ENGINEERING-PDH.com
ONLINE CONTINUING EDUCATION

ACCIDENT & OPERATIONAL SAFETY ANALYSIS - VOL 1 OF 2 - FUNDAMENTAL CONCEPTS

Main Category:	Project Management
Sub Category:	-
Course #:	PRJ-124
Course Content:	50 pgs
PDH/CE Hours:	5

OFFICIAL COURSE/EXAM

(SEE INSTRUCTIONS ON NEXT PAGE)

WWW.ENGINEERING-PDH.COM
TOLL FREE (US & CA): 1-833-ENGR-PDH (1-833-364-7734)
SUPPORT@ENGINEERING-PDH.COM

PRJ-124 EXAM PREVIEW

- TAKE EXAM! -

Instructions:

- At your convenience and own pace, review the course material below. When ready, click "Take Exam!" above to complete the live graded exam. (Note it may take a few seconds for the link to pull up the exam.) You will be able to re-take the exam as many times as needed to pass.
- Upon a satisfactory completion of the course exam, which is a score of 70% or better, you will be provided with your course completion certificate. Be sure to download and print your certificates to keep for your records.

Exam Preview:

1. An accident model is the frame of reference, or stereotypical way of thinking about an accident, that are used in trying to understand how an accident happen.
    a. True
    b. False
2. The Domino Theory of Accident Causation developed by H.W. Heinrich in ____ is an example of a sequence of events model.
    a. 1927
    b. 1929
    c. 1935
    d. 1931
3. According to the reference material, a major benefit of the epidemiological model is that it provides a more complete understanding of the subtle interactions that contributed to the event.
    a. True
    b. False
4. According to the reference material, which popular game is an excellent metaphor for describing the complex, non-linear accident model?
    a. Connect 4
    b. Jenga
    c. Twister
    d. Suspend

5. Using Figure 1-3: Error Precursors, which of the following error precursors belongs to the Individual Capabilities category of the TWIN Analysis Matrix?
    a. Lack of or unclear standards
    b. Inaccurate risk perception
    c. Unsafe attitudes
    d. Distractions/interruptions
6. According to the reference material, there are three fundamental types of accidents which DOE seeks to avoid; individual, workplace, and system accidents.
    a. True
    b. False
7. Organizations left untended trend in the direction of disorder. In the safety literature this phenomenon is referred to as organizational drift. Which level of organizational drift examines issues at the physics level - Break-the-Chain Framework (BTC)?
    a. Level 1
    b. Level 2
    c. Level 3
    d. Level 4
8. The High Level Model for examining organizational drift, shown in Figure 1-13, was adapted from work by the Institute of Nuclear Power Operations (INPO). Using this model and the reference material, what is the first step of analysis for DOE sites?
    a. Job-Site Conditions
    b. Worker Behavior
    c. Operational Results
    d. Organizational Processes and Values
9. According to the reference material, a healthy culture exists when the "work-as-done" (culture artifacts and behavior) overlap the "work-as-planned" (espoused beliefs and values) indicating an alignment with the underlying assumptions (those factors felt important to management).
    a. True
    b. False
10. Using the Glossary of the reference material, which of the following terms matches the description: A designated authority responsible for assigning Accident Investigation Boards for investigations, with responsibilities as prescribed in DOE O 225.1B?
    a. Head of Field Elements
    b. Appointing Official
    c. Board Chairperson
    d. DOE Accident Investigator

ACCIDENT & OPERATIONAL SAFETY ANALYSIS PART 1: FUNDAMENTAL CONCEPTS

Table of Contents

CHAPTER 1

1. Fundamentals

This chapter discusses fundamental concepts of accident dynamics, accident prevention, and accident analysis. The purpose of this chapter is to emphasize that accident investigators and improvement analysts need to understand the theoretical bases of safety management and accident analysis, and the practical application of the Integrated Safety Management (ISM) framework. This provides investigators the framework to get at the relevant facts, surmise the appropriate causal factors and to understand those organizational factors that leave the organization vulnerable for future events with potentially worse consequences.

1.1 Definition of an Accident

Accidents are unexpected events or occurrences that result in unwanted or undesirable outcomes. The unwanted outcomes can include harm or loss to personnel, property, production, or nearly anything that has some inherent value. These losses increase an organization's operating cost through higher production costs, decreased efficiency, and the long-term effects of decreased employee morale and unfavorable public opinion.

How then may safety be defined? Dr. Karl Weick has noted that safety is a "dynamic non-event." Dr. James Reason offers that "safety is noted more in its absence than its presence." Scholars of safety science and organizational behavior argue, often to the chagrin of designers, that safety is not an inherent property of well designed systems. To the contrary Prof. Jens Rasmussen maintains that "the operator's role is to make up for holes in designers 'work'." If the measurement of safety is that nothing happens, how does the analyst then understand how systems operate effectively to produce nothing? In other words, since accidents are probabilistic outcomes, it is the challenge to determine by evidence if the absence of accidents is by good design or by lucky chance. Yet, this is the job of the accident investigator, safety scientists and analysts.

1.2 The Contemporary Understanding of Accident Causation

The basis for conducting any occurrence investigation is to understand the organizational, cultural or technical factors that left unattended could result in future accidents or unacceptable mission interruption or quality concerns. Guiding concepts may be summarized as follows:

- Within complex systems human error does not emanate from the individual but is a bi-product or symptom of the ever present latent conditions built into the complexity of organizational culture and strategic decision-making processes.

- The triggering or initiating error that releases the hazard is only the last in a network of errors that often are only remotely related to the accident. Accident occurrences emerge

from the organization's complexity, taking many factors to overcome systems' network of barriers and allowing a threat to initiate the hazard release.

- Investigations require delving into the basic organizational processes: designing, constructing, operating, maintaining, communicating, selecting, and training, supervising, and managing that contain the kinds of latent conditions most likely to constitute a threat to the safety of the system.

- The inherent nature of organizational culture and strategic decision-making means latent conditions are inevitable. Systems and organizational complexity means not all problems can be solved in one pass. Resources are always limited and safety is only one of many competing priorities. Therefore, event investigators should target the latent conditions most in need of urgent attention and make them visible to those who manage the organization so they can be corrected. [Hollnagel, 2004][10] [Dekker, 2011][11] [Reiman and Oedewald, 2009][12]

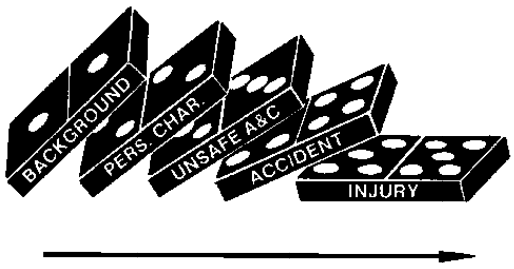
1.3 Accident Models – A Basic Understanding

An accident model is the frame of reference, or stereotypical way of thinking about an accident, that are used in trying to understand how an accident happened. The frame of reference is often an unspoken, but commonly held understanding, of how accidents occur. The advantage is that communication and understanding become more efficient because some things (e.g., common terminology, common experiences, common points-of-reference, or typical sequences) can be taken for granted. The disadvantage is that it favors a single point of view and does not consider alternate explanations (i.e., the hypothesis model creates a recognized solution, causing the user to discard or ignore information inconsistent with the model). This is particularly important when addressing human component because preconceived ideas of how the accident occurred can influence the investigators' assumptions of the peoples' roles and affect the line of questioning. [Hollnagel, 2004][10]

What investigators look for when trying to understand and analyze an accident depends on how it is believed an accident happens. A model, whether formal or simply what you believe, is extremely helpful because it brings order to a confusing situation and suggests ways you can explain relationships. But the model is also constraining because it views the accident in a particular way, to the exclusion of other viewpoints. Accident models have evolved over time and can be characterized by the three models below. [Hollnagel, 2004][10]

1.3.1 Sequence of Events Model

This is a simple, linear cause and effect model where accidents are seen the natural culmination of a series of events or circumstances, which occur in a specific and recognizable order. The model is often represented by a chain with a weak link or a series of falling dominos. In this model, accidents are prevented by fixing or eliminating the weak link, by removing a domino, or placing a barrier between two



dominos to interrupt the series of events. The Domino Theory of Accident Causation developed by H.W. Heinrich in 1931 is an example of a sequence of events model. [Heinrich, 1931][13]

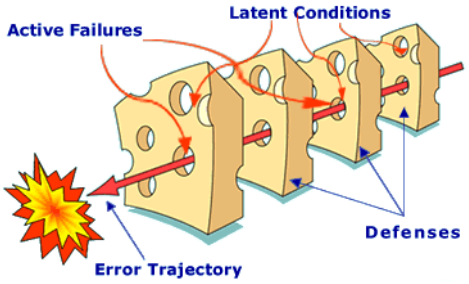
The sequential model is not limited to a simple series and may utilize multiple sequences or hierarchies such as event trees, fault trees, or critical path models. Sequential models are attractive because they encourage thinking in causal series, which is easier to represent graphically and easier to understand. In this model, an unexpected event initiates a sequence of consequences culminating in the unwanted outcome. The unexpected event is typically taken to be an unsafe act, with human error as the predominant cause.

