

Appendix F

ORM Details and Examples

1.0 HAZARD IDENTIFICATION TOOLS, DETAILS AND EXAMPLES

Chapter 15 summarizes the Operational Risk Management methodology. This Appendix provides examples of those tools, as they are applied to the ORM process:

- Hazard Identification
- Risk Assessment
- Risk Control Option Analysis
- Risk Control Decisions
- Risk Control Implementation
- Supervision and Review

1.1 PRIMARY HAZARD IDENTIFICATION TOOLS

The seven described in this appendix are considered the basic set of hazard identification tools to be applied on a day-to-day basis in organizations at all levels. These tools have been chosen for the following reasons:

They are simple to use, though they require some training.

They have been proven effective.

Widespread application has demonstrated they can and will be used by operators and will consistently be perceived as positive.

As a group, they complement each other, blending the intuitive and experiential with the more structured and rigorous.

They are well supported with worksheets and job aids.

In an organization with a mature ORM culture, the use of these tools by all personnel will be regarded as the natural course of events. The norm will be “Why would I even consider exposing myself and others to the risks of this activity before I have identified the hazards involved using the best procedures or designs available?” The following pages describe each tool using a standard format with models and examples.

1.1.1 THE OPERATIONS ANALYSIS AND FLOW DIAGRAM

FORMAL NAME: The Operations Analysis



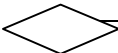
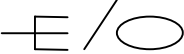

ALTERNATIVE NAMES: The flow diagram, flow chart, operation timeline

PURPOSE: The Operations Analysis (OA) provides an itemized sequence of events or a flow diagram depicting the major events of an operation. This assures that all elements of the operation are evaluated as potential sources of risk. This analysis overcomes a major weaknesses of traditional risk management, which tends to focus effort on one or two aspects of an operation that are intuitively identified as risky, often to the exclusion of other aspects that may actually be riskier. The Operations Analysis also guides the allocation of risk management resources over time as an operation unfolds event by event in a systematic manner.

APPLICATION: The Operations Analysis or flow diagram is used in nearly all risk management applications, including the most time-critical situations. It responds to the key risk management question “What am I facing here and from where can risk arise?”

METHOD: Whenever possible, the Operations Analysis is taken directly from the planning of the operation. It is difficult to imagine planning an operation without identifying the key events in a time sequence. If for some reason such a list is not available, the analyst creates it using the best available understanding of the operation. The best practice is to break down the operation into time-sequenced segments strongly related by tasks and activities. Normally, this is well above the detail of individual tasks. It may be appropriate to break down aspects of an operation that carry obviously higher risk into more detail than less risky areas. The product of an OA is a compilation of the major events of an operation in sequence, with or without time checks. An alternative to the Operations Analysis is the flow diagram. Commonly used symbols are provided at Figure 1.1.1A. Putting the steps of the process on index cards or sticky-back note paper allows the diagram to be rearranged without erasing and redrawing, thus encouraging contributions.

Figure 1.1.1A Example Flow Chart Symbols

SYMBOL	REPRESENTS	EXAMPLE
	START	RECEIVE TASKING BEGIN TRIP OPEN CHECKLIST
	ACTIVITY	OPERATION PLANNING START CAR STEP ONE IN CHECKLIST
	DECISION POINT (OR)	YES/NO APPROVE/DISAPPROVE PASS/FAIL
	FORK / SPLIT (AND)	PREPOSITION VEHICLES AND SUPPLIES RELEASE CLUTCH AND PRESS ACCELERATOR OBSERVE FLIGHT CONTROLS WHILE MOVING STICK
	END	FINAL REPORT ARRIVE AT DESTINATION AIRCRAFT ACCEPTED

RESOURCES: The key resource for the Operations Analysis are the operational planners. Using their operational layout will facilitate the integration of risk controls in the main operational plan and will eliminate the expenditure of duplicate resources on this aspect of hazard identification.

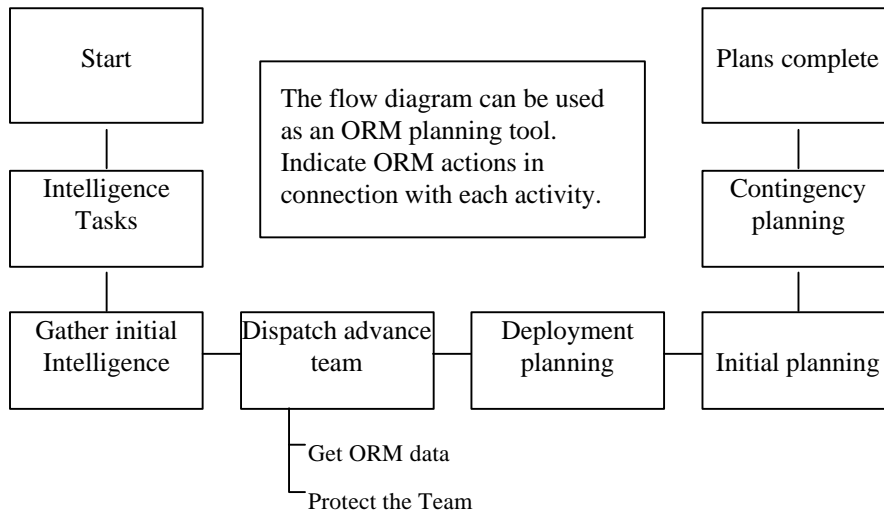
COMMENTS: Look back on your own experience. How many times have you been surprised or seen others surprised because they overlooked possible sources of problems? The OA is the key to minimizing this source of accidents.

THE PLANNING PHASE

- Initial Intelligence Received (Maps, Facility Lists, Environment, Etc.
- Advance Party Dispatched
- Advance Party Data Received
- Deployment Planning Underway
- Deployment Preparations Initiated
- Initial Operation Planning Underway
- Contingency Planning Underway

If more detail and more structured examination of the operational flow are desired, the flow diagram can be used. This diagram will add information through the use of graphic symbols. A flow diagram of the planning phase above might be developed as illustrated in Figure 1.1.1B below.

Figure 1.1.1B Example Flow Diagram



1.1.2 THE PRELIMINARY HAZARD ANALYSIS

FORMAL NAME: Preliminary Hazard Analysis

ALTERNATIVE NAMES: The PHA, the PHL

PURPOSE: 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 deep. The key idea of the PHA is to consider the risk inherent to every aspect of an operation. The PHA helps overcome the tendency to focus immediately on risk in one aspect of an operation, sometimes at the expense of overlooking more serious issues elsewhere in the operation. The PHA will often serve as the hazard identification process when risk is low or routine. In higher risk operations, it serves to focus and prioritize follow-on hazard analyses by displaying the full range of risk issues.

APPLICATION: The PHA is used in nearly all risk management applications except the most time-critical. Its broad scope is an excellent guide to the identification of issues that may require more detailed hazard identification tools.

METHOD: The PHA is usually based on the Operations Analysis or flow diagram, taking each event in turn from it. Analysts apply their experience and intuition, use reference publications and standards of various kinds, and consult with personnel who may have useful input. The extent of the effort is dictated by resource and time limitations, and by the estimate of the degree of overall risk inherent in the operation. Hazards that are detected are often listed directly on a copy of the Operations Analysis as shown at Figure 1.1.2A. Alternatively, a more formal PHA format such as the worksheet shown at Figure 1.1.2B can be used. Operations Analysis. The completed PHA is used to identify hazards requiring more in-depth hazard identification or it may lead directly to the remaining five steps of the ORM process, if

hazard levels are judged to be low. Key to the effectiveness of the PHA is assuring that all events of the operation are covered.

Figure 1.1.2A Building the PHA directly From the Operations Analysis Flow Diagram

Operational Phase	Hazards
List the operational phases vertically down the page. Be sure to leave plenty of space on the worksheet between each phase to allow several hazards to be noted	List the hazards noted for each operational phase here. Strive for detail within the limits imposed by the time you have set aside for this tool.

RESOURCES: The two key resources for the PHA are the expertise of personnel actually experienced in the operation and the body of regulations, standards, and instructions that may be available. The PHA can be accomplished in small groups to broaden the List the operational phases vertically down the page. Be sure to leave plenty of space on the worksheet between each phase to allow several hazards to be noted for each phase. List the hazards noted for each operational phase. Strive for detail within the limits imposed by time. A copy of a PHA accomplished for an earlier similar operation would aid in the process.

COMMENTS: The PHA is relatively easy to use and takes little time. Its significant power to impact risk arises from the forced consideration of risk in **all** phases of an operation. This means that a key to success is to link the PHA closely to the Operations Analysis.

EXAMPLES: The following (Figure 1.1.2B) is an example of a PHA.

Figure 1.1.2B Example PHA

MOVING A HEAVY PIECE OF EQUIPMENT	
<p>The example below uses an operation analysis for moving a heavy piece of equipment as the start point and illustrates the process of building the PHA direct from the Operations Analysis. Operation: Move a 3-ton machine from one building to another. Start Point: The machine is in its original position in building A End Point: The machine is in its new position in building B</p>	
ACTIVITY / EVENT	HAZARD
Raise the machine to permit positioning of the forklift	Machine overturns due to imbalance Machine overturns due to failure of lifting device Machine drops on person or equipment due to failure of lifting device or improper placement (person lifting device) Machine strikes overhead obstacle Machine is damaged by the lifting process
Position the forklift	Forklift strikes the machine Forklift strikes other items in the area
Lift the machine	Machine strikes overhead obstacle Lift fails due to mechanical failure (damage to machine, objects, or people) Machine overturns due to imbalance
Move machine to the truck	Instability due to rough surface or weather condition Operator error causes load instability The load shifts
Place machine on the truck	Improper tiedown produces instability Truck overloaded or improper load distribution
Drive truck to building B	Vehicle accident during the move Poor driving technique produces instability Instability due to road condition
Remove machine from the truck	Same factors as "Move it to the truck"
Place machine in proper position in building B	Same factors as "Raise the machine" except focused on lowering the machine

1.1.3 THE "WHAT IF" TOOL

FORMAL NAME: The "What If" tool

ALTERNATIVE NAMES: None.

PURPOSE: The "What If" tool is one of the most powerful hazard identification tools. As in the case of the Scenario Process tool, it is designed to add structure to the intuitive and experiential expertise of operational personnel. The "What If" tool is especially effective in capturing hazard data about failure modes that may create hazards. It is somewhat more structured than 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" tool should be used in most hazard identification applications, including many time-critical applications. A classic use of the "What If" tool is as the first tool used after the Operations Analysis and the PHA. For example, the PHA reveals an area of hazard that needs additional investigation. The best single tool to further investigate that area will be the "What If" tool. The user will zoom in on the particular area of concern, add detail to the OA in this area and then use the "What If" procedure to identify the hazards.

METHOD: Ensure that participants have a thorough knowledge of the anticipated flow of the operation. Visualize the expected flow of events in time sequence from the beginning to the 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 hazards. Ask, "what if various failures occurred or problems arose"? Add hazards 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 developing short scenarios that reflect the worst credible outcome from the compound effects of multiple hazards in the operation.

Follow these guidelines in writing scenarios:

- Target length is 5 or 6 sentences, 60 words
- Don't dwell on grammatical details
- Include elements of Mission, Man, Machine, Management, and Media
- Start with history
- Encourage imagination and intuition
- Carry the scenario to the worst credible outcome
- Use a single person or group to edit

RESOURCES: A key resource for the "What If" tool is the Operations Analysis. It may be desirable to add detail to it in the area to be targeted by the "What If" analysis. However, in most cases an OA can be used as-is, if it is available. The "What If" tool 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 lines supervisors. Because of its effectiveness, dynamic character, and ease of application, these personnel are generally quite willing to support the "What If" process.

COMMENTS: The "What If" tool is so effective that the Occupational Safety and Health Administration (OSHA) has designated as it one of six tools from among which activities facing catastrophic risk situations must choose under the mandatory hazard analysis provisions of the process safety standard.

EXAMPLES: Following (Figure 1.1.3A) is an extract from the typical output from the "What If" tool.

Figure 1.1.3A Example What If Analysis

<p>Situation: Picture a group of 3 operational employees informally applying the round robin procedure for the "What If" tool to a task to move a multi-ton machine from one location to another. A part of the discussion might go as follows:</p>
<p><u>Joe</u>: What if the machine tips over and falls breaking the electrical wires that run within the walls behind it? <u>Bill</u>: What if it strikes the welding manifolds located on the wall on the West Side? (<i>This illustrates "piggybacking" as Bill produces a variation of the hazard initially presented by Joe.</i>) <u>Mary</u>: What if the floor fails due to the concentration of weight on the base of the lifting device? <u>Joe</u>: What if the point on the machine used to lift it is damaged by the lift? <u>Bill</u>: What if there are electrical, air pressure hoses, or other attachments to the machine that are not properly neutralized? <u>Mary</u>: What if the lock out/tag out is not properly applied to energy sources servicing the machine? <i>And so on....</i></p>
<p>Note: The list above for example might be broken down as follows:</p> <p>Group 1: Machine falling hazards Group 2: Weight induced failures Group 3: Machine disconnect and preparation hazards</p> <p>These related groups of hazards are then subjected to the remaining five steps of the ORM process.</p>

1.1.4 THE SCENARIO PROCESS TOOL

FORMAL NAME: The Scenario Process tool

ALTERNATIVE NAMES: The mental movie tool.

PURPOSE: The Scenario Process tool is a time-tested procedure to identify hazards by visualizing them. It is designed to capture the intuitive and experiential expertise of personnel involved in planning or executing an operation, in a structured manner. It is especially useful in connecting individual hazards into situations that might actually occur. It is also used to visualize the worst credible outcome of one or more related hazards, and is therefore an important contributor to the risk assessment process.

APPLICATION: The Scenario Process tool should be used in most hazard identification applications, including some time-critical applications. In the time-critical mode, it is indeed one of the few practical

tools, in that the user can quickly form a “mental movie” of the flow of events immediately ahead and the associated hazards.

