Fire Protection Website for guidance on developing a fire hazard analysis.

Back to Top

1.0-032001/standard/2m/2m13e011.htm

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.

Radiological Shielding Analysis

Pending the availability of site-specific guidance on the requirements for a radiological shielding analysis, it is expected that such analyses would be based on the use of commercial or widely accepted public domain software packages, such as

Microshield
CASIM
MCNP
LAHET
EGS

Individuals conducting the analysis must have demonstrated expertise in the particular program chosen. For further information, contact the Radiological Engineering Group.

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/EH-Draft, "Preliminary Guide for Conformance with OSHA's Rule for Process Safety Management of Highly Hazardous Chemicals," March 1993.

Department of Energy, DOE/EH-Draft, "Guide for Chemical Process Hazard Analysis," March 1993.

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	

Subject Area: ***Hazard Analysis***

Hazard Analysis and Review Matrix (HARM)

Effective Date: **March 2001**
Point of Contact: Hazard Analysis Subject Matter Expert

A Preliminary 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 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 Fire Hazard Analysis,
- Guidance on Fault Tree Analysis,
- Guidance on Failure Modes and Effects Analysis,
- Guidance on Preliminary Hazard Analysis,
- Guidance on Radiological Shielding 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 Program Subject Area for guidance on an ALARA Analysis.

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

		Change Analysis	
Chemical	Working with Chemicals Subject Area, Respiratory Protection 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	ES&H Standard 5.1.0, Nonflammable Cryogenic Liquids, ES&H Standard 5.2.0, Flammable Cryogenic Liquids	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 Factor; Equipment Failure Rate Estimates; Fatality Rate Determination; and Oxygen Concentration in Ventilated Spaces.	SME, Laboratory Environmental Safety and Health Committee
	ES&H Standard 1.5.0, Electrical Safety, ES&H Standard 1.5.1, Lockout/Tagout Requirements, ES&H		SME, Laboratory

Electrical	Requirements, ES&H Standard 1.5.2, Design Criteria for Electrical Equipment, ES&H Standard 1.5.3, Interlock Safety for Protection of Personnel	Failure Modes and Effect Analysis	SME, Laboratory Electrical Safety Committee
Environmental	Environmental Assessments Subject Area, Process Assessment Subject Area, National Environmental Policy Act (NEPA) and Cultural Resources Evaluations Subject Area	What-if Analysis, Job Safety Analysis, NPH	SME
Explosives		What-if Analysis, Barrier Analysis, Failure Modes and Effects Analysis	SME, Laboratory Laboratory Environmental Safety and Health Committee
Extremely Hazardous Materials	Working with Chemicals Subject Area, Bloodborne Pathogens Subject Area, Exhaust Ventilation Subject Area	NPH, Barrier Analysis, Change Analysis	SME
Fire	ES&H Standard 4.0.0, Fire Safety Program, ES&H Standard 4.1.2, Means-of-Egress (Exits), ES&H Standard 4.10.2, Flammable Liquids: Storage, Use, & Disposal, ES&H Standard 4.11.0, Installation of Flammable Gas Systems (Experimental and Temporary Installations), ES&H Standard 4.12.0, Special Precautions for Locations	FHA, Life Safety Code, Change Analysis	SME