The sequential model is also limited because it requires strong cause and effect relationships that typically do not exist outside the technical or mechanistic aspect of the accident. In other words, true cause and effect relationships can be found when analyzing the equipment failures, but causal relationships are extremely weak when addressing the human or organizational aspect of the accident. For example: While it is easy to assert that "time pressure caused workers to take shortcuts," it is also apparent that workers do not always take shortcuts when under time pressure. See Section 1.4, Cause and Effect Relationships.

In response to large scale industrial accidents in the 1970's and 1980's, the epidemiological models were developed that viewed an accident the outcome of a combination of factors, some active and some latent, that existed together at the time of the accident. [Hollnagel, 2004][10]

1.3.2 Epidemiological or Latent Failure Model

This is a complex, linear cause and effect model where accidents are seen as the result of a combination of active failures (unsafe acts) and latent conditions (unsafe conditions). These are often referred to as epidemiological models, using a medical metaphor that likens the latent conditions to pathogens in the human body that lay dormant until triggered by the unsafe act. In this model, accidents are prevented by strengthening barriers and defenses. The "Swiss Cheese" model developed by James Reason is an example of the epidemiological model. [Reason, 1997][14]



This model views the accident to be the result of long standing deficiencies that are triggered by the active failures. The focus is on the organizational contributions to the failure and views the human error as an effect, instead of a cause.

The epidemiological models differ from the sequential models on four main points:

- Performance Deviation – The concept of unsafe acts shifted from being synonymous with human error to the notion of deviation from the expected performance.

- Conditions – The model also considers the contributing factors that could lead to the performance deviation, which directs analysis upstream from the worker and process deviations.

- Barriers – The consideration of barriers or defenses at all stages of the accident development.

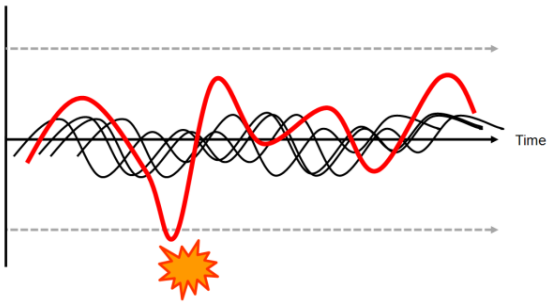
- Latent Conditions – The introduction of latent or dormant conditions that are present within the system well before there is any recognizable accident sequence.

The epidemiological model allows the investigator to think in terms other than causal series, offers the possibility of seeing some complex interaction, and focuses attention on the organizational issues. The model is still sequential, however, with a clear trajectory through the ordered defenses. Because it is linear, it tends to oversimplify the complex interactions between the multitude of active failures and latent conditions.

The limitation of epidemiological models is that they rely on "failures" up and down the organizational hierarchy, but does nothing to explain why these conditions or decisions were seen as normal or rational before the accident. The recently developed systemic models start to understand accidents as unexpected combinations of normal variability. [Hollnagel, 2004][10] [Dekker, 2006][15]

1.3.3 Systemic Model

This is a complex, non-linear model where both accidents (and success) are seen to emerge from unexpected combinations of normal variability in the system. In this model, accidents are triggered by unexpected combinations of normal actions, rather than action failures, which combine, or resonate, with other normal variability in the process to produce the necessary and jointly sufficient conditions for failure to succeed. Because of the complex, non-linear nature of this model, it is difficult to represent graphically. The Functional Resonance model from Erik Hollnagel uses a signal metaphor to visualize this model with the undetectable variabilities unexpectedly resonating to result in a detectable outcome.



The Jenga™ game is also an excellent metaphor for describing the complex, non-linear accident model. Every time a block is pulled from the stack, it has subtle interactions with the other blocks that cause them to loosen or tighten in the stack. The missing blocks represent the sources of variability in the process and are typically described as organizational weaknesses or latent conditions. Realistically, these labels are applied retrospectively only after what was seen as normal before the accident, is seen as having contributed to the event, but only in combination with other factors. Often, the

worker makes an error or takes an action that seems appropriate, but when combined with the other variables, brings the stack crashing down. The first response is to blame the worker because his action demonstrably led to the failure, but it must be recognized that without the other missing blocks, there would have been no consequence.

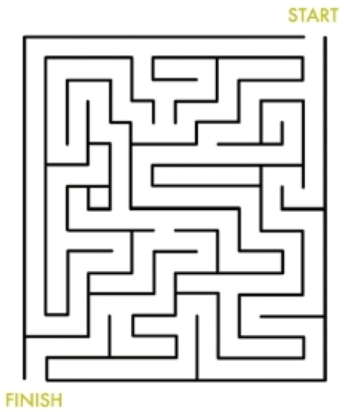
A major benefit of the systemic model is that it provides a more complete understanding of the subtle interactions that contributed to the event. Because the model views accidents as resulting from unexpected combinations of normal variability, it seeks an understanding of how normal variability combined to create the accident. From this understanding of contributing interactions, latent conditions or organizational weaknesses can be identified.

1.4 Cause and Effect Relationships

Although generally accepted as the overarching purpose of the investigation, the identification of causes can be problematic. Causal analysis gives the appearance of rigor and the strenuous application of time-tested methodologies, but the problem is that causality (i.e., a cause-effect relationship) is often constructed where it does not really exist. To understand how this happens, we need to take a hard look at how accidents are investigated, how cause – effect relationships are determined, and the requirements for a true cause - effect relationship.

1.4.1 Investigations Look Backwards

The best metaphor for how accidents are investigated is a simple maze. If a group of people are asked to solve the maze as quickly as possible and ask the "winners" how they did it, invariably the answer will be that they worked it from the Finish to the Start. Most mazes are designed to be difficult working from the Start to the Finish, but are simple working from the Finish to the Start. Like a maze, accident investigations look backwards. What was uncertain for the people working forward through the maze becomes clear for the investigator looking backwards.



Because accident investigations look backwards, it is easy to oversimplify the search for causes. Investigators look backwards with the undesired outcome (effect) preceded by actions, which is opposite of how the people experienced it (actions followed by effects). When looking for cause - effect relationships (and there many actions taking place along the timeline), there are usually one or more actions or conditions before the effect (accident) that seem to be plausible candidates for the cause(s).

There are some common and mostly unavoidable problems when looking backwards to find causality. As humans, investigators have a strong tendency to draw conclusions that are not logically valid and which are based on educated guesses, intuitive judgment, "common sense", or other heuristics, instead of valid rules of logic. The use of event timelines, while beneficial in understanding the event, creates sequential relationships that seem to infer causal relationships. A quick Primer on cause and effect may help to clarify.

1.4.2 Cause and Effect are Inferred

Cause and effect relationships are normally inferred from observation, but are generally not something that can be observed directly.

Normally, the observer repeatedly observes Action A, followed by Effect B and conclude that B was caused by A. It is the consistent and unwavering repeatability of the cause followed by the effect that actually establishes a true cause – effect relationship.

For example: Kink a garden hose (action A), water flow stops (effect B), conclusion is kinking garden hose causes water to stop flowing. This cause and effect relationship is so well established that the person will immediately look for a kink in the hose if the flow is interrupted,

Accident investigations, however, involve the notion of backward causality, i.e., reasoning backward from Effect to Action.

The investigator observes Effect B (the bad outcome), assumes that it was caused by something and then tries to find out which preceding Action was the cause of it. Lacking the certainty of repeatability (unless the conditions are repeated) and a causal relationship can only be assumed because it seems plausible. [Hollnagel, 2004][10]

1.4.3 Establishing a Cause and Effect Relationship

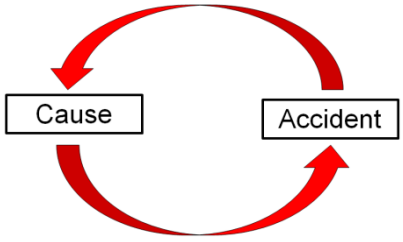
A true cause and effect relationship must meet these requirements:

- The cause must precede the effect (in time).
- The cause and effect must have a necessary and constant connection between them, such that the same cause always has the same effect.

This second requirement is the one that invalidates most of the proposed causes identified in accident investigations. As an example, a cause statement such as "the accident was due to inadequate supervision" cannot be valid because the inadequate supervision does not cause accidents all the time. This type of cause statement is generally based on the simple "fact" that the supervisor failed to prevent the accident. There are generally some examples, such as not spending enough time observing workers, to support the conclusion, but these examples are cherry-picked to support the conclusion and are typically value judgments made after the fact. [Dekker, 2006][15]

1.4.4 The Circular Argument for Cause

The example (inadequate supervision) above is what is generally termed a "circular argument." The statement is made that the accident was caused by "inadequate XXX." But when challenged as to why it was judged to be inadequate, the only evidence is that it must be inadequate because the accident happened. The circular argument is usually evidenced by the use of negative descriptors such



as inadequate, insufficient, less than adequate, poor, etc. The Accident Investigation Board (AIB) needs to eliminate this type of judgmental language and simply state the facts. For example, the fact that a supervisor was not present at the time of the accident can be identified as a contributing factor, although it is obviously clear that accidents do not happen every time a supervisor is absent.