METHOD: The user of the Scenario Process tool attempts to visualize the flow of events in an operation. This is often described as constructing a “mental movie”. It is often effective to close the eyes, relax and let the images flow. Usually the best procedure is to use the flow of events established in the OA. An effective method is to visualize the flow of events twice. The first time, see the events as they are intended to flow. The next time, inject “Murphy” at every possible turn. As hazards are visualized, they are recorded for further action. Some good guidelines for the development of scenarios are as follows:

Limit them to 60 words or less. Don’t get tied up in grammatical excellence (in fact they don’t have to be recorded at all). Use historical experience but avoid embarrassing anyone. Encourage imagination (this helps identify risks that have not been previously encountered). Carry scenarios to the worst credible event.

RESOURCES: The key resource for the Scenario Process tool is the Operations Analysis. It provides the script for the flow of events that will be visualized. Using the tool does not require a specialist. Operational personnel leading or actually performing the task being assessed are key resources for the OA. Using this tool is often entertaining, dynamic and often motivates even the most junior personnel in the organization.

COMMENTS: A special value of the Scenario Process tool is its ability to link two or more individual hazards developed using other tools into an operation relevant scenario.

EXAMPLES. Following is an example (Figure 1.1.4A) of how the Scenario Process tool might be used in an operational situation.

Figure 1.1.4A Example Machine Movement Scenario

FROM MACHINE MOVEMENT EXAMPLE: As the machine was being jacked-up to permit placement of the forklift, the fitting that was the lift point on the machine broke. The machine tilted in that direction and fell over striking the nearby wall. This in turn broke a fuel gas line in the wall. The gas was turned off as a precaution, but the blow to the metal line caused the valve to which it was attached to break, releasing gas into the atmosphere. The gas quickly reached the motor of a nearby fan (not explosion proof) and a small explosion followed. Several personnel were badly burned and that entire section of the shop was badly damaged. The shop was out of action for 3 weeks.

1.1.5 THE LOGIC DIAGRAM

FORMAL NAME: The Logic Diagram

ALTERNATIVE NAMES: The Logic Tree

PURPOSE: The Logic Diagram is intended to provide considerable structure and detail as a primary hazard identification procedure. Its graphic structure is an excellent means of capturing and correlating

the hazard data produced by the other primary tools. Because of its graphic display, it can also be an effective hazard-briefing tool. The more structured and logical nature of the Logic Diagram adds substantial depth to the hazard identification process to complement the other more intuitive and experiential tools. Finally, an important purpose of the Logic Diagram is to establish the connectivity and linkages that often exist between hazards. It does this very effectively through its tree-like structure.

APPLICATION: Because it is more structured, the Logic Diagram requires considerable time and effort to accomplish. Following the principles of ORM, its use will be more limited than the other primary tools. This means limiting its use to higher risk issues. By its nature it is also most effective with more complicated operations in which several hazards may be interlinked in various ways. Because it is more complicated than the other primary tools, it requires more practice, and may not appeal to all operational personnel. However, in an organizational climate committed to ORM excellence, the Logic Diagram will be a welcomed and often used addition to the hazard identification toolbox.

METHOD: There are three types of Logic Diagrams. These are the:

Positive diagram. This variation is designed to highlight the factors that must be in place if risk is to be effectively controlled in the operation. It works from a safe outcome back to the factors that must be in place to produce it.

Event diagram. This variation focuses on an individual operational event (often a failure or hazard identified using the "What If" tool) and examines the possible consequences of the event. It works from an event that may produce risk and shows what the loss outcomes of the event may be.

Negative diagram. This variation selects a loss event and then analyzes the various hazards that could combine to produce that loss. It works from an actual or possible loss and identifies what factors could produce it.

All of the various Logic Diagram options can be applied either to an actual operating system or one being planned. Of course, the best time for application is in the planning stages of the operational lifecycle. All of the Logic Diagram options begin with a top block. In the case of the positive diagram, this is a desired outcome; in the case of the event diagram, this is an operations event or contingency possibility; in the case of the negative diagram, it is a loss event. When working with positive diagram or negative diagram, the user then, reasons out the factors that could produce the top event. These are entered on the next line of blocks. With the event diagram, the user lists the possible results of the event being analyzed. The conditions that could produce the factors on the second line are then considered and they are entered on the third line. The goal is to be as logical as possible when constructing Logic Diagrams, but it is more important to keep the hazard identification goal in mind than to construct a masterpiece of logical thinking. Therefore, a Logic Diagram should be a worksheet with lots of changes and variations marked on it. With the addition of a chalkboard or flip chart, it becomes an excellent group tool.

Figure 1.1.5A below is a generic diagram, and it is followed by a simplified example of each of the types of Logic Diagrams (Figures 1.1.5B, 1.1.5C, 1.1.5D).

Figure 1.1.5A Generic Logic Diagram

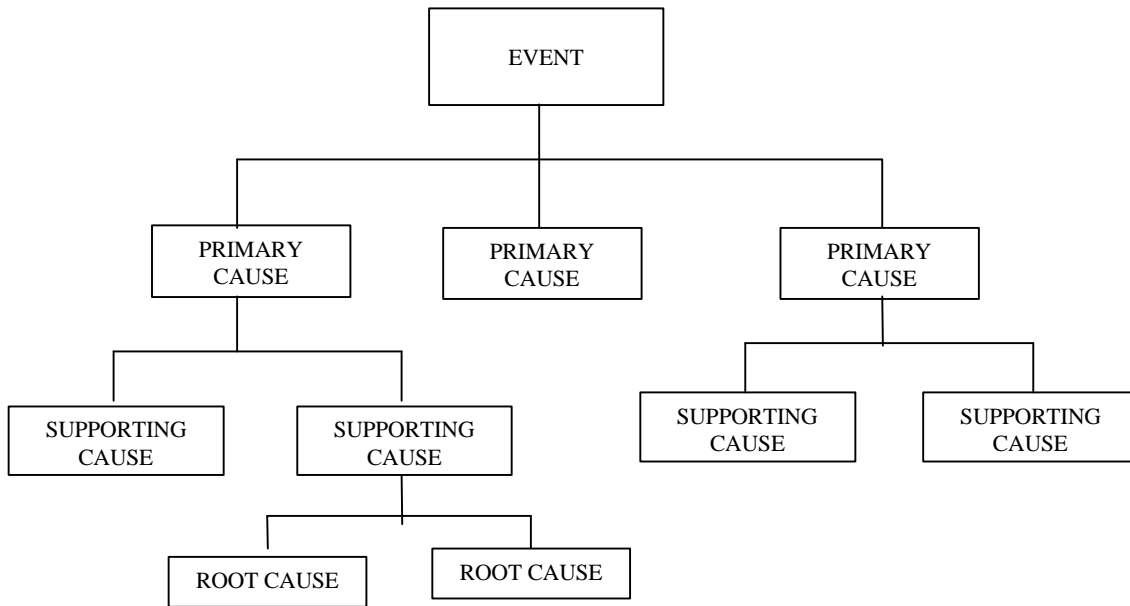


Figure 1.1.5B Positive Event Logic Diagram

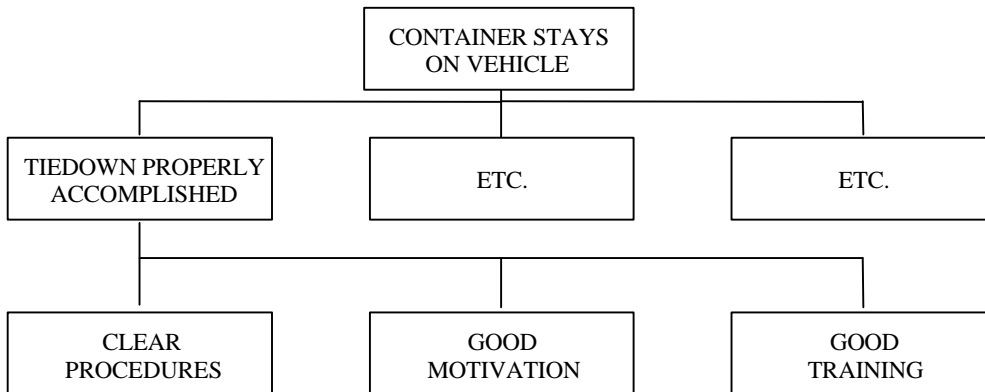


Figure 1.1.5C Risk Event Diagram

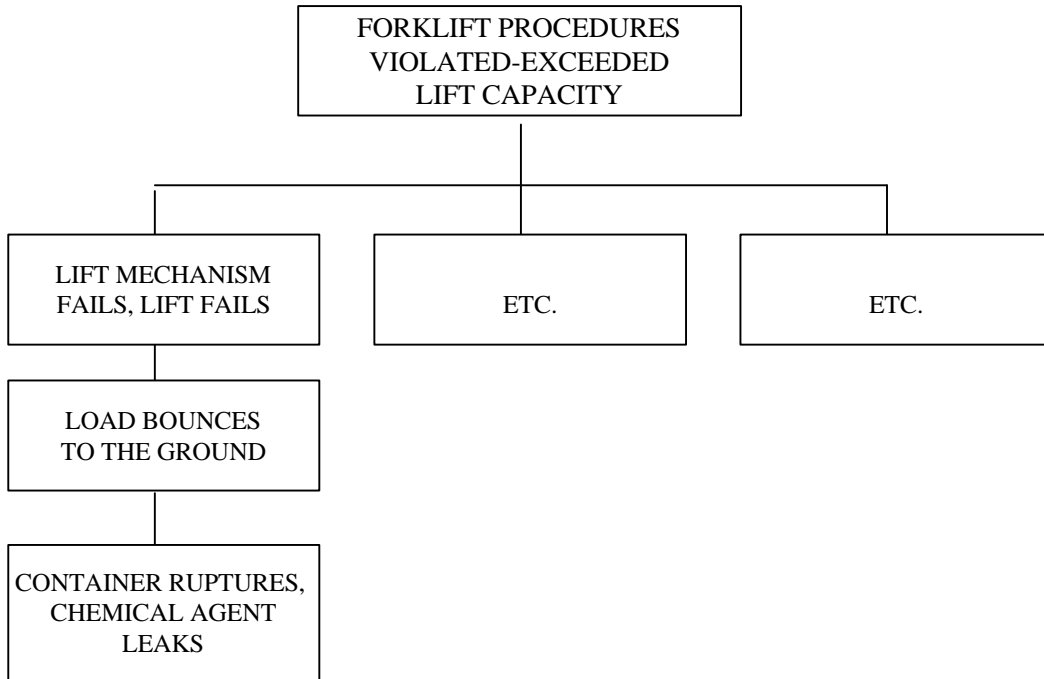
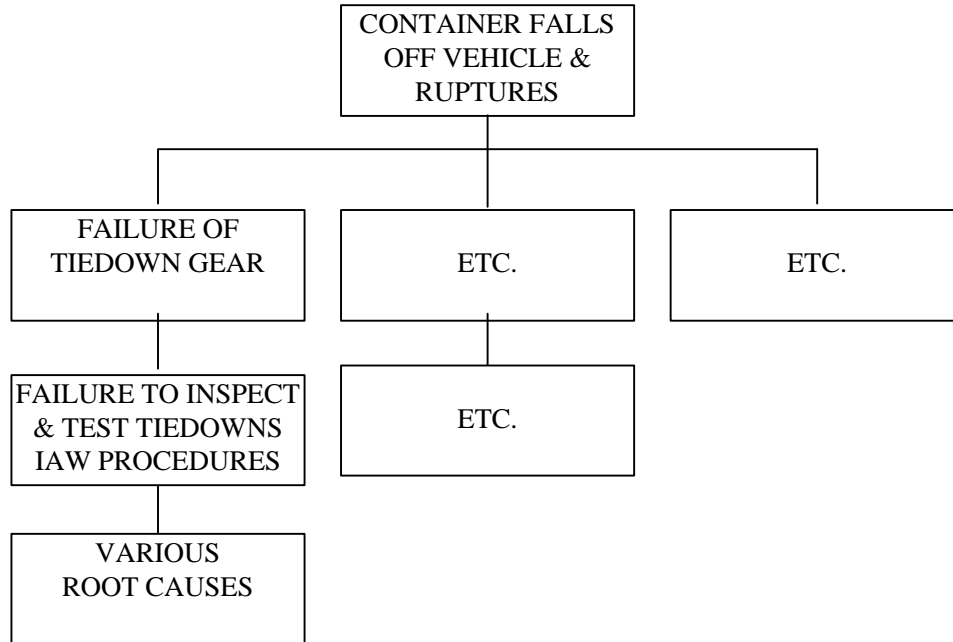


Figure 1.1.5D Negative Event Logic Diagram

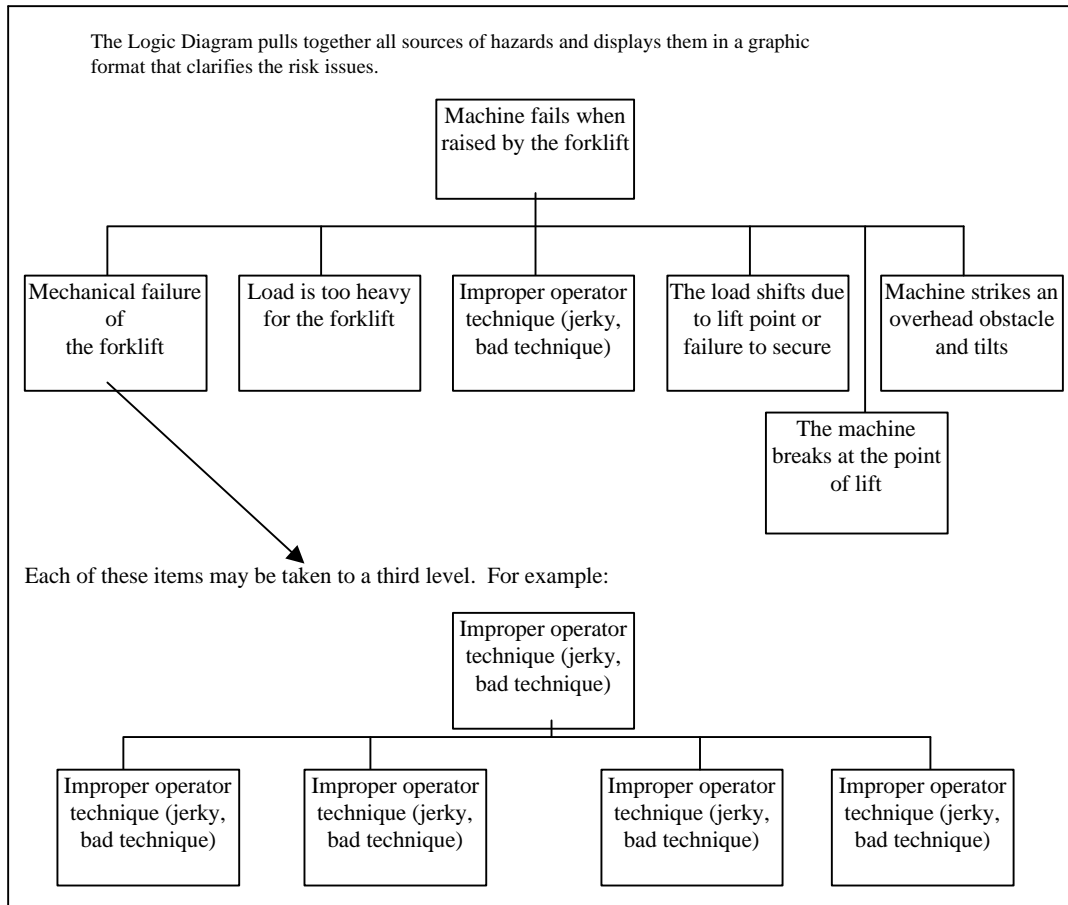


RESOURCES: All of the other primary tools are key resources for the Logic Diagram, as it can correlate hazards that they generate. If available, a safety professional may be an effective facilitator for the Logic Diagram process.