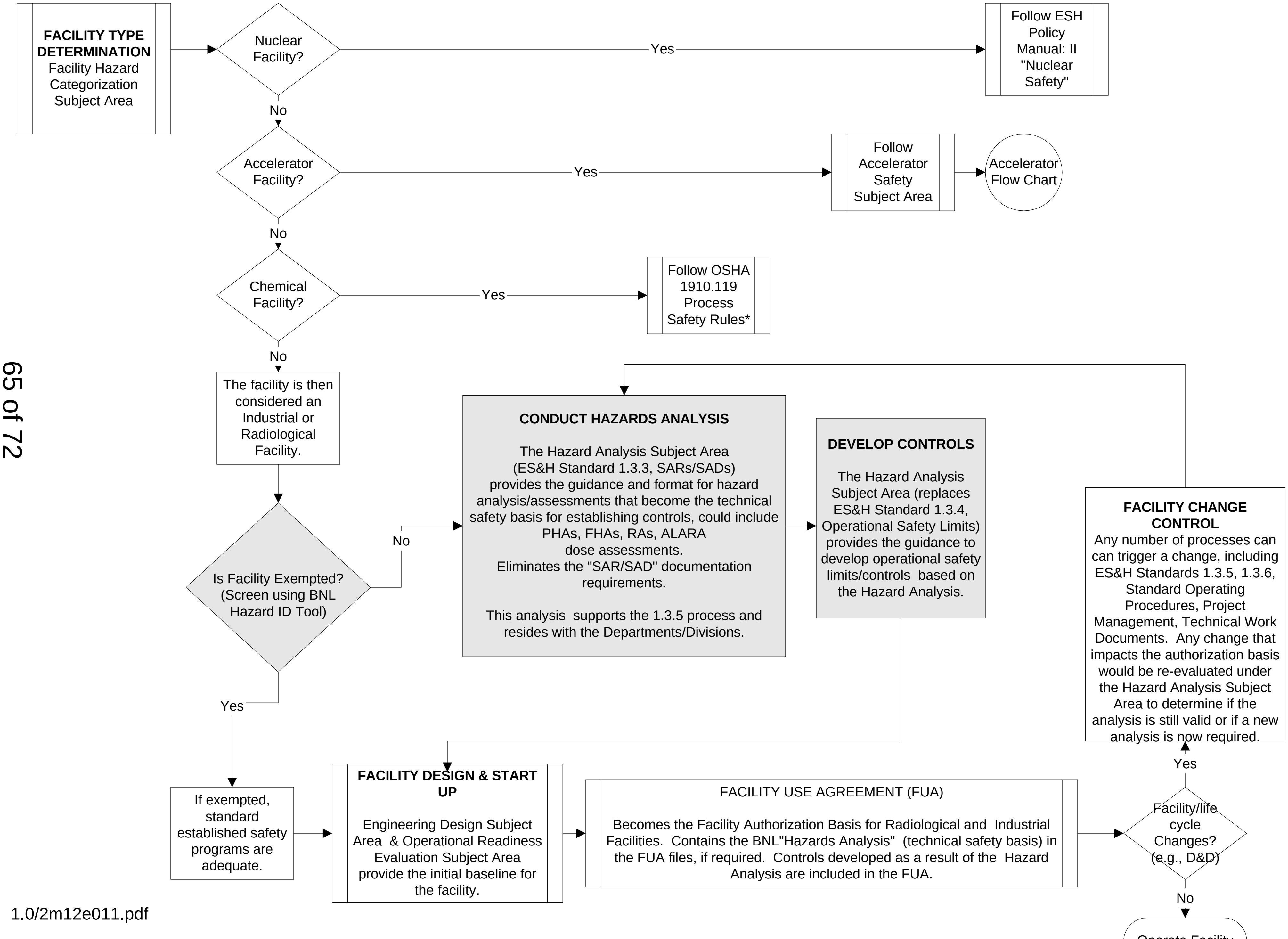
	Containing Flammable Atmospheres, ES&H Standard 4.12.1, Refrigerators for Flammable Liquid Storage		
Firearms		What-if Analysis, Barrier Analysis	SME, Firearms Safety Committee
Human Subjects		What-if Analysis	SME, Institutional Review Board, Radioactive Drug Review Board
Laser	Laser Safety Subject Area	Failure Modes and Effects Analysis (interlock)	SME, Laser Safety Committee, Laboratory Environment, Safety & Health Committee
Magnetic Fields/ Microwave	ES&H Standard 2.3.2, RF and Microwaves	What-if, Job Safety Analysis	SME
Radiological	Radiological Control Manual Program Description, ALARA Program 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
Special Equipment not Normally Used Onsite	Lifting Safety Subject Area	What-if Analysis, Barrier Analysis, Change Analysis	SME, Laboratory Environment, Safety & Health Committee
Stored Energy/ Mechanical Equipment/ Pressure/Vacuum	ES&H Standard 1.4.0, Compressed Gas Cylinder Safety, ES&H Standard 1.4.1, Pressurized Systems for Experimental Use, ES&H Standard 1.4.2, Glass and Plastic Window Design for Pressure Vessels	What-if Analysis, Barrier Analysis Failure Modes and Effects Analysis, Change Analysis, Job Safety Analysis	SME
Thermal	ES&H Standard 1.14.0, Identification of Piping Systems	What-if Analysis, Barrier Analysis, Job Safety Analysis	SME
	Facility Hazard		

Transportation (Radiological or Hazardous Material On-site or Off-site)	Categorization Subject Area, Sealed Radioactive Source Control Subject Area, Storage and Transfer of Hazardous and Nonhazardous Waste Materials Subject Area, Traffic Safety Subject Area	What-if Analysis, Barrier Analysis	SME, Transportation Safety Officer, Traffic Safety Committee

Back to Top

1.8-082004/standard/2m/2m03e011.htm

Authorization Basis Flow



1.0/2m12e011.pdf

* BNL currently has no chemical facilities; if one were developed a whole new control methodology would need to be implemented before we could authorize use.