True cause and effect relationships do exist, but they are almost always limited to the mechanistic or physics-based aspects of the event. In a complex socio-technical system involving people, processes and programs, the observed effects are uaually emergent phenomena due to interactions within the system rather than resultant phenomena due to cause and effect.

With the exception of physical causes, such as a shorted electrical wire as the ignition source for a fire, causes are not found; they are constructed in the mind of the investigator. Since accidents do happen, there are obviously many factors that contribute to the undesired outcome and these factors need to be addressed. Although truly repeatable cause and effect relationships are almost impossible to find, many factors that seemed to have contributed to the outcome can be identified. These factors are often identified by missed opportunities and missing barriers which get miss labeled as causes. Because it is really opinion, sufficient information needs to be assembled and presented in a form that makes the rationale of that opinion understandable to others reviewing it.

The investigation should focus on understanding the context of decisions and explaining the event. In order to understand human performance, do not limit yourself to the quest for causes. An explanation of why people did what they did provides a much better understanding and with understanding comes the ability to develop solutions that will improve operations.

1.4.5 Counterfactuals

Using the maze metaphor, what was complex, with multiple paths and unknown outcomes for the workers, becomes simple and obvious for the investigator. The investigator can easily retrace the workers path through the maze and see where they chose a path that led to the accident rather than one that avoided the accident. The result is a counterfactual (literally, counter the facts) statement of what people should or could have done to avoid the accident. The counterfactual statements are easy to identify because they use common phrases like:

- “they could have …”
- “they did not …”
- “they failed to …”
- “if only they had …”

The problem with counterfactuals is that they are a statement of what people did not do and does not explain why the workers did what they did do. Counterfactuals take place in an alternate reality that did not happen and basically represent a list of what the investigators wish had happened instead.

Discrepancies between a static procedure and actual work practices in a dynamic and ever changing workplace are common and are not especially unique to the circumstances involved in the accident. Discrepancies are discovered during the investigation simply because considerable effort was expended in looking for them, but they could also be found throughout the organization where an accident has not occurred. This does not mean that counterfactual statements should be discounted. They can be essential to understanding why the decisions the worker made and the actions (or no actions) that the worker took were seen as the best way to proceed. [Dekker, 2006][15]

1.5 Human Performance Considerations

In order to understand human performance, do not limit yourself to the quest for causes. The investigation should focus on understanding the context of decisions and explaining the event. An explanation of why people did what they did provides a much richer understanding and with understanding comes the ability to develop solutions that will improve operations.

The safety culture maturity model from the International Atomic Energy Agency (IAEA) provides the basis for an improved understanding the human performance aspect of the accident investigation. IAEA TECDOC 1329, *Safety Culture in Nuclear Installations: Guidance for Use in the Enhancement of Safety Culture*, was developed for use in IAEA's Safety Culture Services to assist their Member States in their efforts to develop a sound safety culture. Although the emphasis is on the assessment and improvement of a safety culture, the introductory sections, which lay the groundwork for understanding safety culture maturity, provide a framework to understand the environment which forms the organization's human performance.

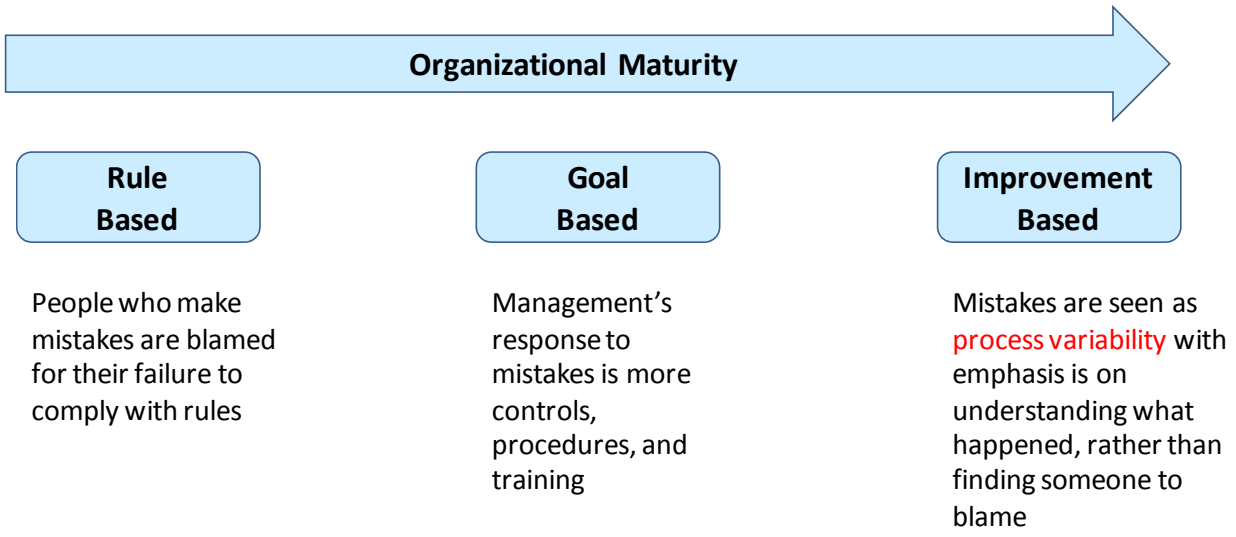


Figure 1-1: IAEA-TECDOC-1329 – Safety Culture in Nuclear Installations

The model (Figure 1-1) defines three levels of safety culture maturity and presents characteristics for each of the maturity levels based on the underlying beliefs and assumptions. The concept is illustrated below with the characteristics for how the organization responds to an accident.

- **Rule Based** –Safety is based on rules and regulations. Workers who make mistakes are blamed for their failure to comply with the rules.

- **Goal Based** –Safety becomes an organizational goal. Management's response to mistakes is to pile on more broadly enforced controls, procedures and training with little or no performance rationale or basis for the changes.

- **Improvement Based** –The concept of continuous improvement is applied to safety. Almost all mistakes are viewed in terms of process variability, with the emphasis placed on understanding what happened rather than finding someone to blame, and a targeted response to fix the underlying factors.

When an accident occurs that causes harm or has the potential to cause harm, a choice exists: to vector forward on the maturity model and learn from the accident or vector backwards by blaming the worker and increasing enforcement. In order to do no harm, accident investigations need to move from the rule based response, where workers are blamed, to the improvement based response where mistakes are seen as process variability needing improvement.

1.5.1 Bad Apples

The Bad Apple Theory is based on the belief that the system in which people work is basically safe and worker errors and mistakes are seen as the cause of the accident. An investigation based on this belief focuses on the workers' bad decisions or inappropriate behavior and deviation from written guidance, with a conclusion that the workers failed to adhere to procedures. Because the supervisor's role is seen as enforcing the rules, the investigation will often focus on supervisory activities and conclude that the supervisor failed to adequately monitor the worker's performance and did not correct noncompliant behavior. [Dekker, 2002][16]

From the investigation perspective, knowing what the outcome was creates a hindsight bias which makes it difficult to view the event from the perspective of the worker before the accident. It is easy to blame the worker and difficult to look for weaknesses within the organization or system in which they worked. The pressure to find an obvious cause and quickly finish the investigation can be overpowering.

1.5.2 Human Performance Modes – Cognitive Demands

People are fallible, even the best people make mistakes. This is the first principle of Human Performance Improvement and accident investigators need to understand the nature of the error to determine the appropriate response to the error. Jen Rasmussen developed a classification of the different types of information processing involved in industrial tasks. Usually referred to as performance modes, these three classifications describe how the worker's mind is processing information while performing the task. (Figure 1-2) The three performance modes are:

- **Skill mode** - Actions associated with highly practiced actions in a familiar situation usually executed from memory. Because the worker is highly familiar with the task, little attention is required and the worker can perform the task without significant conscious thought. This

mode is very reliable, with infrequent errors on the order of 1 in every 10,000 iterations of the task.

- **Rule mode** - Actions based on selection of written or *stored rules* derived from one's recognition of the situation. The worker is familiar with the task and is taking actions in response to the changing situation. Errors are more frequent, on the order of 1 in 1,000, and are due to a misrepresentation of either the situation or the correct response.

- **Knowledge mode** - Actions in response to an unfamiliar situation. This could be new task or a previously familiar task that has changed in an unanticipated manner. Rather than using known rules, the worker is trying to reason or even guess their way through the situation. Errors can be as frequent as 1 in 2, literally a coin flip.