COMMENTS: The Logic Diagram is the most comprehensive tool available among the primary procedures. Compared to other approaches to hazard identification, it will substantially increase the quantity and quality of hazards identified.

EXAMPLE: Figure 1.1.5E illustrates how a negative diagram could be constructed for moving a heavy piece of equipment.

Figure 1.1.5E Example Negative Diagram



1.1.6 THE CHANGE ANALYSIS

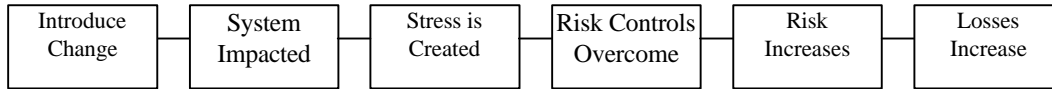
FORMAL NAME: The Change Analysis

ALTERNATIVE NAMES: None

PURPOSE: Change is an important source of risk in operational processes.

Figure 1.1.6A illustrates this causal relationship.

Figure 1.1.6A Change Causation



Some changes are planned, but many others occur incrementally over time, without any conscious direction. The Change Analysis is intended to analyze the hazard implications of either planned or incremental changes. The Change Analysis helps to focus only on the changed aspects of the operation, thus eliminating the need to reanalyze the total operation, just because a change has occurred in one area. The Change Analysis is also used to detect the occurrence of change. By periodically comparing current procedures with previous ones, unplanned changes are identified and clearly defined. Finally, Change Analysis is an important accident investigation tool. Because many incidents/accidents are due to the injection of change into systems, an important investigative objective is to identify these changes using the Change Analysis procedure.

APPLICATION: Change analysis should be routinely used in the following situations.

Whenever significant changes are planned in operations in which there is significant operational risk of any kind. An example is the decision to conduct a certain type of operation at night that has heretofore only been done in daylight.

Periodically in any important operation, to detect the occurrence of unplanned changes.

As an accident investigation tool.

As the only hazard identification tool required when an operational area has been subjected to in-depth hazard analysis, the Change Analysis will reveal whether any elements exist in the current operations that were not considered in the previous in-depth analysis.

METHOD: The Change Analysis is best accomplished using a format such as the sample worksheet shown at Figure 1.1.6B. The factors in the column on the left side of this tool are intended as a comprehensive change checklist.

Figure 1.1.6B Sample Change Analysis Worksheet

Target: _____		Date: _____		
FACTORS	EVALUATED SITUATION	COMPARABLE SITUATION	DIFFERENCE	SIGNIFICANCE
WHAT Objects Energy Defects Protective Devices WHERE On the object In the process Place WHEN In time In the process WHO Operator Fellow worker Supervisor Others TASK Goal Procedure Quality WORKING CONDITIONS Environmental Overtime Schedule Delays TRIGGER EVENT MANAGERIAL CONTROLS Control Chain Hazard Analysis Monitoring Risk Review				
<p>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. When used in an accident investigation, the accident situation is compared to a previous baseline. The significance of detected changes can be evaluated intuitively or they can be subjected to "What If", Logic Diagram, or scenario, other specialized analyses.</p>				

RESOURCES: Experienced operational personnel are a key resource for the Change Analysis tool. Those who have long-term involvement in an operational process must help define the “comparable situation.” Another important resource is the documentation of process flows and task analyses. Large numbers of such analyses have been completed in recent years in connection with quality improvement and reengineering projects. These materials are excellent definitions of the baseline against which change can be evaluated.

COMMENTS: In organizations with mature ORM processes, most, if not all, higher risk activities will have been subjected to thorough ORM applications and the resulting risk controls will have been incorporated into operational guidance. In these situations, the majority of day-to-day ORM activity will be the application of Change Analysis to determine if the operation has any unique aspects that have not been previously analyzed.

1.1.7 THE CAUSE AND EFFECT TOOL

FORMAL NAME: The Cause and Effect Tool

ALTERNATIVE NAMES: The cause and effect diagram. The fishbone tool, the Ishikawa Diagram

PURPOSE: The Cause and Effect Tool is a variation of the Logic Tree tool and is used in the same hazard identification role as the general Logic Diagram. The particular advantage of the Cause and Effect Tool is its origin in the quality management process and the thousands of personnel who have been trained in the tool. Because it is widely used, thousands of personnel are familiar with it and therefore require little training to apply it to the problem of detecting risk.

APPLICATION: The Cause and Effect Tool will be effective in organizations that have had some success with the quality initiative. It should be used in the same manner as the Logic Diagram and can be applied in both a positive and negative variation.

METHOD: The Cause And Effect diagram is a Logic Diagram with a significant variation. It provides more structure than the Logic Diagram through the branches that give it one of its alternate names, the fishbone diagram. The user can tailor the basic “bones” based upon special characteristics of the operation being analyzed. Either a positive or negative outcome block is designated at the right side of the diagram. Using the structure of the diagram, the user completes the diagram by adding causal factors in either the “M” or “P” structure. Using branches off the basic entries, additional hazards can be added. The Cause And Effect diagram should be used in a team setting whenever possible.

RESOURCES: There are many publications describing in great detail how to use cause and effect diagrams.¹

COMMENTS:

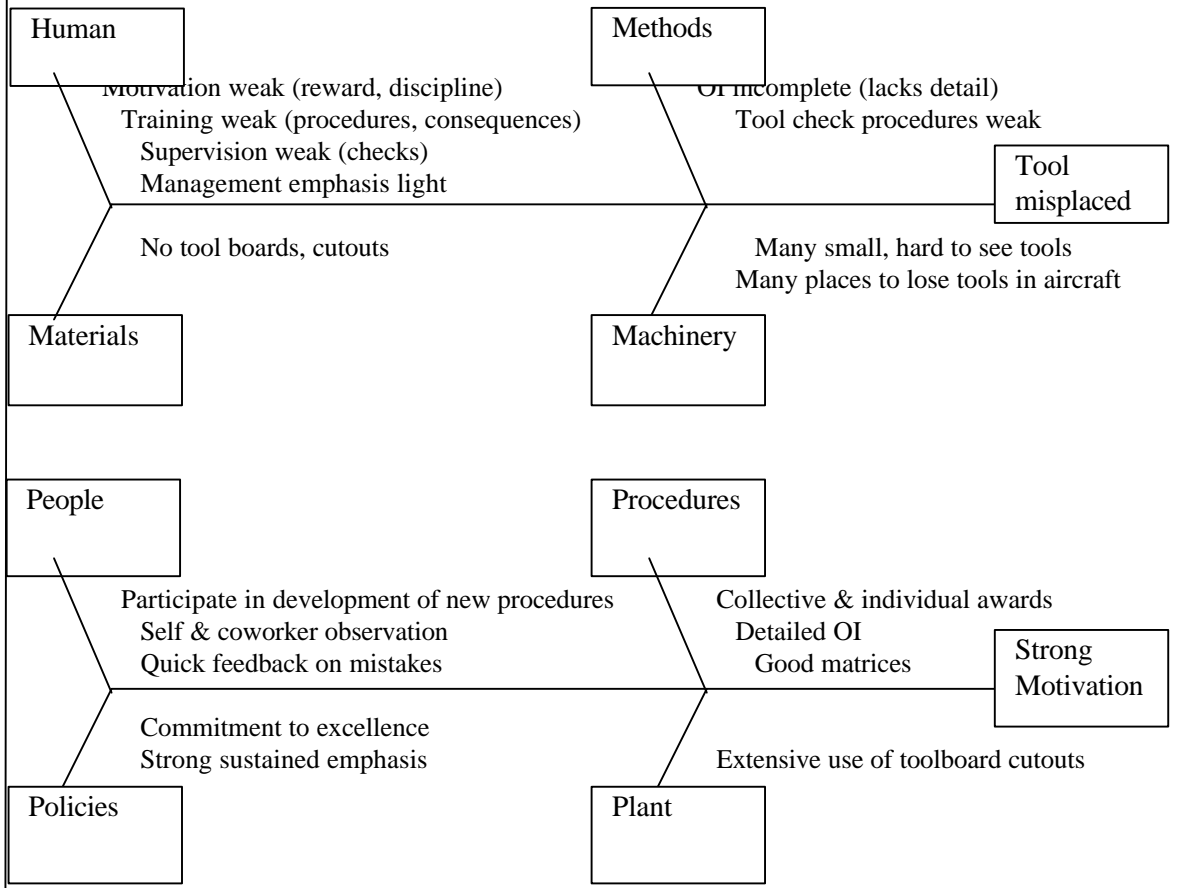
EXAMPLES: An example of Cause and Effect Tool in action is illustrated at Figure 1.1.7A.

¹ K. Ishikawa, Guide to Quality Control, Quality Resources, White Plains, New York, 12th Printing 1994.

Figure 1.1.7 Example of Cause and Effect

SITUATION: The supervisor of an aircraft maintenance operation has been receiving reports from Quality Assurance regarding tools in aircraft after maintenance over the last six months. The supervisor has followed up but each case has involved a different individual and his spot checks seem to indicate good compliance with tool control procedures. He decides to use a cause and effect diagram to consider all the possible sources of the tool control problem. The supervisor develops the cause and effect diagram with the help of two or three of his best maintenance personnel in a group application.

NOTE: Tool control is one of the areas where 99% performance is not adequate. That would mean one in a hundred tools are misplaced. The standard must be that among the tens (or hundreds) of thousands of individual uses of tools over a year, not one is misplaced.



Using the positive diagram as a guide the supervisor and working group apply all possible and practical options developed from it.

1.2 THE SPECIALTY HAZARD IDENTIFICATION TOOLS

The tools that follow are designed to augment the primary tools described in part 1.1. These tools have several advantages:

They can be used by nearly everyone in the organization, though some may require either training or professional facilitation.

Each tool provides a capability not fully realized in any of the primary tools.

They use the tools of the less formal safety program to support the ORM process.

They are well supported with forms, job aids, and models.

Their effectiveness has been proven. In an organization with a mature ORM process, all personnel will be aware of the existence of these specialty tools and capable of recognizing the need for their application. While not everyone will be comfortable using every procedure, a number of people within the organization will have experience applying one or another of them.

1.2.1 THE HAZARD AND OPERABILITY TOOL

FORMAL NAME: The Hazard and Operability Tool

ALTERNATIVE NAMES: The HAZOP analysis

PURPOSE: The special role of the HAZOP is hazard analysis of completely new operations. In these situations, traditional intuitive and experiential hazard identification procedures are especially weak. This lack of experience hobbles tools such as the "What If" and Scenario Process tools, which rely heavily on experienced operational personnel. The HAZOP deliberately maximizes structure and minimizes the need for experience to increase its usefulness in these situations.

APPLICATION: The HAZOP should be considered when a completely new process or procedure is going to be undertaken. The issue should be one where there is significant risk because the HAZOP does demand significant expenditure of effort and may not be cost effective if used against low risk issues. The HAZOP is also useful when an operator or leader senses that "something is wrong" but they can't identify it. The HAZOP will dig very deeply into the operation and to identify what that "something" is.

METHOD: The HAZOP is the most highly structured of the hazard identification procedures. It uses a standard set of guide terms (Figure 1.1) which are then linked in every possible way with a tailored set of process terms (for example "flow"). The process terms are developed directly from the actual process or from the Operations Analysis. The two words together, for example "no" (a guideword) and "flow" (a process term) will describe a deviation. These are then evaluated to see if a meaningful hazard is indicated. If so, the hazard is entered in the hazard inventory for further evaluation. Because of its rigid process, the HAZOP is especially suitable for one-person hazard identification efforts.

Figure 1.2.1A Standard HAZOP Guidewords

NO	Note: This basic set of guidewords should be all that are needed for all applications. Nevertheless, when useful, specialized terms can be added to the list. In less complex applications only some of the terms may be needed.
MORE	
LESS	
REVERSE	
LATE	
EARLY	

RESOURCES: There are few resources available to assist with HAZOP; none are really needed.

COMMENTS: The HAZOP is highly structured, and often time-consuming. Nevertheless, in its special role, this tool works very effectively. OSHA selected it for inclusion in the set of six mandated procedures of the OSHA process safety standard.