(03/2001)

Risk Screening Matrix Questions

CONSEQUENCE / PROBABILITY	**FREQUENT** Likely to occur repeatedly in life cycle	**PROBABLE** Likely to occur several times in life cycle	**OCCASIONAL** Likely to occur some time in life cycle	**REMOTE** Unlikely to occur in life cycle but possible	**EXT. REMOTE** Likelihood of occurrence ~ zero	**IMPOSSIBLE** Physically impossible to occur
Can a radiological or chemical hazard cause multiple deaths or serious injury, off-site evacuation, >100 rem to an individual, > $1,000,000 damage, > 4 mos. facility downtime, total loss of mission data, or have a public impact that closes the Department buildings or a User Facility?	HIGH RISK	HIGH RISK	HIGH RISK	MODERATE RISK	LOW RISK	ROUTINE RISK
Can a radiological or chemical hazard cause a death or serious injury, >25 rem to an individual, > $250,000 damage, 3 weeks to 4 months program downtime, severe loss of experimental data, or have a public impact that closes down an experiment or program?	HIGH RISK	HIGH RISK	MODERATE RISK	LOW RISK	LOW RISK	ROUTINE RISK
Can a radiological or chemical hazard cause multiple moderate injuries, local evacuation, > 5 rem to an individual, > $50,000 damage, 4 days to 3 weeks program downtime, major loss of experimental data, or have a public impact that brings the experiment to the attention of the community and activist groups?	MODERATE RISK	MODERATE RISK	LOW RISK	LOW RISK	ROUTINE RISK	ROUTINE RISK
Can a radiological or chemical hazard cause minor injuries, no on-site or off-site evacuation, < 2 rem to an individual, < than $50,000 damage, < 4 days program downtime, minor loss of experimental data, or have a public impact that is below public perception?	ROUTINE RISK	ROUTINE RISK	ROUTINE RISK	ROUTINE RISK	ROUTINE RISK	ROUTINE RISK

Key*
High Risk = 3
Moderate Risk = 2
Low Risk = 1
Routine Risk = 0

*Hazard Rating Results from Hazard Identification Tool.

SBMS

Forms | Contact List | SBMS Instructions | Help Desk

Find Subject Areas: Index | Categories | Alpha

Show Side Menu

Search Subject Areas & Legacy Documents:

Subject Area: ***Hazard Analysis***

Authorization Plan Memorandum

Effective Date: **March 2001**

Point of Contact: Hazard Analysis Subject Matter Expert

The Authorization Plan Memorandum is provided as a Word file.

Back to Top

The only official copy of this file is the one online in SBMS. Before using a printed copy, verify that it is the most current version by checking the document effective date on the BNL SBMS website.

1.6-052004/standard/2m/2m02e011.htm

Send a question or comment to the SBMS Help Desk

Disclaimer

Managed by Brookhaven Science Associates
for the U.S. Department of Energy

BROOKHAVEN NATIONAL LABORATORY

Memo

date: ***(enter date)***

to: *M. Bebon, Deputy Director for Operations*

from: ***(Organization Associate Laboratory Director)***

subject: *Authorization Plan for (**Identify Activity or Project**)*

As required by the Hazard Analysis Subject Area, this memorandum forms the basis for agreement on the necessary hazard analysis, schedule, and authorization for the following activity:

Activity/Project:	
Location: (Drawing Number/Building Number):	
Responsible Department/Division:	
Date of Evaluation:	
Result of Evaluation - Hazard Analysis Rating 2 or 3:	

The following hazards analysis have been identified as appropriate to document the authorization of this activity and establish necessary operational limits:

	Y	N	Comments (principal hazards)
ALARA Analysis	☐	☐	
Barrier Analysis	☐	☐	
Change Analysis	☐	☐	
Energy Trace Barrier Analysis	☐	☐	
Failure Modes and Effects Analysis (FMEA)	☐	☐	
Fault Tree Analysis (FTA)	☐	☐	
Fire Hazards Analysis (FHA)	☐	☐	
HAZOP	☐	☐	
Job Safety Analysis (JSA)	☐	☐	
Natural Phenomena Hazards Analysis	☐	☐	
Preliminary Hazard Analysis (PHA)	☐	☐	
Shielding Analysis	☐	☐	
What-If Analysis	☐	☐	
Other(s) (specify)	☐	☐	

The analysis will be completed and necessary changes made to the Facility Use Agreement (FUA), as appropriate by (insert date)____________________.