The performance modes refer to the amount of conscious control exercised by the individual doing the task, not the type of work itself. In other words, the skill performance mode does not imply work by crafts; rule mode does not imply supervision; and the knowledge mode does not imply work by professionals. This is a scale of the conscious thought required to react properly to a hazardous condition; from drilled automatic response, to conscious selection and compliance to proper rules, to needing to recognize there is a hazardous condition. The more unfamiliar the worker is with the work environment or situation, the more reliance there is on the individual's alert awareness, rational reasoning and quick decision-making skills in the face of new hazards. Knowledge mode would be commonly relied on in typically simple, mundane, low hazard tasks. All work, whether performed by a carpenter or surgeon, can exist in any of the performance modes. In fact, the performance mode is always changing, based on the nature of the work at the time. [Reason and Hobbs, 2003][17]

Understanding the performance mode the worker was in when he/she made the error is essential to developing the response to the accident (Figure 1-2). Errors in the skill mode typically involve mental slips and lapses in attention or concentration. The error does not involve lack of knowledge or understanding and, therefore, training can often be inappropriate. The worker is literally the expert on their job and training is insulting to the worker and causes the organization to lose credibility. Likewise, changing the procedure or process in response to a single event is inappropriate. It effectively pushes the worker out of the skill mode into rule-based until the new process can be assimilated. Because rule mode has a higher error rate, the result is usually an increase in errors (and accidents) until the workers assimilate the changes and return to skill mode. Training can be appropriate where the lapse is deemed due to a drift in the skills competence, out-of-date mindset, or the need for a drilled response without lapses.

Training might be appropriate for errors that occurred in rule mode because the error generally involved misinterpretation of either the situation or the correct response. In these instances, understanding requirements and knowing where and under what circumstance those requirements apply is cognitive in nature and must be learned or acquired in some way. Procedural changes are appropriate if the instructions were incorrect, unclear or misleading.

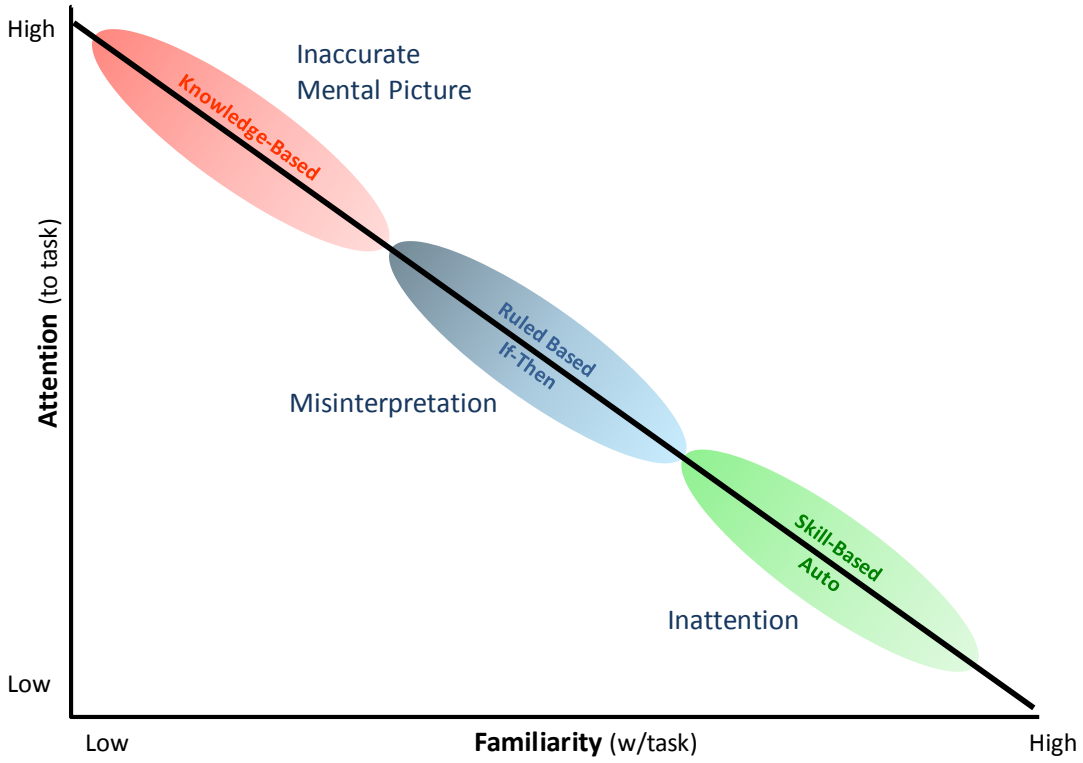


Figure 1-2: Performance Modes

Training might also be appropriate for errors that occurred in the knowledge mode, if the workers' understanding of the system was inadequate. However, the problem might have been issues like communication and problem-solving during the event, rather than inadequate knowledge.

1.5.3 Error Precursors

"Knowledge and error flow from the same mental sources, only success can tell the one from the other." The idea of human error as "cause" in consequential accidents is one that has been debunked by safety science since the early work by Johnson and the System Safety Development Center (SSDC) team. As Perrow stated the situation "Formal accident investigations usually start with an assumption that the operator must have failed, and if this attribution can be made, that is the end of serious inquiry. Finding that faulty designs were responsible would entail enormous shutdown and retrofitting costs; finding that management was responsible would threaten those in charge, but finding that operators were responsible preserves the system, with some soporific injunctions about better training." [Mach, 1976][18] [Perrow, 1984][5]

In contemporary safety science the concept of error is simply when unintended results occurred during human performance. Error is viewed as a mismatch between the human condition and environmental factors operative at a given moment or within a series of actions. Research has demonstrated that presence of various factors in combination increase the potential for error;

these factors may be referred to as error precursors. Anticipation and identification of such precursors is a distinguishing performance strategy of highly performing individuals and organizations. The following Task, Work Environment, Individual Capabilities and Human Nature (TWIN) model is a useful diagnostic tool for investigation (Figure 1-3).

TWIN Analysis Matrix

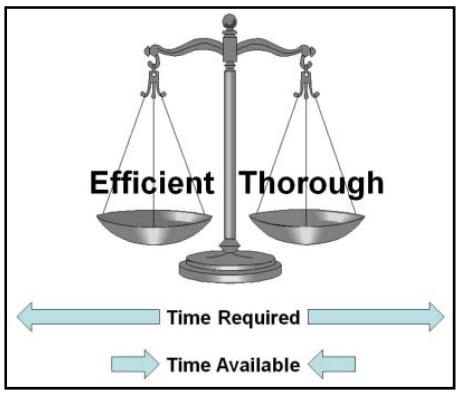
(Human Performance Error Precursors)

Task Demands	**Individual Capabilities**
Time Pressure (in a hurry)	Unfamiliarity with task / First time
High workload (large memory)	Lack of knowledge (faulty mental model)
Simultaneous, multiple actions	New techniques not used before
Repetitive actions / Monotony	Imprecise communication habits
Irreversible actions	Lack of proficiency / Inexperience
Interpretation requirements	Indistinct problem-solving skills
Unclear goals, roles, or responsibilities	Unsafe attitudes
Lack of or unclear standards	Illness or fatigue; general poor health or injury
Work Environment	**Human Nature**
Distractions / Interruptions	Stress
Changes / Departure from routine	Habit patterns
Confusing displays or controls	Assumptions
Work-arounds	Complacency / Overconfidence
Hidden system / equipment response	Mind-set (intentions)
Unexpected equipment conditions	Inaccurate risk perception
Lack of alternative indication	Mental shortcuts or biases
Personality conflict	Limited short-term memory

Figure 1-3: Error Precursors

1.5.4 Optimization

Human performance is often summarized as the individual working within organizational systems to meet the expectations of leaders. Performance variability is all about meeting expectations and actions intended to produce a successful outcome.

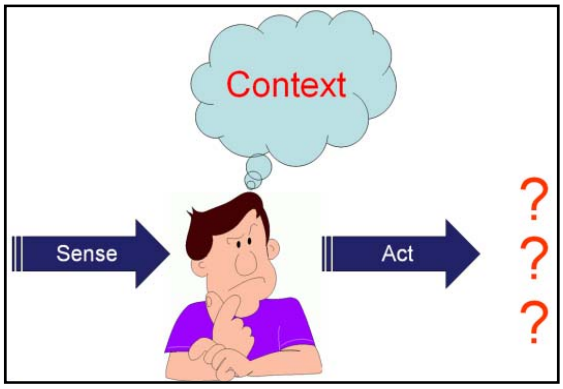


To understand performance variability, an investigator must understand the nature of humans. Regardless of the task, whether at work or not, people constantly strive to optimize their performance by striking a balance between resources and demands. Both of these vary over time as people make a trade-off between thoroughness and efficiency. In simple terms, thoroughness represents the time and resources expended in preparation to do the work and efficiency is the time and resources expended in completing the work. To do both completely requires more time and resources than is available and people must choose between them. The immediate and certain reward for meeting schedule and production expectations easily overrides the delayed and uncertain consequence of insufficient preparation and people lean towards efficiency. They are as thorough as they believe is necessary, but without expending unnecessary effort or wasting time.

The result is a deviation from expectation and the reason is obvious. It saves time and effort which is then available for more important or pressing activities. How the deviation is judged afterwards, is a function of the outcome, not the decision. If organizational expectations are met without incident, the deviations are typically disregarded or may even be condoned and rewarded as process improvements. If the outcome was an accident, the same actions can be quickly judged as violations. This is the probabilistic nature of organizational decision-making which is driven by the perceptions or misperceptions of risks. A deviation or violation is not the end of the investigation; it is the beginning as the investigator tries to understand what perceptions were going on in the system that drove the choice to deviate. [Hollnagel, 2009][19]

1.5.5 Work Context

Context matters and performance variability is driven by context. The simple sense – think – act model illustrates the role of context. Information comes to the worker, he makes a decision based on the context, and different actions are possible, based on the context.