1.2.2 THE MAPPING TOOL

FORMAL NAME: The Mapping Tool

ALTERNATIVE NAMES: Map analysis

PURPOSE: The map analysis is designed to use terrain maps and other system models and schematics to identify both things at risk and the sources of hazards. Properly applied the tool will reveal the following:

Task elements at risk

The sources of risk

The extent of the risk (proximity)

Potential barriers between hazard sources and operational assets

APPLICATION: The Mapping Tool can be used in a variety of situations. The explosive quantity-distance criteria are a classic example of map analysis. The location of the flammable storage is plotted and then the distance to various vulnerable locations (inhabited buildings, highways, etc.) is determined. The same principles can be extended to any facility. We can use a diagram of a maintenance shop to note the location of hazards such as gases, pressure vessels, flammables, etc. Key assets can also be plotted. Then hazardous interactions are noted and the layout of the facility can be optimized in terms of risk reduction.

METHOD: The Mapping Tool requires some creativity to realize its full potential. The starting point is a map, facility layout, or equipment schematic. The locations of hazard sources are noted. The easiest way to detect these sources is to locate energy sources, since all hazards involve the unwanted release of energy. Figure 1.2.2A lists the kinds of energy to look for. Mark the locations of these sources on the map or diagram. Then, keeping the operation in mind, locate the personnel, equipment, and facilities that the various potentially hazardous energy sources could impact. Note these potentially hazardous links and enter them in the hazard inventory for risk management.

Figure 1.2.2A Major Types of Energy

Electrical Kinetic (moving mass e.g. a vehicle, a machine part, a bullet) Potential (not moving mass e.g. a heavy object suspended overhead) Chemical (e.g. explosives, corrosive materials) Noise and Vibration Thermal (heat) Radiation (Non-ionizing e.g. microwave, and ionizing e.g. nuclear radiation, x-rays) Pressure (air, hydraulic, water)
--

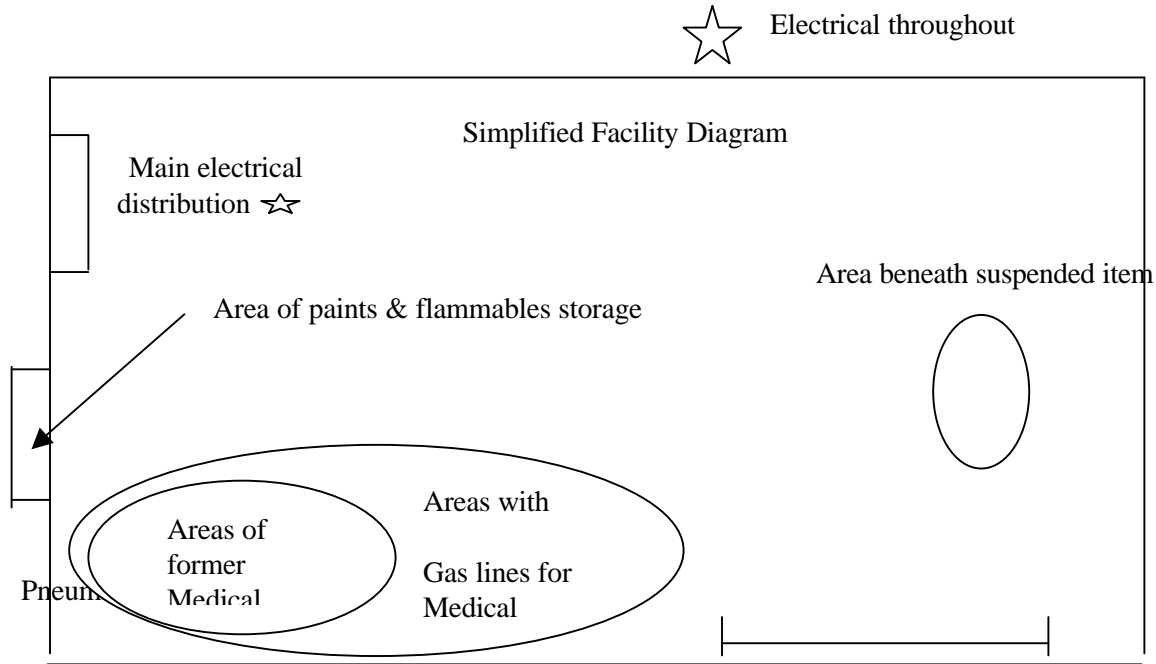
RESOURCES: Maps can convey a great deal of information, but cannot replace the value of an on-site assessment. Similarly, when working with an equipment schematic or a facility layout, there is no substitute for an on-site inspection of the equipment or survey of the facility.

COMMENTS: The map analysis is valuable in itself, but it is also excellent input for many other tools such as the Interface Analysis, Energy Trace and Barrier Analysis, and Change Analysis.

EXAMPLE: The following example (Figure 1.2.2B) illustrates the use of a facility schematic that focuses on the energy sources there as might be accomplished in support of an Energy Trace and Barrier Analysis.

SITUATION: A team has been assigned the task of renovating an older facility for use as a museum for historical aviation memorabilia. They evaluate the facility layout (schematic below). By evaluating the potential energy sources presented in this schematic, it is possible to identify hazards that may be created by the operations to be conducted.

Figure 1.2.2B Example Map Analysis
FACILITY ENERGY SOURCES



1.2.3 THE INTERFACE ANALYSIS

FORMAL NAME: The Interface Analysis

ALTERNATIVE NAMES: Interface Hazard Analysis

PURPOSE: The Interface Analysis is intended to uncover the hazardous linkages or interfaces between seemingly unrelated activities. For example, we plan to build a new facility. What hazards may be created for other operations during construction and after the facility is operational? The Interface Analysis reveals these hazards by focusing on energy exchanges. By looking at these potential energy transfers between two different activities, we can often detect hazards that are difficult to detect in any other way.

APPLICATION: An Interface Analysis should be conducted any time a new activity is being introduced and there is any chance at all that unfavorable interaction could occur. A good cue to the need for an Interface Analysis is the use of either the Change Analysis (indicating the injection of something new) or the map analysis (with the possibility of interactions).

METHOD: The Interface Analysis is normally based on an outline such as the one illustrated at Figure 3.1. The outline provides a list of potential energy types and guides the consideration of the potential interactions. A determination is made whether a particular type of energy is present and then whether

there is potential for that form of energy to adversely affect other activities. As in all aspects of hazard identification, the creation of a good Operations Analysis is vital.

Figure 1.2.3A The Interface Analysis Worksheet

Energy Element
Kinetic (objects in motion)
Electromagnetic (microwave, radio, laser)
Radiation (radioactive, x-ray)
Chemical
Other
Personnel Element: Personnel moving from one area to another
Equipment Element: Machines and material moving from one area to another
Supply/materiel Element:
Intentional movement from one area to another
Unintentional movement from one area to another
Product Element: Movement of product from one area to another
Information Element: Flow of information from one area to another or interference (i.e. jamming)
Bio-material Element
Infectious materials (virus, bacteria, etc.)
Wildlife
Odors

RESOURCES: Interface Analyses are best accomplished when personnel from all of the involved activities participate, so that hazards and interfaces in *both* directions can be effectively and knowledgeably addressed. A safety office representative can also be useful in advising on the types and characteristics of energy transfers that are possible.

COMMENTS: The lessons of the past indicate that we should give serious attention to use of the Interface Analysis. Nearly anyone who has been involved in operations for any length of time can relate stories of overlooked interfaces that have had serious adverse consequences.

EXAMPLES: An Interface Analysis using the general outline is shown below.

Figure 1.2.3B Example Interface Analysis

SITUATION: Construction of a heavy equipment maintenance facility is planned for the periphery of the complex at a major facility. This is a major complex costing over \$2,000,000 and requiring about eight months to complete. The objective is to detect interface issues in both directions. Notice that the analysis reveals a variety of interface issues that need to be thought through carefully.

Energy Interface

Movement of heavy construction equipment

Movement of heavy building supplies

Movement of heavy equipment for repair

Possible hazmat storage/use at the facility

Personnel Interface

Movement of construction personnel (vehicle or pedestrian) through base area

Movement of repair facility personnel through base area

Possible movement of base personnel (vehicular or pedestrian) near or through the facility

Equipment Interface: Movement of equipment as indicated above

Supply Interface

Possible movement of hazmat through base area

Possible movement of fuels and gases

Supply flow for maintenance area through base area

Product Interface

Movement of equipment for repair by tow truck or heavy equipment transport through the base area

Information Interface

Damage to buried or overhead wires during construction or movement of equipment

Possible Electro-magnetic interference due to maintenance testing, arcing, etc.

Biomaterial Interface: None

1.2.4 THE ACCIDENT/INCIDENT ANALYSIS

FORMAL NAME: The Accident/Incident Analysis

ALTERNATIVE NAMES: The accident analysis

PURPOSE: Most organizations have accumulated extensive, detailed databases that are gold mines of risk data. The purpose of the analysis is to apply this data to the prevention of future accidents or incidents.

APPLICATION: Every organization should complete an operation incident analysis annually. The objective is to update the understanding of current trends and causal factors. The analysis should be completed for each organizational component that is likely to have unique factors.

METHOD: The analysis can be approached in many ways. The process generally builds a database of the factors listed below and which serves as the basis to identify the risk drivers
Typical factors to examine include the following:

Activity at the time of the accident
Distribution of incidents among personnel
Accident locations
Distribution of incidents by sub-unit
Patterns of unsafe acts or conditions

RESOURCES: The analysis relies upon a relatively complete and accurate database. The FAA's system safety office (ASY) may have the needed data. That office can also provide assistance in the analysis process. System Safety personnel may have already completed analyses of similar activities or may be able to suggest the most productive areas for initial analysis.

COMMENTS: The data in databases has been acquired the hard way - through the painful and costly mistakes of hundreds of individuals. By taking full advantage of this information the analysis process can be more realistic, efficient, and thorough and thereby preventing the same accidents (incidents?) from occurring over and over again.

1.2.5 THE INTERVIEW TOOL

FORMAL NAME: The Interview Tool

ALTERNATIVE NAMES: None

PURPOSE: Often the most knowledgeable personnel in the area of risk are those who operate the system. They see the problems and often think about potential solutions. The purpose of the Interview Tool is to capture the experience of these personnel in ways that are efficient and positive for them. Properly implemented, the Interview Tool can be among the most valuable hazard identification tools.

APPLICATION: Every organization can use the Interview Tool in one form or another.

METHOD: The Interview Tool's great strength is versatility. Figure 1.2.5A illustrates the many options available to collect interview data. Key to all of these is to create a situation in which interviewees feel free to honestly report what they know, without fear of any adverse consequences. This means absolute confidentiality must be assured, by not using names in connection with data.

Figure 1.2.5A Interview Tool Alternatives

Direct interviews with operational personnel Supervisors interview their subordinates and report results Questionnaire interviews are completed and returns Group interview sessions (several personnel at one time) Hazards reported formally Coworkers interview each other
--

RESOURCES: It is possible to operate the interview process facility-wide with the data being supplied to individual units. Hazard interviews can also be integrated into other interview activities. For example, counseling sessions could include a hazard interview segment. In these ways, the expertise and resource demands of the Interview Tool can be minimized.

COMMENTS: The key source of risk is human error. Of all the hazard identification tools, the Interview Tool is potentially the most effective at capturing human error data.

EXAMPLES: Figure 1.2.5B illustrates several variations of the Interview Tool.

Figure 1.2.5B Example Exit Interview Format

Name (optional) _____ Organization _____
1. Describe below incidents, near misses or close calls that you have experienced or seen since you have been in this organization. State the location and nature (i.e. what happened and why) of the incident. If you can't think of an incident, then describe two hazards you have observed.
INCIDENT 1: Location: _____ What happened and why? _____ _____
INCIDENT 2: Location: _____ What happened and why? _____ _____
2. What do you think other personnel can do to eliminate these problems?
Personnel: _____
Incident 1 _____
Incident 2 _____
Supervisors: _____
Incident 1 _____
Incident 2 _____
Top Leadership: _____
Incident 1 _____
Incident 2 _____

1.2.6 THE INSPECTION TOOL

FORMAL NAME: The Inspection Tool

ALTERNATIVE NAMES: The survey tool

PURPOSE: Inspections have two primary purposes. (1) The detection of hazards. Inspections accomplish this through the direct observation of operations. The process is aided by the existence of detailed standards against which operations can be compared. The OSHA standards and various national standards organizations provide good examples. (2) To evaluate the degree of compliance with established risk controls. When inspections are targeted at management and safety management processes, they are usually called surveys. These surveys assess the effectiveness of management procedures by evaluating status against some survey criteria or standard. Inspections are also important as accountability tools and can be turned into important training opportunities

APPLICATION: Inspections and surveys are used in the risk management process in much the same manner as in traditional safety programs. Where the traditional approach may require that all facilities are inspected on the same frequency schedule, the ORM concept might dictate that high-risk activities be inspected ten times or more frequently than lower risk operations, and that some of the lowest risk operations be inspected once every five years or so. The degree of risk drives the frequency and depth of the inspections and surveys.

METHOD: There are many methods of conducting inspections. From a risk management point of view the key is focusing upon what will be inspected. The first step in effective inspections is the selection of inspection criteria and the development of a checklist or protocol. This must be risk-based. Commercial protocols are available that contain criteria validated to be connected with safety excellence. Alternatively, excellent criteria can be developed using incident databases and the results of other hazard identification tools such as the Operations Analysis and Logic Diagrams, etc. Some these have been computerized to facilitate entry and processing of data. Once criteria are developed, a schedule is created and inspections are begun. The inspection itself must be as positive an experience as possible for the people whose activity is being inspected. Personnel performing inspections should be carefully trained, not only in the technical processes involved, but also in human relations. During inspections, the ORM concept encourages another departure from traditional inspection practices. This makes it possible to evaluate the trend in organization performance by calculating the percentage of unsafe (non-standard) versus safe (meet or exceed standard) observations. Once the observations are made the data must be carefully entered in the overall hazard inventory database. Once in the database the data can be analyzed as part of the overall body of data or as a mini-database composed of inspection findings only.

RESOURCES: There are many inspection criteria, checklists and related job aids available commercially. Many have been tailored for specific types of organizations and activities. The System Safety Office can be a valuable resource in the development of criteria and can provide technical support in the form of interpretations, procedural guidance, and correlation of data.