This activity may affect the existing hazard categorization of the facility in which it resides Y/N. If yes, the Facility Hazard Categorization Subject Matter Expert must concur and the Facility Hazard Categorization Subject Area must be followed.

Required independent reviewers/committees: ______________________________.

Authorization Signatures

Hazard Analysis Subject Matter Expert
____________________________ Date: ______________

Facility Hazard Categorization Subject Matter Expert (Concurrence if activity impacts existing Hazard Categorization)
____________________________ Date: ______________

Department Chair/Division Manager (Concurrence for Hazard Rating 2 or 3)
____________________________ Date: ______________

Deputy Director for Operations (Concurrence for Hazard Rating 3)
____________________________ Date: ______________

Brookhaven Group Office Representative (Concurrence for any activity with off-site impact)
____________________________ Date: ______________

* Retain in Department/Division file

Cc: Organization Manager
Department of Energy (DOE) Brookhaven Group Office (BHG) Representative
Hazard Analysis Subject Matter Expert
Facility Hazard Categorization Subject Matter Expert

Definitions: Hazard Analysis

Effective Date: **March 2001**
Point of Contact: Hazard Analysis Subject Matter Expert

Term	Definition
authorization basis	The set of documents or requirements upon which a decision is made by BSA and/or DOE whether to authorize the commencement or continuation of activities. This typically includes safety documentation (Safety Assessment Document or Safety Analysis Report, technical hazard analysis), established Operational Safety Limits (safety envelope, readiness review) and is determined by the type of facility/operation.
Facility Use Agreement (FUA)	A landlord-tenant contract that must be established between Plant Engineering and each facility to define the capabilities and processes that are in place within a facility and to ensure that the identified hazards are controlled within the confines of the facility or immediate work area.
hazard rating	The determination, as made by the use of the Hazard Identification Tool, of a numerical value (0,1, 2, or 3) related to the potential severity (with '3' being highest) of hazards in an operation before mitigation is considered. Hazard rating is only applicable to industrial or radiological facilities.
hazard screening	The determination, as made by guidance from the Facility Hazard Categorization Subject Area, for proper categorization of a facility/project/activity. It should result in either a categorization of Nuclear Facility, Accelerator Facility, Chemical Hazard facility, Radiological Facility, or Industrial Facility.
industrial facility	A facility with no radiological inventory 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 routine hazards such as electrical, pressure.
Operational Safety Limits (OSL)	These are auditable boundaries of operation, which are not to be exceeded during normal operations to ensure safety. The OSLs define the conditions, safe boundaries, and administrative controls necessary to ensure that a facility is operated within the guideline

	defined.
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 probability of occurrence and severity of consequence.
safety documentation	That body of written and retained material prepared by the user organization (or their agents), which identifies and categorizes hazards by severity and probability of occurrence, provides for mitigation of these hazards by elimination or control, documents the boundaries that an operation can run within, and to a depth and breadth commensurate with the overall risk, and required level of review and approval. This body of information forms the authorization basis for the facility.
technical hazard analysis (THA)	The rollup of completed and documented specific analytical method (s) used to assess the level of hazard associated with a given facility, including as a minimum, the Preliminary Hazard Analysis (PHA) and any supplemental types of analyses, as called out in the Authorization Plan Memorandum. The THA becomes the technical basis for establishing controls for radiological and industrial facilities in the form of operational safety limits.

Back to Top

Revision History: Hazard Analysis

Point of Contact: Hazard Analysis Subject Matter Expert

Revision History of this Subject Area

Date	Description	Management System
August 2004 -- Minor 1.8	References to ES&H Standard 1.9.0, Traffic Safety were replaced by the Traffic Safety Subject Area.	Facility Safety
March 2001	This subject area describes the procedures and guidelines for ensuring that facilities categorized as radiological or industrial have the appropriate authorization basis to perform their missions. The subject area provides a "hazard screening" process, which is applied to facilities and proposed modifications according to the magnitude of their hazards to determine the need for and extent of follow-on safety analysis. It assists the line management in choosing the proper and most efficient hazard analysis technique to use when the need is identified, and describes how to document that analysis appropriately. Based on the technical safety analysis, this subject area also identifies controls and/or safety limits that need to be included in the Facility Use Agreement (FUA). The FUA then becomes the authorization basis for the facility. This subject area replaces ES&H Standards 1.3.3, Safety Analysis Reports/Safety Assessment Documents and 1.3.4, Operational Safety Limits.	Facility Safety

Back to Top

1.8-082004/standard/2m/2m00a011.htm