The context of the decision relate to the goals, knowledge and focus of the worker. Successful completion of the immediate task is the obvious goal, but it takes place within the greater work environment where the need to optimize the use of

time and resources is critical. Workers have knowledge, but the application of knowledge is not always straight forward because it needs to be accurate, complete and available at the time of the decision. Goals and knowledge combine together to determine the worker's focus. Because workers cannot know and see everything all the time, what they are trying to accomplish and what they know drives where they direct their attention.

All this combines to create decisions that vary based on the influences that are present at the time of the decision and the basic differences in people. These influences and differences include:

- Organization - actions taken to meet management priorities and production expectations.
- Knowledge - actions taken by knowledgeable workers with intent to produce a better outcome.
- Social – actions taken to meet co-worker expectations, informal work standards.
- Experience – actions based on past experience in an effort to repeat success and avoid failure.
- Inherent variability – actions vary due to individual psychological & physiological differences.
- Ingenuity and creativity – adaptability in overcoming constraints and under specification.

The result is variable performance. From the safety perspective, this means that the reason workers sometimes trigger an accident is because the outcome of their action differs from what was intended. The actions, however, are taken in response to the variability of the context and conditions of the work. Conversely, successful performance and process improvement also arises from this same performance variability. Expressed another way, performance variability is not aberrant behavior; it is the probabilistic nature of decisions made by each individual in the organization that can result in both success and failure emerging from same normal work sequence.

In accident investigations, performance variability needs to be acknowledged as a characteristic of the work, not as the cause of the accident. Rather than simply judging a decision as wrong in retrospect, the decision needs to be evaluated in the context in which it was made. In accident investigation, the context or influences that drive the deviation need to be understood and addressed as contributing factors. Stopping with worker's deviation as the cause corrects nothing. The next worker, working in the same context, will eventually adapt and deviate from work-as imagined until chance aligns the deviation to other organization system weaknesses for a new accident.

Performance variability is not limited to just the worker who triggers the accident. People are involved in all aspects of the work, and the result is variability of all factors associated with the work. This can include variation in the actions of the co-workers, the expectations of the leaders, accuracy of the procedures, the effectiveness of the defenses and barriers, or even the basic

policies of the organization. This is reflected in the complex, non-linear (non-Newtonian) accident model where unexpected combinations of normal variability can result in the accident.

1.5.6 Accountability, Culpability and Just Culture

"Name, blame, shame, retrain" is an oft used phrase for older ineffective paradigms of safety management and accident analysis. Dr. Rosabeth Moss Kanter of Harvard Business School phased the situation this way: "Accountability is a favorite word to invoke when the lack of it has become so apparent." [Kanter, 2009][20]

The concepts of accountability, culpability and just culture are inextricably entwined. Accountability has been defined in various ways but in general with this characterization; "The expectation that an individual or an organization is answerable for results; to explain actions, or; the degree to which individuals accept responsibility for the consequences of their actions, including the rewards or sanctions." As Dr. Kanter explains "The tools of accountability — data, details, metrics, measurement, analyses, charts, tests, assessments, performance evaluations — are neutral. What matters is their interpretation, the manner of their use, and the culture that surrounds them. In declining organizations, use of these tools signals that people are watched too closely, not trusted, about to be punished. In successful organizations, they are vital tools that high achievers use to understand and improve performance regularly and rapidly."

Culpability is about considering if the actions of an individual are blame worthy. The concept of culpability in safety is based largely on the work of Dr. James Reason as a function of creating a Just Culture. The purpose is to pursue a humane culture in which learning as individuals and collectively is valued and human fallibility is recognized as simply part of the human condition. Being human however is to be distinguished from being a malefactor. He explains; "The term 'no-blame culture' flourished in the 1990's and still endures today. Compared to the largely punitive cultures that it sought to replace, it was clearly a step in the right direction. It acknowledged that a large proportion of unsafe acts were 'honest errors' (the kinds of slips, lapses and mistakes that even the best people can make) and were not truly blameworthy, nor was there much in the way of remedial or preventative benefit to be had by punishing their perpetrators. But the 'no-blame' concept had two serious weaknesses. First, it ignored – or at least, failed to confront – those individuals who willfully (and often repeatedly) engaged in dangerous behaviors that most observers would recognize as being likely to increase the risk of a bad outcome. Second, it did not properly address the crucial business of distinguishing between culpable and non-culpable unsafe acts."

> *"…a safety culture depends critically on first negotiating where the line should be drawn between unacceptable behaviour and blameless unsafe acts. There will always be a grey area between these two extremes where the issue has to be decided on a case by case basis."*

"… the large majority of unsafe acts can be reported without fear of sanction. Once this crucial trust has been established, the organization begins to have a reporting culture, something that provides the system with an accessible memory, which, in turn, is the essential underpinning to a learning culture. There will, of course, be setbacks along the way. But engineering a just culture is the all-important early step; so much else depends upon it." [GAIN Working Group E, 2004][21]

Along the road to a Just Culture organizations may benefit from explicit "amnesty" programs designed to persuade people to report their personal mistakes. In complex events, individual actions are never the sole causes. Thus determination of individual culpability and personnel actions that might be warranted should be explicitly separated from the accident investigation. Failure to make such separation may result in reticence or even refusal of individuals involved to cooperate in the investigation, may skew recollections and testimony, may prevent investigators from obtaining important information, and may unfairly taint the reputations and credibility of well intended individuals to whom no blame should be attached.

1.6 From Latent Conditions to Active Failures

An organizational event causal story developed by James Reason starts with the organizational factors: strategic decisions, generic organizational processes – forecasting, budgeting, allocating resources, planning, scheduling, communicating, managing, auditing, etc. These processes are colored and shaped by the corporate culture or the unspoken attitudes and unwritten rules concerning the way the organization carries out its business. [Reason, 1997][14]

These factors result in biases in the management decision process that create "latent conditions" that are always present in complex systems. The quality of both production systems and protection systems are dependent upon the same underlying organizational decision processes; hence, latent conditions cannot be eliminated from the management systems, since they are an inevitable product of the cultural biases in strategic decisions. [Reason, p. 36, 1997][14]

Figure 1-4 illustrates an example of latent conditions produced from the pressures of commitment to a heavy work load as an organizational factor at the base of the pyramid. This passes into the organization as a local work place factor in the form of stress in the work place. This is the latent condition that is a precursor or contributing factor to the worker cutting corners (the active failure of the safety system).

A distinction between active failures and latent conditions rests on two differences. The first difference is the time taken to have an adverse impact. Active failures usually have immediate and relatively short-lived effects. Latent conditions can lie dormant, doing no particular harm, until they interact with local circumstances to defeat the systems' defenses. The second difference is the location within the organization of the human instigators. Active failures are committed by those at the human-system interface, the front-line activities, or the "sharp-end" personnel. Latent conditions, on the other hand, are spawned in the upper echelons of the organization and within related manufacturing, contracting, regulatory and governmental agencies that are not directly interfacing with the system failures.

The consequences of these latent conditions permeate throughout the organization to local workplaces—control rooms, work areas, maintenance facilities etc. —where they reveal themselves as workplace factors likely to promote unsafe acts (moving up the pyramid in Figure 1-4). These local workplace factors include undue time pressure, inadequate tools and equipment, poor human-machine interfaces, insufficient training, under-manning, poor supervisor-worker ratios, low pay, low morale, low status, macho culture, unworkable or ambiguous procedures, and poor communications.

Within the workplace, these local workplace factors can combine with natural human performance tendencies such as limited attention, habit patterns, assumptions, complacency, or mental shortcuts. These combinations produce unintentional errors and intentional violations — collectively termed "adaptive acts"—committed by individuals and teams at the "sharp end," or the direct human-system interface (active error).

Large numbers of these adaptive acts will happen (small red arrows in Figure 1-4), but very few will align with the holes in the defenses (holes are created by the latent conditions deep within the organization). With defense-in-depth providing a multi-barrier defense, it takes multiple human performance errors to breach the multiple defenses. However, when defenses have become sufficiently flawed and organizational behavior consistently drifts from desired behavior accidents can occur. In such events causes are multiple and only the most superficial analysis would suggest otherwise.