COMMENTS: Inspections and surveys have long track records of success in detecting hazards and reducing risk. However, they have been criticized as being inconsistent with modern management practice because they are a form of “downstream” quality control. By the time a hazard is detected by an inspection, it may already have caused loss. The ORM approach to inspections emphasizes focus on the

higher risks within the organization and emphasizes the use of management and safety program surveys that detect the underlying causes of hazards, rather than the hazards themselves.

EXAMPLES: Conventional inspections normally involve seeking and recording unsafe acts or conditions. The number of these may reflect either the number of unsafe acts or conditions occurring in the organization or the extent of the effort extended to find hazards. Thus, conventional inspections are not a reliable indicator of the extent of risk. To change the nature of the process, it is often only necessary to record the total number of observations made of key behaviors, then determine the number of unsafe behaviors. This yields a rate of “unsafeness” that is independent of the number of observations made.

1.2.7 THE JOB HAZARD ANALYSIS

FORMAL NAME: The Job Hazard Analysis

ALTERNATIVE NAMES: The task analysis, job safety analysis, JHA, JSA

PURPOSE: The purpose of the Job Hazard Analysis (JHA) is to examine in detail the safety considerations of a single job. A variation of the JHA called a task analysis focuses on a single task, i.e., some smaller segment of a “job.”

APPLICATION: Some organizations have established the goal of completing a JHA on every job in the organization. If this can be accomplished cost effectively, it is worthwhile. Certainly, the higher risk jobs in an organization warrant application of the JHA procedure. Within the risk management approach, it is important that such a plan be accomplished by beginning with the most significant risk areas first.

The JHA is best accomplished using an outline similar to the one illustrated at Figure 1.2.7A. As shown in the illustration, the job is broken down into its individual steps. Jobs that involve many quite different tasks should be handled by analyzing each major task separately. The illustration considers risks both to the workers involved, and to the system, as well as. Risk controls for both. Tools such as the Scenario and "What If" tools can contribute to the identification of potential hazards. There are two alternative ways to accomplish the JHA process. A safety professional can complete the process by asking questions of the workers and supervisors involved. Alternatively, supervisors could be trained in the JHA process and directed to analyze the jobs they supervise.

Figure 1.2.7A Sample Job Hazard Analysis Format

Job Safety Analysis	Job Title or Operation		Page of ISA Number
	Job Series/AFSC		Supervisor
Organization Symbol	Location/Building Number	Shop Title	Reviewed By
Required and/or Recommended Personal Protective Equipment			Approved By
SEQUENCE OF BASIC JOB STPES	POTENTIAL HAZARDS USAFE ACTS OR CONDITIONS	RECOMMENDED ACTION OR PROCEDURE	

RESOURCES: The System Safety Office has personnel trained in detail in the JHA process who can serve as consultants, and may have videos that walk a person through the process.

COMMENTS: The JHA is risk management. The concept of completing in-depth hazard assessments of all jobs involving significant risk with the active participation of the personnel doing the work is an ideal model of ORM in action.

1.2.8 THE OPPORTUNITY ASSESSMENT

FORMAL NAME: The Opportunity Assessment

ALTERNATIVE NAMES: The opportunity-risk tool

PURPOSE: The Opportunity Assessment is intended to identify opportunities to expand the capabilities of the organization and/or to significantly reduce the operational cost of risk control procedures. Either of these possibilities means expanded capabilities.

APPLICATION: Organizations should systematically assess their capabilities on a regular basis, especially in critical areas. The Opportunity Assessment can be one of the most useful tools in this process and therefore should be completed on all-important operations and then be periodically updated.

METHOD: The Opportunity Assessment involves five key steps as outlined at Figure 1.2.10A. In Step 1, operational areas that would benefit substantially from expanded capabilities are identified and prioritized. Additionally, areas where risk controls are consuming extensive resources or are otherwise constraining operation capabilities are listed and prioritized. Step 2 involves the analysis of the specific risk-related barriers that are limiting the desired expanded performance or causing the significant expense. This is a critical step. Only by identifying the risk issues precisely can focused effort be brought to bear to overcome them. Step 3 attacks the barriers by using the risk management process. This normally involves reassessment of the hazards, application of improved risk controls, improved implementation of existing controls, or a combination of these options. Step 4 is used when available risk management procedures don't appear to offer any breakthrough possibilities. In these cases the organization must seek out new

ORM tools using benchmarking procedures or, if necessary, innovate new procedures. Step 5 involves the exploitation of any breakthroughs achieved by pushing the operational limits or cost saving until a new barrier is reached. The cycle then repeats and a process of continuous improvement begins.

Figure 1.2.9A Opportunity Analysis Steps

- | |
|--|
| <p>Step 1. Review key operations to identify opportunities for enhancement. Prioritize.</p> <p>Step 2. In areas where opportunities exist, analyze for risk barriers.</p> <p>Step 3. When barriers are found, apply the ORM process.</p> <p>Step 4. When available ORM processes can't breakthrough, innovate!</p> <p>Step 5. When a barrier is breached, push through until a new barrier is reached.</p> |
|--|

RESOURCES: The Opportunity Assessment depends upon a detailed understanding of operational processes so that barriers can be identified. An effective Opportunity Assessment will necessarily involve operations experts.

1.3 THE ADVANCED HAZARD IDENTIFICATION TOOLS

The five tools that follow are advanced hazard identification tools designed to support strategic hazard analysis of higher risk and critical operations. These advanced tools are often essential when in-depth hazard identification is needed. They provide the mechanism needed to push the limits of current hazard identification technology. For example, the Management Oversight and Risk Tree (MORT) represents the full-time efforts of dozens of experts over decades to fully develop an understanding of all of the sources of hazards.

As might be expected, these tools are complex and require significant training to use. Full proficiency also requires experience in using them. They are best reserved for use by, loss control professionals. Those with an engineering, scientific, or other technical background are certainly capable of using these tools with a little read-in. Even though professionals use the tools, much of the data that must be fed into the procedures must come from operators.

In an organization with a mature ORM culture, all personnel in the organization will be aware that higher risk justifies more extensive hazard identification. They will feel comfortable calling for help from loss control professionals, knowing that these individuals have the advanced tools needed to cope with the most serious situations. These advanced tools will play a key role in the mature ORM culture in helping the organization reach its hazard identification goal: No significant hazard undetected.

1.3.1 THE ENERGY TRACE AND BARRIER ANALYSIS

FORMAL NAME: The Energy Trace and Barrier Analysis

ALTERNATIVE NAMES: Abnormal energy exchange

PURPOSE: The Energy Trace and Barrier Analysis (ETBA) is a procedure intended to detect hazards by focusing in detail on the presence of energy in a system and the barriers for controlling that energy. It is conceptually similar to the Interface Analysis in its focus on energy forms, but is considerably more thorough and systematic.

APPLICATION: The ETBA is intended for use by loss system safety professionals and is targeted against higher risk operations, especially those involving large amounts of energy or a wide variety of energy types. The method is used extensively in the acquisition of new systems and other complex systems.

METHOD: The ETBA involves 5 basic steps as shown at Figure 1.3.1A.

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 listed at Figure 1.3.1B.

Step 2 is the 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 the energy are assessed. Finally, in Step 5, risk control options are considered and selected.

Figure 1.3.1A ETBA Steps

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

Figure 1.3.1B Types of Energy

Electrical
Kinetic (moving mass e.g. a vehicle, a machine part, a bullet)
Potential (not moving mass e.g. a heavy object suspended overhead)
Chemical (e.g. explosives, corrosive materials)
Noise and Vibration
Thermal (heat)
Radiation (Non-ionizing e.g. microwave, and ionizing e.g. nuclear radiation, x-rays)
Pressure (air, Hydraulic, water)

RESOURCES: This tool requires sophisticated understanding of the technical characteristics of systems and of the various energy types and barriers. Availability of a safety professional, especially a safety engineer or other professional engineer is important.

COMMENTS: Most accidents involve the unwanted release of one kind of energy or another. This fact makes the ETBA a powerful hazard identification tool. When the risk stakes are high and the system is complex, the ETBA is a must have.

EXAMPLES: A simplified example of the ETBA procedure is provided at Figure 1.3.

Figure 1.3.1C Example ETBA

Scenario: The supervisor of a maintenance facility has just investigated a serious incident involving one of his personnel who received a serious shock while using a portable power drill in the maintenance area. The tool involved used a standard three-prong plug. Investigation revealed that the tool and the receptacle were both functioning properly. The individual was shocked when he was holding the tool and made contact with a piece of metal electrical conduit (it one his drill was plugged into) that had become energized as a result of an internal fault. As a result the current flowed through the individual to the tool and through the grounded tool to ground resulting in the severe shock. The supervisor decides to fully assess the control of electrical energy in this area.

Option 1. Three prong tool. Electrical energy flow that is from the source through an insulated wire, to the tool, to a single insulated electric motor. In the event of an internal fault the flow is from the case of the tool through the ground wire to ground through the grounded third prong through a properly grounded receptacle.

Hazards: Receptacle not properly grounded, third prong removed, person provides lower path of resistance, break in any of the ground paths (case, cord, plug, and receptacle). These hazards are serious in terms of the frequency encountered in the work environment and might be expected to be present in 10% or more cases.

Option 2. Double insulated tool. The tool is not grounded. Protection that is provided by double insulating the complete flow of electrical energy at all points in the tool. In the event of an internal fault, there are two layers of insulation protection between the fault and the person preventing shorting through the user.

Hazards: If the double layers of insulation are damaged as a result of extended use, rough handling, or repair/maintenance activity, the double insulation barrier can be compromised. In the absence of a fully effective tool inspection and replacement program such damage is not an unusual situation.

Option 3. Grand Fault Circuit Fault Interrupters. Either of the above types of tools is used (double insulated is preferred). Electrical energy flows as described above in both the normal and fault situations. However, in the event of a fault (or any other cause of a differential between the potential of a circuit), it is detected almost instantly and the circuit is opened preventing the flow of dangerous amounts of current. Because no dangerous amount of current can flow the individual using the tool is in no danger of shock. Circuit interrupters are reliable at a level of 1 in 10,000 or higher and when they do fail, most failure modes are in the fail-safe mode. Ground Fault circuit interrupters are inexpensive to purchase and relatively easy to install. In this case, the best option is very likely to be the use of the circuit interrupter in connection with either Option 1 or 2, with 2 the preferred. This combination for all practical purposes eliminates the possibility of electric shock and injury/death as a result of using portable power tools.

1.3.2 THE FAULT TREE ANALYSIS

FORMAL NAME: The Fault Tree Analysis

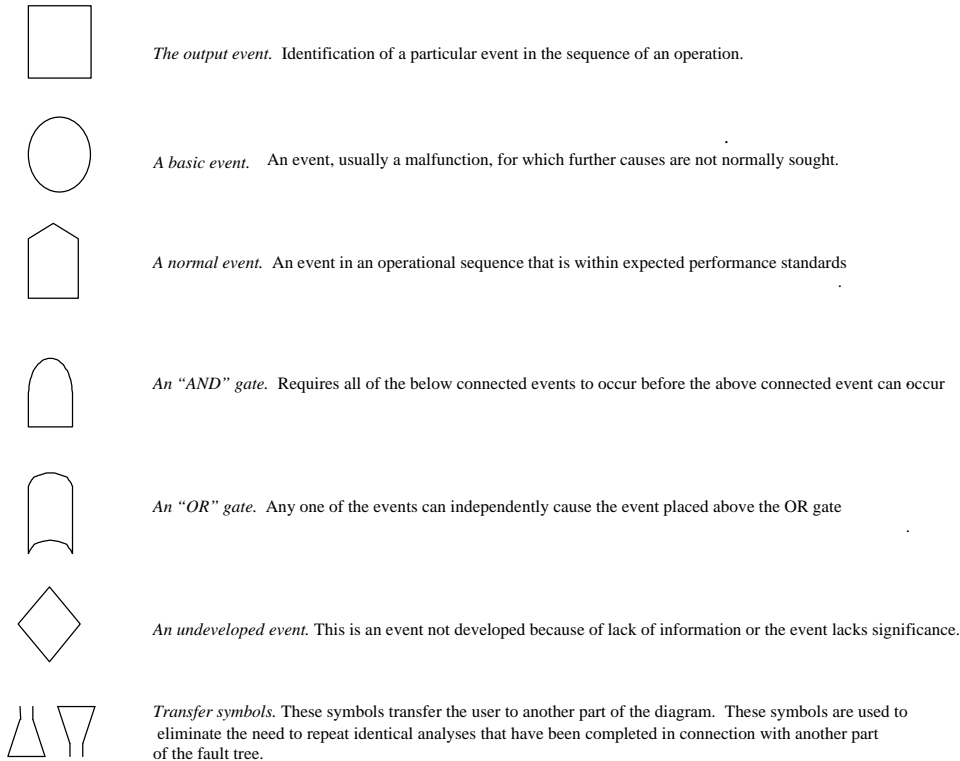
ALTERNATIVE NAMES: The logic tree

PURPOSE: The Fault Tree Analysis (FTA) is a hazard identification tool based on the negative type Logic Diagram. The FTA adds several dimensions to the basic logic tree. The most important of these additions are the use of symbols to add information to the trees and the possibility of adding quantitative risk data to the diagrams. With these additions, the FTA adds substantial hazard identification value to the basic Logic Diagram previously discussed.

APPLICATION: Because of its relative complexity and detail, it is normally not cost effective to use the FTA against risks assessed below the level of extremely high or high. The method is used extensively in the acquisition of new systems and other complex systems where, due to the complexity and criticality of the system, the tool is a must.

METHOD: The FTA is constructed exactly like a negative Logic Diagram except that the symbols depicted in Figure 1.3.2A are used.

Figure 1.3.2A Key Fault Tree Analysis Symbols

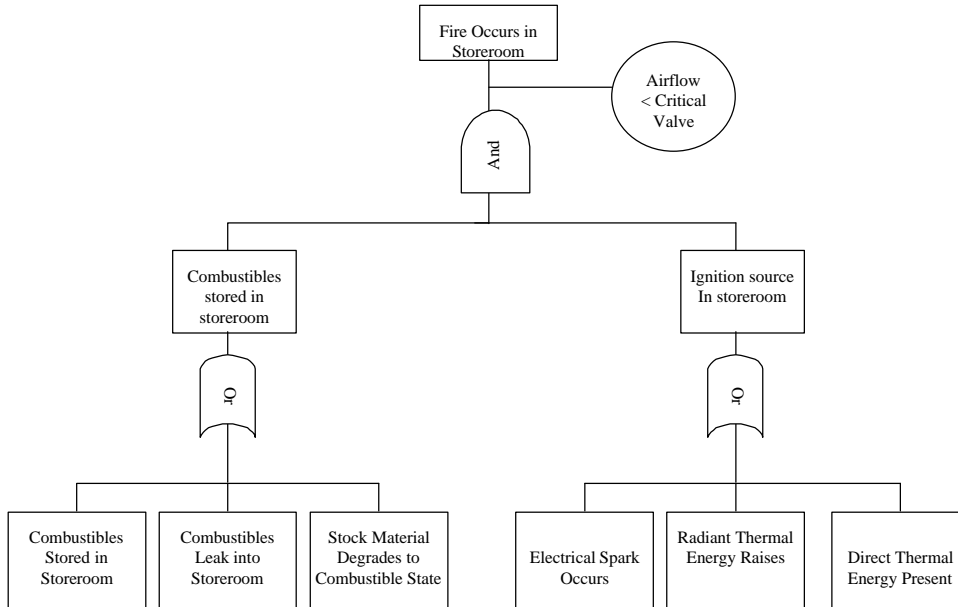


RESOURCES: The System Safety Office is the best source of information regarding Fault Tree Analysis. Like the other advanced tools, the FTA will involve the consultation of a safety professional or engineer trained in the use of the tool. If the probabilistic aspects are added, it will also require a database capable of supplying the detailed data needed.

COMMENTS: The FTA is one of the few hazard identification procedures that will support quantification when the necessary data resources are available.

EXAMPLE: A brief example of the FTA is provided at Figure 1.3.2B. It illustrates how an event may be traced to specific causes that can be very precisely identified at the lowest levels.

Figure 1.3.2B Example of Fault Tree Analysis



1.3.3 THE FAILURE MODES AND EFFECTS ANALYSIS

FORMAL NAME: The Failure Modes and Effects Analysis

ALTERNATIVE NAMES: The FMEA

PURPOSE: The Failure Modes and Effects Analysis (FMEA) is designed to evaluate the impact due to the failure of various system components. A brief example of FMEA illustrating this purpose is the analysis of the impact of the failure of the communications component (radio, landline, computer, etc.) of a system on the overall operation. The focus of the FMEA is on how such a failure could occur (failure mode) and the impact of such a failure (effects).

APPLICATION: The FMEA is generally regarded as a reliability tool but most operational personnel can use the tool effectively. The FMEA can be thought of as a more detailed "What If" analysis. It is especially useful in contingency planning, where it is used to evaluate the impact of various possible failures (contingencies). 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" tool in much greater detail.

METHOD: The FMEA uses a worksheet similar to the one illustrated at Figure 1.3.3A. As noted on the sample worksheet, a specific component of the system to be analyzed is identified. Several components can be analyzed. For example, a rotating part might freeze up, explode, breakup, slow down, or even reverse direction. Each of these failure modes may have differing impacts on connected components and the overall system. The worksheet calls for an assessment of the probability of each identified failure mode.

Figure 1.3.3A Sample Failure Mode and Effects Analysis Worksheet

FAILURE MODES AND EFFECTS ANALYSIS						
Page ___ of ___ Pages						
System _____				Date _____		
Subsystem _____				Analyst _____		
Component Description	Failure Mode	Effects on Other Components	Effects On System	RAC or Hazard Category	Failure Frequency Effects Probability	Remarks

RESOURCES: The best source of more detailed information on the FMEA is the System Safety Office.

EXAMPLES: An example of the FMEA is provided at Figure 1.3.3B.

Figure 1.3.3B Example FMEA

Situation: The manager of a major facility is concerned about the possible impact of the failure of the landline communications system that provides the sole communications capability at the site. The decision is made to do a Failure Modes and Effects Analysis. An extract from the resulting FMEA is shown below.						
Component	Function	Failure Mode & Cause	Failure Effect on Higher Item	System	Probability	Corrective Action
Landline Wire	Comm	Cut-natural cause, falling tree, etc.	Comm system down	Cease Fire	Probable	Clear natural obstacle from around wires

Wire		Cut-unrelated operational activities	Comm system down	Cease Fire	Probable	Warn all operations placement of wire
Wire		Line failure	Comm system down	Cease Fire	Probable	Placement of wires Proper grounding
Wire		Cut – vandals & thieves	Comm system down	Cease Fire	Unlikely	Placement of wires Area security

1.3.4 THE MULTI-LINEAR EVENTS SEQUENCING TOOL

FORMAL NAME: The Multi-linear Events Sequencing Tool

ALTERNATIVE NAMES: The timeline tool, the sequential time event plot (STEP)²

PURPOSE: The Multi-linear Events Sequencing Tool (MES) is a specialized hazard identification procedure designed to detect hazards arising from the time relationship of various operational activities. The MES detects situations in which either the absolute or relative timing of events may create risk. For example, an operational planner may have crammed too many events into a single period of time, creating a task overload problem for the personnel involved. Alternatively, the MES may reveal that two or more events in an operational plan conflict because a person or piece of equipment is required for both but obviously cannot be in two places at once. The MES can be used as a hazard identification tool or as an incident investigation tool.

APPLICATION: The MES is usually considered a loss prevention method, but the MES worksheet simplifies the process to the point that a motivated individual can effectively use it. The MES should be used any time that risk levels are significant and when timing and/or time relationships may be a source of risk. It is an essential tool when the time relationships are relatively complex.

METHOD: The MES uses a worksheet similar to the one illustrated at Figure 4.1. The sample worksheet displays the timeline of the operation across the top and the “actors” (people or things) down the left side. The flow of events is displayed on the worksheet, showing the relationship between the actors on a time basis. Once the operation is displayed on the worksheet, the sources of risk will be evident as the flow is examined.

² K. Hendrisk, and L. Benner, Investigating Accidents with Step, Marcel Dekker, New York, 1988.

Figure 1.3.4A Multi-linear Events Sequencing Form

Timeline	(Time units in seconds or minutes as needed)
Actors	
(People or things involved in the process)	

RESOURCES: The best sources for more detailed information on the MES is the System Safety staff. As with the other advanced tools, using the MES will normally involve consultation with a safety professional familiar with its application.

COMMENTS: The MES is unique in its role of examining the time-risk implications of operations.

1.3.5 THE MANAGEMENT OVERSIGHT AND RISK TREE

FORMAL NAME: The Management Oversight and Risk Tree

ALTERNATIVE NAMES: The MORT

PURPOSE: The Management Oversight and Risk Tree (MORT) uses a series of charts developed and perfected over several years by the Department of Energy in connection with their nuclear safety programs. Each chart identifies a potential operating or management level hazard that might be present in an operation. The attention to detail characteristic of MORT is illustrated by the fact that the full MORT diagram or tree contains more than 10,000 blocks. Even the simplest MORT chart contains over 300 blocks. The full application of MORT is a time-consuming and costly venture. The basic MORT chart with about 300 blocks can be routinely used as a check on the other hazard identification tools. By reviewing the major headings of the MORT chart, an analyst will often be reminded of a type of hazard that was overlooked in the initial analysis. The MORT diagram is also very effective in assuring attention to the underlying management root causes of hazards.

APPLICATION: Full application of MORT is reserved for the highest risks and most operation-critical activities because of the time and expense required. MORT generally requires a specially trained loss control professional to assure proper application.

METHOD: MORT is accomplished using the MORT diagrams, of which there are several levels available. The most comprehensive, with about 10,000 blocks, fills a book. There is an intermediate diagram with about 1500 blocks, and a basic diagram with about 300. It is possible to tailor a MORT diagram by choosing various branches of the tree and using only those segments. The MORT is essentially a negative tree, so the process begins by placing an undesired loss event at the top of the

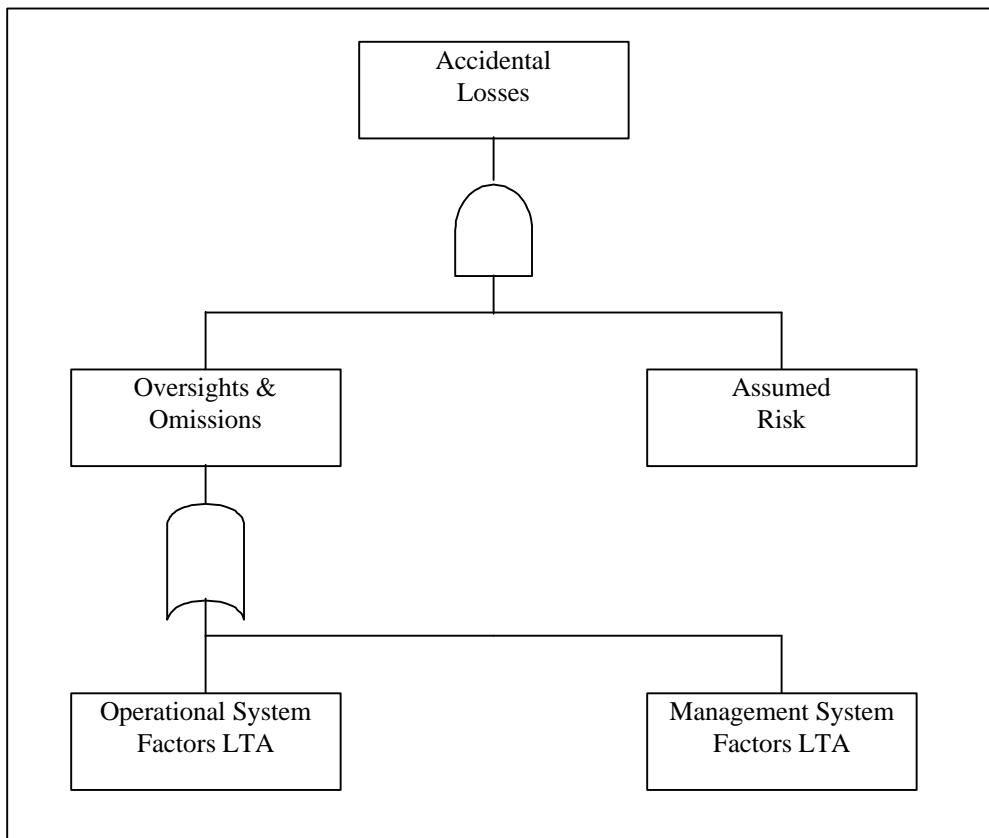
diagram used. The user then systematically responds to the issues posed by the diagram. All aspects of the diagram are considered and the “less than adequate” blocks are highlighted for risk control action.

RESOURCES: The best source of information on MORT is the System Safety Office.

COMMENTS: The MORT diagram is an elaborate negative Logic Diagram. The difference is primarily that the MORT diagram is already filled out for the user, allowing a person to identify the contributory factors for a given undesirable event. Since the MORT is very detailed, as mentioned above, a person can identify basic causes for essentially any type of event.

EXAMPLES: The top blocks of the MORT diagram are displayed at Figure 1.3.5A.

Figure 1.3.5A Example MORT Section



2.0 RISK ASSESSMENT TOOLS, DETAILS, AND EXAMPLES

Introduction. This section contains an example of assessing risk, using a risk assessment matrix (Figure 2). The easiest way to understand the application of the matrix is to apply it. The reasoning used in constructing the matrix in the example below is provided.

Example. The example below demonstrates the application of the matrix to the risk associated with moving a heavy piece of machinery.

Risk to be assessed: The risk of the machine falling over and injuring personnel.

Probability assessment: The following paragraphs illustrate the thinking process that might be followed in developing the probability segment of the risk assessment:

Use previous experience and the database, if available. “We moved a similar machine once before and although it did not fall over, there were some close calls. This machine is not as easy to secure as that machine and has a higher center of gravity and poses an even greater chance of falling. The base safety office indicates that there was an accident about 18 months ago that involved a similar operation. An individual received a broken leg in that case.”

Use the output of the hazard analysis process. “Our hazard analysis shows that there are several steps in the machine movement process where the machine is vulnerable to falling. Furthermore, there are several different types of contributory hazards that could cause the machine to fall. Both these factors increase the probability of falling.”

Consider expert opinion. “My experienced manager feels that there is a real danger of the machine falling”

Consider your own intuition and judgment. “My gut feeling is that there is a real possibility we could lose control of this machine and topple it. The fact that we rarely move machines quite like this one increases the probability of trouble.”

Refer to the matrix terms. “Hmmm, the decision seems to be between *likely* and *occasional*. I understand *likely* to mean that the machine is likely to fall, meaning a pretty high probability. Certainly there is a real chance it may fall, but if we are careful, there should be no problem. I am going to select *Occasional* as the best option from the matrix.”

Severity assessment. The following illustrates the thinking process that might occur in selecting the severity portion of the risk assessment matrix for the machine falling risk:

Identify likely outcomes. “If the machine falls, it will crush whatever it lands on. Such an injury will almost certainly be severe. Because of the height of the machine, it can easily fall on a person’s head and body with almost certain fatal results. There are also a variety of different crushing injuries, especially of the feet, even if the machine falls only a short distance.

Identify the most likely outcomes. “Because of the weight of the machine, a severe injury is almost certain. Because people are fairly agile and the fact that the falling machine gives a little warning that it is falling, death is not likely.”

Consider factors other than injuries. “We identified several equipment and facility items at risk. Most of these we have guarded, but some are still vulnerable. If the machine falls nobody can do any thing to protect these items. It would take a couple of days at least to get us back in full production.”

Refer to the matrix (see Figure 2.1A). “Let’s see, any injury is likely to be severe, but a fatality is not very probable, property damage could be expensive and could cost us a lot of production time. Considering both factors, I think that *critical* is the best choice.”