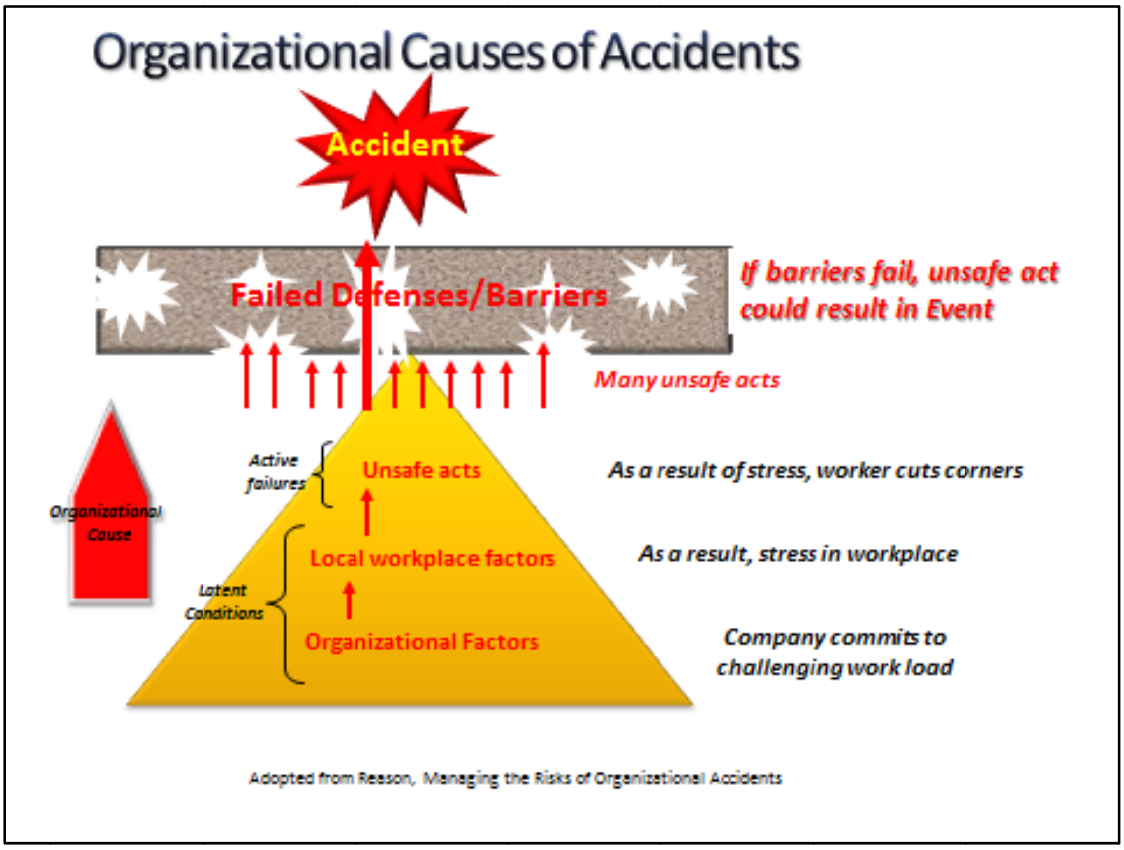


Figure 1-4: Organizational Causes of Accidents

1.7 Doing Work Safely - Safety Management Systems

Safety Management Systems (SMS) were developed to integrate safety as part of an organization's management of mission performance. The benefits of process based management systems is a well established component of quality performance. As organizations and the technologies they employ became more complex and diverse, and the rate of change in pace of societal expectations, technical innovations, and competitiveness increased, the importance of sound management of functions essential to safe operations became heightened.

A SMS is essentially a quality management approach to controlling risk. It also provides the organizational framework to support a sound safety culture. Systems can be described in terms of integrated networks of people and other resources performing activities that accomplish some mission or goal in a prescribed environment. Management of the system's activities involves planning, organizing, directing, and controlling these assets toward the organization's goals. Several important characteristics of systems and their underlying process are known as "process attributes" or "safety attributes" when they are applied to safety related operational and support processes.

The SMS for DOE is the Integrated Safety Management System (ISMS), defined in Federal Acquisition Regulation and amplified though DOE directives and guidance. The ISMS is the overarching safety system used by DOE to ensure safety of the worker, the community and the environment. The DOE ISMS is characterized by seven principles and five core functions:

Seven Principles

- **Line management responsibility for safety**
  Line management is directly responsible for the protection of workers, the public and the environment.

- **Clear roles and responsibilities**
  Clear and unambiguous lines of authority and responsibility for ensuring safety is established and maintained at all organizational levels and for subcontractors.

- **Competence commensurate with responsibilities**
  Personnel are required to have the experience, knowledge, skills and capabilities necessary to discharge their responsibilities.

- **Balanced priorities**
  Managers must allocate resources to address safety, as well as programmatic and operational considerations. Protection of workers, the public and the environment is a priority whenever activities are planned and performed.

- **Identification of safety standards and requirements**
  Before work is performed, the associated hazards must be evaluated, and an agreed-upon set of safety standards and requirements must be established to provide adequate assurance that workers, the public and the environment are protected from adverse consequences.

- **Hazard controls tailored to work being performed**
  Administrative and engineering controls are tailored to the work being performed to prevent adverse effects and to mitigate hazards.

- **Operations authorization**
  The conditions and requirements to be satisfied before operations are initiated are clearly established and agreed upon.

Five Core Functions (Figure 1-5)

- **Define the scope of work**
  Missions are translated into work, expectations are set, tasks are identified and prioritized and resources are allocated.

- **Analyze the hazards**
  Hazards associated with the work are identified, analyzed and categorized.

- **Develop and implement hazard controls**
  Applicable standards, policies, procedures and requirements are identified and agreed upon; controls to prevent/mitigate hazards are identified; and controls are implemented.

- **Perform work within controls**
  Readiness is confirmed and work is performed safely.

- **Provide feedback and continuous improvement**
  Information on the adequacy of controls is gathered, opportunities for improving the definition and planning of work are identified, and line and independent oversight is conducted.

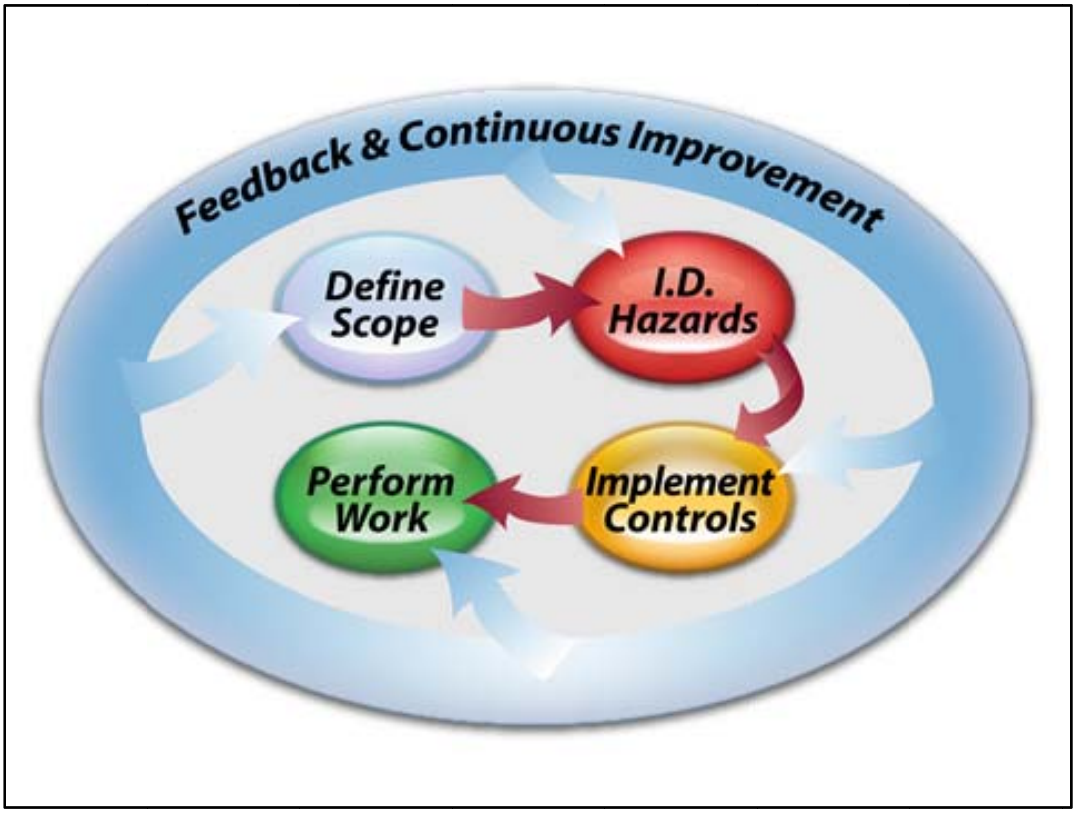


Figure 1-5: Five Core Functions of DOE's Integrated Safety Management System

1.7.1 The Function of Safety Barriers

The use of controls or barriers to protect the people from the hazards is a core principal of safety. Barriers are employed to serve two purposes; to prevent release of hazardous energy and to mitigate harm in the event hazardous energy is released. Energy is defined broadly as used here, and includes multiple forms, for example; kinetic, biological, acoustical, chemical, electrical, mechanical, potential, electromagnetic, thermal, or radiation.[ii]

[ii] For a detailed discussion of barriers refer to "Barriers and Accident Prevention" by Erik Hollnagel, 2004.

The dynamics of accidents may be categorized into five basic components, illustrated in Figure 1-6: 1) the threat or triggering action or energy, 2) the prevention barrier between the threat and the hazard, 3) the hazard or energy potential, 4) the mitigation barrier to mitigate hazardous consequences towards the target, 5) the targets in the path of the potential hazard consequences. When these controls or barriers fail, they allow unwanted energy to flow resulting in an accident or other adverse consequence.

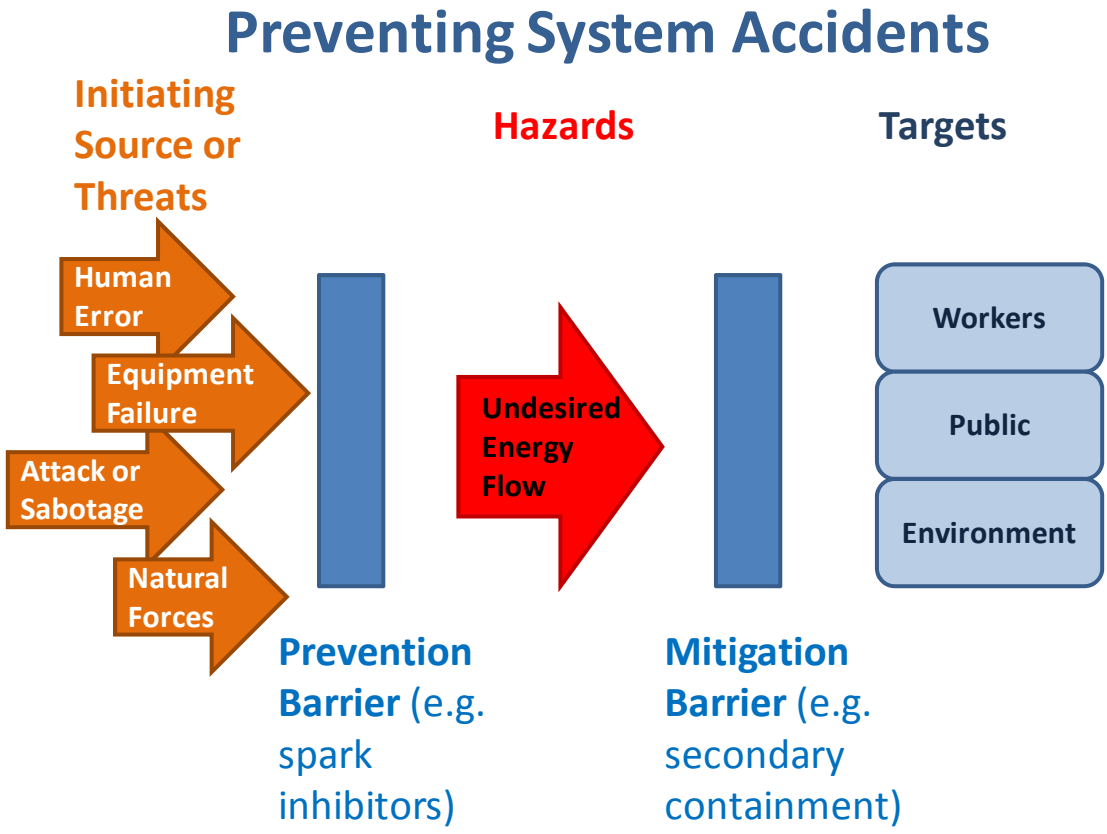


Figure 1-6: Barriers and Accident Dynamics – Simplistic Design

The objective is to contain or isolate hazards though the use of protective barriers. Prevention barriers are intended to preclude release of hazards by human acts, equipment degradation, or natural phenomena. Mitigation barriers are used to shield, contain, divert or dissipate the hazardous energy if it is released thus precluding negative consequences to the employees or the surrounding communities. Distance from the hazard is a common mitigating barrier.

Barrier analysis is based on the premise that hazards are associated with all accidents. Barriers are developed and integrated into a system or work process to protect personnel and equipment from hazards. For an accident to occur the design of technical systems did not provide adequate barriers, work design did not specify use of appropriate barriers, or barriers failed. Investigators use barrier analysis to identify hazards associated with an accident and the barriers that should/could have prevented it. Barrier analysis addresses:

- Barriers that were in place and how they performed
- Barriers that were in place but not used
- Barriers that were not in place but were required
- The barrier(s) that, if present or strengthened, would prevent the same or a similar accident from occurring in the future.

All barriers are not the same and differ significantly in how well they perform. The following are some of the general characteristics of barriers that need to be considered when selecting barriers to control hazards. When evaluating the performance of a barrier after an accident, these characteristics also suggest how well we would expect the barrier to have performed to control the hazard.

- Effectiveness – how well it meets its intended purpose
- Availability – assurance the barrier will function when needed
- Assessment – how easy to determine whether barrier will work as intended
- Interpretation – extent to which the barrier depends on interpretation by humans to achieve its purpose

1.7.2 Categorization of Barriers

Barriers may also be categorized according to a hierarchy of cost/reliability and according to barrier function. The barrier cost/reliability hierarchy includes:

Physical or engineered barriers – These are the structures that are built, or sometimes naturally exist, to prevent the flow of energy or personnel access to the hazards. These barriers require an investment to design and build and have a cost to maintain and update. Examples: Personnel cage around a multi-story ladder, a guard rail on a platform, or a barricade to prevent access.

Administrative or management policy barriers – These include rules, procedures, policies, training, work plans that describe the requirements to avoid hazards. These barriers require less capital investment but have a cost in the development, review, updating, training, communication, and enforcement to assure adequacy and compliance. Examples: Requirement to use harness and strap ties while climbing a multi-story ladder, a prescriptive process procedure sequence, or laws against trespassing.

Personal knowledge or skill barriers – These include human performance aspects of: fundamental lessons-learned, knowledge, common sense, life experiences, and education that contribute to the individuals' survival instincts and decision-making ability. These barriers require little or no investment except in the screening and selection process for qualified personnel used in a task and providing supervision. Examples: The decision not to climb a

ladder with a tool in one hand, the decision not to violate one of the administrative barriers, or recognizing a dangerous situation.

Another analysis system divides barriers into four categories that reflect the nature of the barriers' performance function. These four categories can be useful in the barrier analysis for characterizing more precisely the purpose of the barrier and its type of weakness. Examples for each of the four categories are as follows:

Physical– physically prevents an action from being carried out or an event from happening

- Containing or protecting - walls, fences, railings, containers, tanks
- Restraining or preventing movement - safety belts, harnesses, cages
- Separating or protecting – crumple zones, scrubbers, filters

Functional– impedes actions through the use of pre-conditions

- Prevent movement/action (hard) – locks, interlocks, equipment alignment
- Prevent movement/action (soft) – passwords, entry codes, palm readers
- Impede actions – delays, distance (too far for single person to reach)
- Dissipate energy/extinguish – air bags, sprinklers

Symbolic– requires an act of interpretation in order to achieve their purpose

- Countering/preventing actions – demarcations, signs, labels, warnings
- Regulating actions – instructions, procedures, dialogues (pre-job brief)
- System status indications – signals, warnings, alarms
- Permission/authorization – permits, work orders

Incorporeal– requires interpretation of knowledge in order to achieve their purpose

- Process – rules, restrictions, guidelines, laws, training
- Comply/conform – self-restraint, ethical norms, morals, social or group pressure

Within DOE organizations, there is typically a defense-in-depth policy for reducing the risks of a system failure or an accident due to the threats. This policy maintains a multiple layered barrier system between the threats or hazards and the requirement to correct any weaknesses or failures identified in a single layer. Therefore, an accident involving such a protected system requires

either a uniquely improbable simultaneous failure of multiple barriers, or poor barrier concepts or implementation, or a period of neglect allowing cascading deterioration of the barriers.[iii]

Defense-in-depth can be comprised of layers of any combination of these types of barriers. Obviously, it is much more difficult to overcome multiple layers of physical or engineered barriers. This is the most reliable and most costly defense. Risk management analysis determines the basis and justification for the level of barrier reliability and investment, based on the probability and consequence of a hazard release scenario. For low probability, low consequence events the level of risk often does not justify the investment of physical barriers. Cost and schedule conscious management may influence selection of non-physical barriers on all but the most likely and catastrophically hazardous conditions. Such choices place greater reliance on layers of the less reliable barriers dependent on human behavior. Adding multiple barrier layers can appear to add more confidence, but multiple layers may also lead to complacency and diminish the ability to use and maintain the individual barrier layers. Complex barrier systems and barrier philosophies place heightened importance on the context of organizational culture and human performance becomes a major concern in the prevention of accidents as barrier systems become more complex and individual barrier layer functionality become less apparent.

A cascading effect can occur in aging facilities. Engineered barriers can become out-of-date, fall into disrepair or wear out; or be removed as part of demolition activity. Management should transition to reliance on a substitute administrative barrier, but this need may not be recognized.[iv] For example, a fire protection system, temporarily or permanently disable, is replaced by a fire watch until the protection system is restored, replaced, or the fire potential threat is removed. Administrative barriers may weaken due to inadequate updates to rules, inadequate communication and training, and inadequate monitoring and enforcement. This results in managements' often unintentional reliance on the personal knowledge barriers. Personal knowledge barriers can be weakened by the inadequate screening for qualifications, inadequate assignment selections, or inadequate supervision.