Combine probability and severity in the matrix. The thinking process should be as follows:

The probability category *occasional* is in the middle of the matrix (refer to the matrix below). I go down until it meets the *critical* category coming from the left side. The result is a *high* rating. I notice that it is among the lower *high* ratings but it is still *high*.”

Figure 2.1A Risk Assessment Matrix

		Probability				
		Frequent	Likely	Occasional	Seldom	Unlikely
		A	B	C	D	E
S E V E R I T Y	Catastrophic I	Extremely				
	Critical II	High	High			
	Moderate III		Medium			
	Negligible IV					Low
		Risk Levels				

Limitations and concerns with the use of the matrix. As you followed the scenario above, you may have noted that there are some problems involved in using the matrix. These include the following:

Subjectivity. There are at least two dimensions of subjectivity involved in the use of the matrix. The first is in the interpretation of the matrix categories. Your interpretation of the term “critical” may be quite different from mine. The second is in the interpretation of the risk. If a few weeks ago I saw a machine much like the one to be moved fall over and crush a person to death, I might have a greater tendency to rate both the probability and severity higher than someone who did not have such an experience. If time and resources permit, averaging the rating of several can reduce this variation personnel.

Inconsistency. The subjectivity described above naturally leads to some inconsistency. A risk rated very high in one organization may only have a high rating in another. This becomes a real problem if the two risks are competing for a limited pot of risk control resources (as they always are). There will be real motivation to inflate risk assessments to enhance competitiveness for limited resources.

3.0 RISK CONTROL OPTION ANALYSIS TOOLS, DETAILS, AND EXAMPLES

3.1 BASIC RISK CONTROL OPTIONS

Major risk control options and examples of each are as follows:

Reject a risk. We can and should refuse to take a risk if the overall costs of the risk exceed its benefits. For example, planner may review the risks associated with a specific particular operation or task. After assessing all the advantages and evaluating the increased risk associated with it, even after application of all available risk controls, he decides the benefits do not outweigh the expected risk costs and it is better off in the long run not doing the operation or task.

Avoiding risk altogether requires canceling or delaying the job, or operation, but is an option that is rarely exercised due to operational importance. However, it may be possible to avoid specific risks: risks associated with a night operation may be avoided by planning the operation for daytime, likewise thunderstorms can be avoided by changing the route of flight.

Delaying a risk. It may be possible to delay a risk. If there is no time deadline or other operational benefit to speedy accomplishment of a risky task, then it is often desirable delay the acceptance of the risk. During the delay, the situation may change and the requirement to accept the risk may go away. During the delay additional risk control options may become available for one reason or another (resources become available, new technology becomes available, etc.) thereby reducing the overall risk.

Risk **transference** does not change probability or severity of the risk, but it may decrease the probability or severity of the risk actually experienced by the individual or organization accomplishing the activity. As a minimum, the risk to the original individual or organization is greatly decreased or eliminated because the possible losses or costs are shifted to another entity.

Risk is commonly **spread** out by either increasing the exposure distance or by lengthening the time between exposure events. Aircraft may be parked so that an explosion or fire in one aircraft will not propagate to others. Risk may also be spread over a group of personnel by rotating the personnel involved in a high-risk operation.

Compensate for a risk. We can create a redundant capability in certain special circumstances. Flight control redundancy is an example of an engineering or design redundancy. Another example is to plan for a back up, and then when a critical piece of equipment or other asset is damaged or destroyed we have capabilities available to bring on line to continue the operation.

Risk can be **reduced**. The overall goal of risk management is to plan operations or design systems that do not contain hazards and risks. However, the nature of most complex operations and systems makes it impossible or impractical to design them completely risk-free. As hazard analyses are performed, hazards will be identified that will require resolution. To be effective, risk management strategies must address the components of risk: probability, severity, or exposure. A proven order of precedence for dealing with risks and reducing the resulting risks is:

Plan or Design for Minimum Risk. From the first, plan the operation or design the system to eliminate risks. Without hazards there is no probability, severity or exposure. If an identified risk cannot be eliminated, reduce the associated risk to an acceptable level. Flight control components can be designed so they cannot be incorrectly connected during maintenance operations as an example.

Incorporate Safety Devices. If identified hazards cannot be eliminated or their associated risk adequately reduced by modifying the operation or system elements or their inputs, that risk should be reduced to an acceptable level through the use of safety design features or devices. Safety devices can effect probability and reduce severity: an automobile seat belt doesn't prevent a collision but reduces the severity of injuries.

Provide Warning Devices. When planning, system design, and safety devices cannot effectively eliminate identified hazards or adequately reduces associated risk, warning devices should be used to detect the condition and alert personnel of the hazard. As an example, aircraft could be retrofitted with a low altitude ground collision warning system to reduce controlled flight into the ground risks. Warning signals and their application should be designed to minimize the probability of the incorrect personnel reaction to the signals and should be standardized. Flashing red lights or sirens are a common warning device that most people understand.

Develop Procedures and Training. Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training should be used. A warning system by itself may not be effective without training or procedures required to respond to the hazardous condition. The greater the human contribution to the functioning of the system or involvement in the operational process, the greater the chance for variability. However, if the system is well designed and the operation well planned, the only remaining risk reduction strategies may be procedures and training. Emergency procedure training and disaster preparedness exercises improve human response to hazardous situations.

In most cases it will not be possible to eliminate safety risk entirely, but it will be possible to significantly reduce it. There are many risk reduction options available. Examples are included in the next section.

3.1.1 THE RISK CONTROL OPTIONS MATRIX

The sample risk control options matrix, illustrated at Figure 3.1.1A, is designed to develop a detailed and comprehensive list of risk control options. These options are listed in priority order of preference, all things being equal, therefore start at the top and consider each option in turn. Add those controls that appear suitable and practical to a list of potential options. Examples of control options for each are suggested in Figure 3.1.1B. Many of the options may be applied at more than one level. For example, the training option may be applied to operators, supervisors, more senior leaders, or staff personnel.

Figure 3.1.1A Sample Risk Control Options Matrix

OPTIONS	OPERATOR	LEADER	STAFF	MGR
ENGINEER (Energy Mgt)				
Limit Energy				
Substitute Safer Form				
Prevent Buildup				
Prevent Release				
Provide Slow Release				

OPTIONS	OPERATOR	LEADER	STAFF	MGR
Rechannel/separate In Time/Space				
Provide Special Maint of Controls				
GUARD				
On Source				
Barrier Between				
On Human or Object				
Raise Threshold (harden)				
IMPROVE TASK DESIGN				
Sequence of Events (Flow)				
Timing (within tasks, between tasks)				
Human-Machine Interface/Ergonomics				
Simplify Tasks				
Reduce Task Loads				
(physical, mental, emotional)				
Backout Options				
LIMIT EXPOSURE				
Number of People or Items				
Time				
Iterations				
SELECTION OF PERSONNEL				
Mental Criteria				
Emotional Criteria				
Physical Criteria				
Experience				
TRAIN AND EDUCATE				
Core Tasks (especially critical tasks)				
Leader Tasks				
Emergency/Contingency Tasks				
Safety Tasks				
Rehearsals				
WARN				
Signs/Color Coding				
Audio/Visual Alarms				
Briefings				
MOTIVATE				
Measurable Standards				
Essential Accountability				
Positive/negative Incentives				
Competition				
Demonstrations of Effects				
REDUCE EFFECTS				
Emergency Equipment				
Rescue Capabilities				

OPTIONS	OPERATOR	LEADER	STAFF	MGR
Emergency Medical Care				
Emergency Procedures				
Damage Control Procedures/Plans				
Backups/Redundant Capabilities				
REHABILITATE				
Personnel				
Facilities/equipment				
Operational Capabilities				

Figure 3.1.1B Example Risk Control Options Matrix

OPTIONS	SOME EXAMPLES
ENGINEER (Energy Mgt.).	
Limit Energy	Lower voltages, small amount of explosives, reduce heights, and reduce speeds
Substitute Safer Form	Use air power, less hazardous chemicals, more stable explosives/chemicals
Prevent Buildup	Use automatic cutoffs, blowout panels, limit momentum, governors
Prevent Release	Containment, double/triple containment
Provide Slow Release	Use pressure relief valves, energy absorbing materials
Rechannel/separate in Time/Space	Automatic processes, deviators, barriers, distance
Provide Special Maint of Controls	Special procedures, special checks/audits
GUARD.	
On Source	Fire suppression systems, energy absorbing systems (crash walls, etc.)
Barrier between	Revetments, walls, distance
On Human or Object	Personal protective equipment, energy absorbing materials
Raise Threshold (harden)	Acclimatization, over-design, reinforcement, physical conditioning
IMPROVE TASK DESIGN.	
Sequence of Events (Flow)	Put tough tasks first before fatigue, don't schedule several tough tasks in a row
Timing (within tasks, between tasks)	Allow sufficient time to perform, to practice. Allow adequate time between tasks
Man-Machine Interface/Ergonomics	Assure equipment fits the people, and effective ergonomic design
Simplify Tasks	Provide job aids, reduce steps, provides tools like lifters communications aids

OPTIONS	SOME EXAMPLES
Reduce Task Loads (physical, mental, emotional)	Set weight limits; automate mental calculations and some monitoring tasks. Avoid excessive stress, provide breaks, vacations, and spread risk among many
Bucket Options	Establish points where process reversal is possible when hazard is detected
LIMIT EXPOSURE.	
Number of People or Items	Only expose essential personnel & things
Time	Minimize the time of exposure -Don't bring the explosives until the last minute
Iterations	Don't do it as often
SELECTION OF PERSONNEL.	
Mental Criteria	Essential basic intelligence, and essential skills and proficiency
Emotional Criteria	Essential stability and maturity
Physical Criteria	Essential strength, motor skills, endurance, size
Experience	Demonstrated performance abilities
TRAIN AND EDUCATE.	
Core Tasks (especially critical tasks)	Define critical minimum abilities, train, test and score
Leader Tasks	Define essential leader tasks and standards, train, test and score
Emergency Contingency Tasks	Define, assign, train, verify ability
Safety Tasks	Hazard identification, risk controls, maintenance of standards
Rehearsals	Validate processes, validate skills, verify interfaces
WARN.	
Signs/Color Coding	Warning signs, instruction signs, traffic signs
Audio/Visual Alarms	Bells, flares, flashing lights, klaxons, whistles
Briefings	Refresher warnings, demonstrate hazards, refresh training
MOTIVATE.	
Measurable Standards	Define minimum acceptable risk controls, see that tasks are assigned
Essential Accountability	Check performance at an essential level of frequency and detail
Positive/negative Incentives	Meaningful individual & group rewards, punishment
Competition	Healthy individual and group competition on a fair basis
Demonstrations of Effects	Graphic, dynamic, but tasteful demonstrations of effects of unsafe acts
REDUCE EFFECTS.	
Emergency Equipment	Fire extinguishers, first aid materials, spill containment materials
Rescue Capabilities	A rescue squad, rescue equipment, helicopter rescue

OPTIONS	SOME EXAMPLES
Emergency Medical Care	Trained first aid personnel, medical facilities
Emergency Damage Control Procedures	Emergency responses for anticipated contingencies, coordinating agencies
Backups/Redundant Capabilities	Alternate ways to continue the operation if primaries are lost
REHABILITATE.	
Personnel	Rehabilitation services restore confidence
Facilities/equipment	Get key elements back in service
Operational Capabilities	Focus on restoration of the operation

4.0 MAKE CONTROL DECISIONS TOOLS, DETAILS, AND EXAMPLES

Introduction. Making control decisions includes the basic options (reject, transfer, spread, etc.) as well as a comprehensive list of risk reduction options generated through use of the risk control options matrix by a decision-maker. The decision-making organization requires a procedure to establish, as a matter of routine, who should make various levels of risk decisions. Finally, after the best available set of risk controls is selected the decision-maker will make a final go/no-go decision.

Developing a decision-making process and system: Risk decision-making should be scrutinized in a risk decision system.

This system will produce the following benefits:

- Promptly get decisions to the right decision-makers
- Create a trail of accountability
- Assure that risk decisions involving comparable levels of risk are generally made at comparable levels of management
- Assure timely decisions
- Explicitly provide for the flexibility in the decision-making process required by the nature of operations.
- A decision matrix is an important part of a good decision-making system. These are normally tied directly to the risk assessment process.

Selecting the best combination of risk controls: This process can be made as simple as intuitively choosing what appears to be the best control or group of controls, or so complex they justify the use of the most sophisticated decision-making tools available. For most risks involving moderate levels of risk and relatively small investments in risk controls, the intuitive method is fully satisfactory. Guidelines for intuitive decisions are:

Don't select control options to produce the lowest level of risk, select the combination yielding the most operational supportive level of risk. This means keeping in mind the need to take risks when those appropriate risks are necessary for improved performance.

Be aware that some risk controls are incompatible. In some cases using risk control A will cancel the effect of risk control B. Obviously using both A and B is wasting resources. For example, a fully

effective machine guard may make it completely unnecessary to use personnel protective equipment such as goggles and face shields. Using both will waste resources and impose a burden on operators.

Be aware that some risk controls reinforce each other. For example, a strong enforcement program to discipline violators of safety rules will be complemented by a positive incentive program to reward safe performance. The impact of the two coordinated together will usually be stronger than the sum of their impacts.

Evaluate full costs versus full benefits. Try to evaluate all the benefits of a risk and evaluate them against all of the costs of the risk control package. Traditionally, this comparison has been limited to comparisons of the incident/accident costs versus the safety function costs.

When it is supportive, choose redundant risk controls to protect against risk in-depth.

Keep in mind the objective is not risk control, it is optimum risk control.

Selecting risk controls when risks are high and risk control costs are important - cost benefit assessment. In these cases, the stakes are high enough to justify application of more formal decision-making processes. All of the tools existing in the management science of decision-making apply to the process of risk decision-making. Two of these tools should be used routinely and deserve space in this publication. The first is cost benefit assessment, a simplified variation of cost benefit analysis. Cost benefit analysis is a science in itself, however, it can be simplified sufficiently for routine use in risk management decision-making even at the lowest organizational levels. Some fiscal accuracy will be lost in this process of simplification, but the result of the application will be a much better selection of risk controls than if the procedures were not used. Budget personnel are usually trained in these procedures and can add value to the application. The process involves the following steps:

Step 1. Measure the full, lifecycle costs of the risk controls to include all costs to all involved parties. For example, a motorcycle helmet standard should account for the fact that each operator will need to pay for a helmet.

Step 2. Develop the best possible estimate of the likely lifecycle benefits of the risk control package to include any non-safety benefits expressed as a dollar estimate. For example, an ergonomics program can be expected to produce significant productivity benefits in addition to a reduction in cumulative trauma injuries.

Step 3. Let your budget expert's fine-tune your efforts.

Step 4. Develop the cost benefit ratio. You are seeking the best possible benefit-to-cost ratio but at least 2 to 1.

Step 5. Fine-tune the risk control package to achieve an improved "bang for the buck". The example at Figure 4.1A illustrates this process of fine-tuning applied to an ergonomics-training course (risk control).

Figure 4.1A Example Maximizing Bang for the Buck

Anyone can throw money at a problem. A manager finds the optimum level of resources producing an optimum level of effectiveness, i.e. maximum bang for the buck. Consider an ergonomics-training program involving training 400 supervisors from across the entire organization in a 4-hour (3 hours training, 1-hour admin) ergonomics-training course that will cost \$30,500 including student time. Ergonomics losses have been averaging \$300,000 per year and estimates are that the risk control will reduce this loss by 10% or \$30,000. On the basis of a cost benefit assessment over the next year (ignoring any out year considerations), this risk control appears to have a one year negative cost benefit ratio i.e. \$30,000 in benefit, versus a \$30,500 investment, a \$500 loss.

Apparently it is not a sound investment on a one-year basis. This is particularly true when we consider that most decision-makers will want the comfort of a 2 or 3 to 1 cost benefit ratio to insure a positive outcome. Can this project be turned into a winner?

We can make it a winner if able to access risk information concerning ergonomics injuries/illnesses from loss control office data, risk management concepts, and a useful tool called "Pareto's Law".

Pareto's Law, as previously mentioned, essentially states that 80% of most problems can be found in 20% of the exposure. For example, 80% of all traffic accidents might involve only 20% of the driver population. We can use this law, guided by our injury/illness data, to turn the training program into a solid winner. Here is what we might do.

Step 1. Let's assume that Pareto's Law applies to the distribution of ergonomics problems within this organization. If so, then 80% of the ergonomics problem can be found in 20% of our exposures. Our data can tell us which 20%. We can then target the 20% (80 students) of the original 400 students that are accounting for 80% of our ergonomics costs (\$240,000).

Step 2. Lets also assume that Pareto's Law applies to the importance of tasks that we intend to teach in the training course. If the three hours of training included 10 tasks, lets assume that two of those tasks (20%) will in fact account for 80% of the benefit of the course. Again our data should be able to indicate this. Lets also assume that by good luck, these two tasks only take the same time to teach as the other eight. We might now decide to teach only these two tasks which will require only 36 minutes (20% of 180 minutes). We will still retain 80% of the \$240,000 target value or \$192,000.

Step 3. Since the training now only requires 36 minutes, we will modify our training procedure to conduct the training in the workshops rather than in a classroom. This reduces our admin time from 1 hour (wash up, travel, get there well before it actually starts, and return to work) to 4 minutes. Our total training time is now 40 minutes.

Summary. We are still targeting \$192,000 of the original \$300,000 annual loss but our cost factor is now 80 employees for 40 minutes at \$15/hour, with our teaching cost cut to 1/5th of the \$6000 (80 students instead of 400) which is \$1200. We still have our staff cost so the total cost of the project is now \$2500. We will still get the 10% reduction in the remaining \$192,000 that we are still targeting, which totals \$19,200. Our cost benefit ratio is now a robust 7.68 to 1. If all goes well with the initial training and we actually demonstrate at 20% loss reduction, we may choose to expand the training to the next riskiest 20% of our 400 personnel which should also produce a very positive return.

Selecting risk controls when risks are high and risk control costs are important - use of decision matrices. An excellent tool for evaluating various risk control options is the decision matrix. On the vertical dimension of the matrix we list the operation supportive characteristics we are looking for in risk controls. Across the top of the matrix we list the various risk control options (individual options or packages of options). Then we rank each control option on a scale of 1 (very low) to 10 (very high) in each of the desirable characteristics. If we choose to, we can weight each desirable characteristic based on its operational significance and calculate the weighted score (illustrated below). All things being the same, the options with the higher scores are the stronger options. A generic illustration is provided at Figure 4.1B.

Figure 4.1B Sample Decision Matrix

RATING FACTOR	WEIGHT*	RISK CONTROL OPTIONS/PACKAGES					
		#1	#2	#3	#4	#5	#6
Low Cost	5	9/45	6/30	4/20	5/25	8/40	8/40
Easy to implement	4	10/40	7/28	5/20	6/24	8/32	8/32
Positive Operator involvement	5	8/40	2/10	1/5	6/30	3/15	7/35
Consistent with Culture	3	10/30	2/6	9/27	6/18	6/18	6/18
Easy to integrate	3	9/27	5/15	6/18	7/21	6/18	5/15
Easy to measure	2	10/20	10/20	10/20	8/16	8/16	5/10
Low risk (sure to succeed)	3	9/27	9/27	10/30	2/6	4/12	5/15
	TOTALS	229	136	140	140	151	165
* Weighting is optional and is designed to reflect the relative importance of the various factors.							

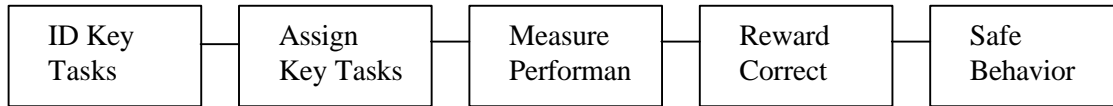
Summary. It is not unusual for a risk control package to cost hundreds of thousands of dollars and even millions over time. Millions of dollars and critical operations may be at risk. The expenditure of several tens of thousands of dollars to get the decision right is sound management practice and good risk management.

5.0 RISK CONTROL IMPLEMENTATION TOOLS AND DETAILS

5.1 Introduction

Figure 5.1A summarizes a Risk Control Implementation model. It is based on accountability being an essential element of risk management success. Organizations and individuals must be held accountable for the risk decisions and actions that they take or the risk control motivation is minimized. The model depicted at Figure 5.1A is the basis of positive accountability and strong risk control behavior.

Figure 5.1A Implementation Model



5.2 Applying the model

The example below illustrates each step in the model applied to the sometimes-difficult task of assuring that personnel consistently wear and use their protective clothing and equipment. The steps of the model should be applied as follows:

5.2.1 Identify key tasks

This step, while obvious however, is critical to actually define the key tasks with enough accuracy that effective accountability is justified. For example, in our example regarding use of protective clothing and equipment, it is essential to identify exactly when the use of such items is required. Is it when I enter the door of a work area? When I approach a machine? How close? What about on the loading dock? Exactly what items are to be worn? Is there any specific way that they should be worn? I can be wearing ear plugs but incorrectly have them stuck in the outer ear, producing little or no noise reduction benefit. Does this meet the requirement? The task needs to be defined with sufficient precision that personnel know what is expected of them and that what is expected of them produces the risk control desired. It is also important that the task be made as simple, pleasant, and trouble free as possible. In this way we significantly increase the ease with which the rest of the process proceeds.

5.2.2 Assign key tasks

Personnel need to know clearly what is expected of them especially if they are going to be held accountable for the task. This is normally not difficult. The task can be included in job descriptions, operating instructions, or in the task procedures contained in manuals. It can be very effectively be embedded in training. In less structured situations, it can be a clear verbal order or directive. It is important that the assignment of the task include the specifics of what is expected.

5.2.3 Measure performance

The task needs to include at least a basic level of measurement. It is important to note that measurement does not need to include every time the behavior is displayed. It is often perfectly practical to sample performance only once in large number of actions, perhaps as few as one in several hundred actions as long as the sample is a random example of routine behavior. Often the only one who needs to do the measuring is the individual responsible for the behavior. In other situations, the supervisor or an outside auditor may need to do the observing. Performance is compared to the standard, which should have been

communicated to the responsible individual. This step of the process is the rigorous application of the old adage that “What is monitored (or measured) and checked gets done.”

5.2.4 Reward correct behavior and correct inadequate behavior

The emphasis should clearly be on reinforcing correct behavior. Reinforcement means any action that increases the likelihood that the person will display the desired behavior again. It can be as informal as a pat on the back or as formal as a major award or cash incentive. Correcting inadequate behavior should be done whenever inadequate behavior is observed. The special case of *punishment* should only be used when all other means of producing the desired behavior have failed.

5.2.5 Risk control performance

If the steps outlined above have been accomplished correctly, the result will be consistent success in controlling risk. Note that the unpleasantness of the task will dictate the extent of the rewards and corrective actions required. The harder the task for whatever reason, the more powerful the rewards and corrective actions needed will be. It is important to make risk control tasks as uncomplicated, and pleasant as possible.

6.0 SUPERVISE AND REVIEW DETAILS AND EXAMPLES

Management involves moving a task or an organization toward a goal. To move toward a goal you must have three things. You must have a goal, you must know where you are in relation to that goal, and you must have a plan to reach it. An effective set of risk matrices provides two of the elements.

In regard to ORM, indicators should provide information concerning the success or lack of success of controls intended to mitigate a risk. These indicators could focus on those key areas identified during the assessment as being critical to minimizing a serious risk area. Additionally, matrices may be developed to generically identify operations/areas where ORM efforts are needed.

A representative set of risk measures that a maintenance shop leader could use to assess the progress of his shop toward the goal of improving safety performance. Similar indicators could be developed in the areas of environment, fire prevention, security, and other loss control areas.

The tool control effectiveness index. Establish key indicators of tool control program effectiveness (percentage of tool checks completed, items found by QA, score on knowledge quiz regarding control procedures, etc.). All that is needed is a sampling of data in one or more of these areas. If more than one area is sampled, the scores can be weighted if desired and rolled up into a single tool control index by averaging them. See Figure 6.1A for the example.

Figure 6.1A Example Tool Control Effectiveness Measurement

The percent of tool checks completed is 94%.
Items found by QA. Items were found in 2% of QA inspections (98% were to standard).
Tool control quiz score is 88%.
If all items are weighted equally ($94+98+88$ divided by $3 = 93.3$) then 93.3 is this quarter's tool control safety index. Of course, in this index, high scores are desirable.

The protective clothing and equipment risk index. Shop personnel are using this index measures the effectiveness with which required protective clothing and equipment. Making spot observations periodically during the workday collects data. Data are recorded on a check sheet and are rolled-up monthly. The index is the percent safe observations of the total number of observations made as illustrated at Figure 6.1B.

Figure 6.1B Example Safety Observation Measurement

TOTAL OBSERVATIONS: 27 SAFE OBSERVATIONS: 21

The protective clothing and equipment safety index is 78 (21 divided by 27 = 78%).
In this index high scores are desirable

The emergency procedures index. This index measures the readiness of the shop to respond to various emergencies such as fires, injuries, and hazmat releases. It is made up of a compilation of indicators as shown at Figure 6.1C A high score is desirable.

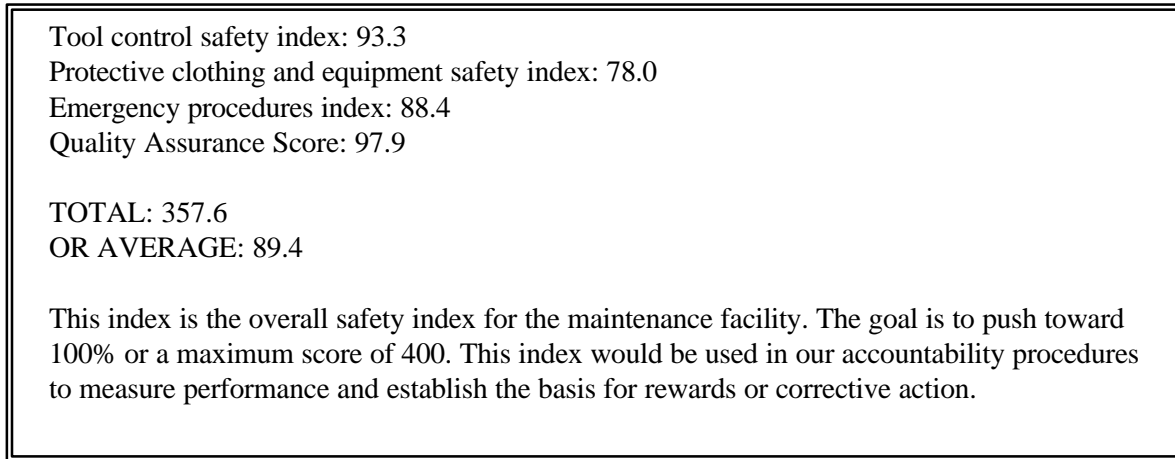
Figure 6.1C Example Emergency Procedures Measurement

Scores on emergency procedure quizzes
Percentage of emergency equipment on hand and fully operational
Scores on emergency response drills indicating speed, correct procedures, and other effectiveness indicators

The quality assurance score. This score measures a defined set of maintenance indicators tailored to the particular type of aircraft serviced. Quality Assurance (QA) personnel record deviations in these target areas as a percentage of total observations made. The specific types of deviations are noted. The score is the percentage of positive observations with a high score being desirable. Secondary scores could be developed for each type of deviation if desired.

The overall index. Any combination of the indicators previously mentioned, along with others as desired, can be rolled up into an overall index for the maintenance facility as illustrated at Figure 6.1D.

Figure 6.1D Example Overall Measurement



Once the data has been collected and analyzed, the results need to be provided to the unit. With this information the unit will be able to concentrate their efforts on those areas where improvement would produce the greatest gain.

Summary. It is not difficult to set up useful and effective measures of operational risk, particularly once the key risks have been identified during a risk assessment. Additionally, the workload associated with such indicators can be minimized by using data already collected and by collecting the data as an integrated routine aspect of operational processes.