An alignment of cascading weaknesses in barriers can result in an unqualified worker unintentionally violating an administrative control and defeating a worn out physical barrier to initiate an accident. Effective management of any of the barriers would have prevented the accident by breaking the chain of events. Therefore, investigating a failure of defense-in-depth requires probing a series of management and individual decisions that form the precursors and chain of actions that lead to the final triggering action.

[iii] A common use of "defense-in-depth" is the Lockout-Tagout (LOTO) Procedure. This procedure administratively requires that a hazardous energy be isolated by a primary physical barrier (e.g., valve or switch), a secondary physical barrier (a lock) that controls inadvertent defeat of the primary barrier, and a tertiary administrative barrier (tagging) controls the removal of the physical barriers. It is understood that omitting any one of these barriers is a violation of the LOTO procedure.

[iv] An example of a cascading effect, related to LOTO, is the discovery that some old facilities have used the out-of-date practice of common neutrals in old electrical systems or that facility circuit diagrams and labeling were not maintained accurately. These latent conditions potentially defeat LOTO entirely, requiring an additional administrative barrier procedure to do de-energized-circuit verification prior to accessing old wiring systems. Latent conditions are explained further in section 1.4.

1.8 Accident Types/ Individual and Systems

There are two fundamental types of accidents which DOE seeks to avoid; individual and system accidents. Confusion between individual and system safety has been frequently cited as causal factors in major accidents.[v] In the ISMS framework, individual accidents are most often associated with failures at the level of the five core functions. System accidents involve failures at the principles level involving decision making, resource allocation and culture factors that may shift the focus and resources of the organization away from doing work safely to detrimental focus on cost or schedule.

1.8.1 Individual Accidents

Individual accidents - an accident occurs wherein the worker is not protected from the hazards of an operation and is injured (e.g., radiation exposure, trips, slips, falls, industrial accident, etc.). The focus of preventing individual accidents is to protect the worker from hazards inherent in mission operation (Figure 1-7). The inherent challenges in investigating an individual accident are due to the source of the human error and the victim or target of the accident can often be the same individual. This can lead to a limited or contained analysis that fails to consider the larger organizational or systemic contributors to the accident. These types of accidents involving individual injuries can overly focus on the mitigating barriers or personnel protection equipment (PPE) that avoid injuries and not consider the appropriate preventative barriers to prevent the actual accident.

[v] Texas City, Buncefield, Deepwater Horizon

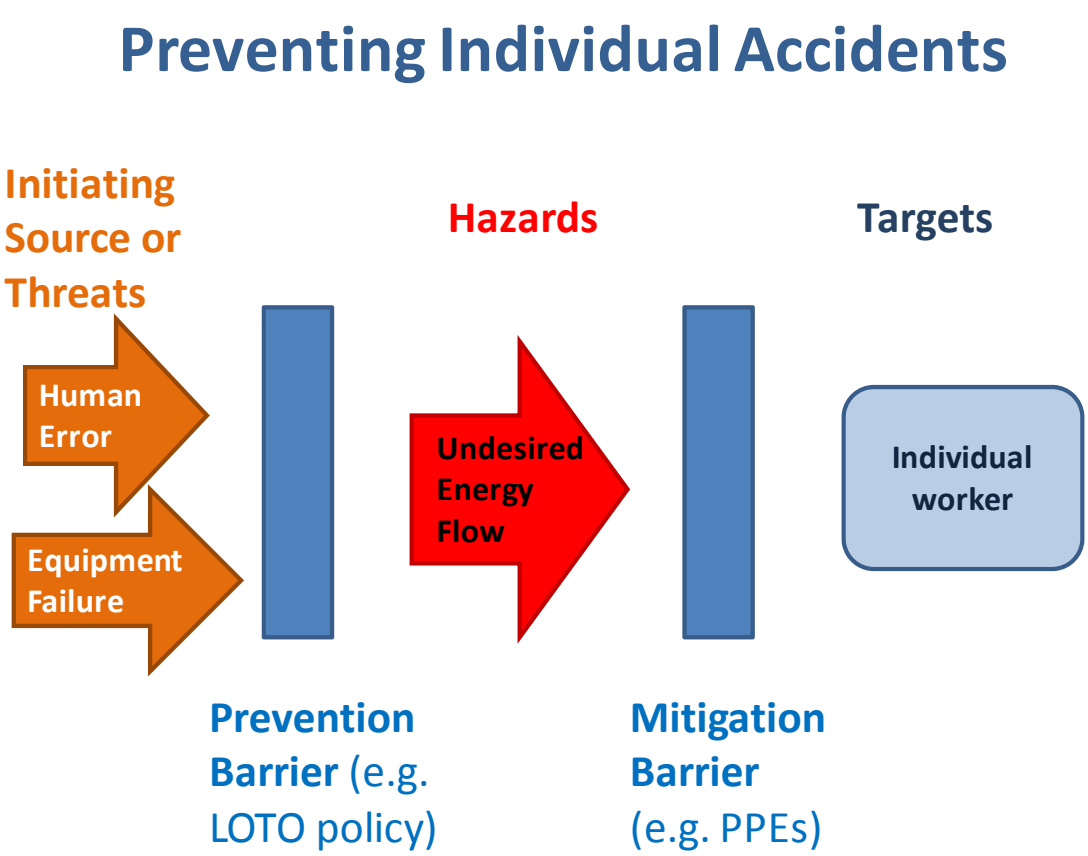


Figure 1-7: Individual Accident

1.8.2 Preventing Individual Accidents

To prevent recurrence of individual injury accidents, corrective actions from accident investigations must identify what barriers failed and why [i.e., stop the source and the flow of energy from the hazards to the target (the worker)]. The mitigating barriers are important to reducing or eliminating the harm or consequences of the accident, but emphasis must be on barriers to prevent the accident from occurring. However, it is possible to find conditions where the threat is deemed acceptable if the consequence can be adequately mitigated.[vi]

[vi] An example of reliance on a mitigating barrier would be in the meat cutting process where chain-mail gloves protect hands from being cut. The threat or initiating energy is the knife moving towards the hand or vice-versa. The hazard energy is the cutting action of the blade. Since the glove does not prevent the knife from impacting the hand, the glove is a mitigation barrier that reduces the hazardous cutting consequence of the impact. Implementing a prevention barrier would require redesigning the process to block or eliminate the need for the hand to be in cutting area. The absence of the prevention barrier is the result of a bias in the organizational decision-making process discussed later in this handbook.

1.8.3 System Accident

A system accident is an accident wherein the protective and mitigating systems collectively fail allowing release of the hazard and adversely affecting many people, the community and potentially the environment. A system accident can be characterized as an "unanticipated interaction of multiple failures in a complex system. This complexity can either be technological or organizational, and often is both." [Perrow, 1984][5]

The focus of preventing system accidents is to maintain the physical integrity of operational barriers such that they prevent threats that may result from human error, malfunctions in equipment or operational processes, facility malfunctions or from natural disasters or such that they mitigate the consequences of the event in case prevention fails. (Figure 1-8).

System hazards are typically managed from cradle to grave through risk management. Risk management processes identify the potential threats, weaknesses, and failures as risks to the design, construction, operations, maintenance, and disposition of the system. Risk management establishes and records the risk parameters (or basis) and the investment decisions, the control systems, and policies to mitigate these risks. Risk management, in a broad organizational sense, can include financial, political, cultural, and social risks. While not excluding the broader societal factors, the principal focus of this handbook is on socio-technical systems and related life-cycle management (design, build, operate, maintain, dispose) system risks.

It is important to recognize the distinction between individual accidents and system accidents as it affects the way the accident is investigated, in particular the way the barriers are analyzed. The most likely differentiation of the type of accident investigation is from experience that individual accidents are likely to be influenced by work practices, plans and oversight, while system failures will most likely be influenced by risk management process for design, operations, or maintenance. System accidents require a more in-depth investigation into the policies and management culture that drives risk management decision-making. Naturally, there is often an overlap that combines individual work hazards control practices and the system risk management policies as potential areas of investigation.

System Accident

An accident wherein the system fails allowing a threat to release the hazard and as a result many* people are adversely affected

* Workers, Enterprise, Environment, Country

Focus

Protect the operations from the threats

The emphasis on the system accident in no way degrades the importance of individual safety, it is a pre-requisite of system safety, but focus on individuals safety is not enough.

Figure 1-8: System Accident

1.8.4 How System Accidents Occur

In order to prevent system accidents and incidents, it is important to first understand (via a mental model) how they occur. Figure 1-9 represents a simple schematic of how system accidents (accidents with large consequences affecting many people) can occur.

As defined in this figure a threat can come from four sources:

- Human error such as someone dropping high explosives resulting in detonation.
- Failure of a piece of equipment, tooling or facility. For example a piece of tooling with faulty bolts causes high explosive to drop on the floor resulting in detonation.
- From a natural disaster such as an earthquake resulting in falling debris that could detonation high explosives.
- "Other" as of yet undiscovered to accommodate future discoveries.

Based on this simplistic system accident scenario it is clear technical system integrity must be protected from deterioration from physical and human/social factors.

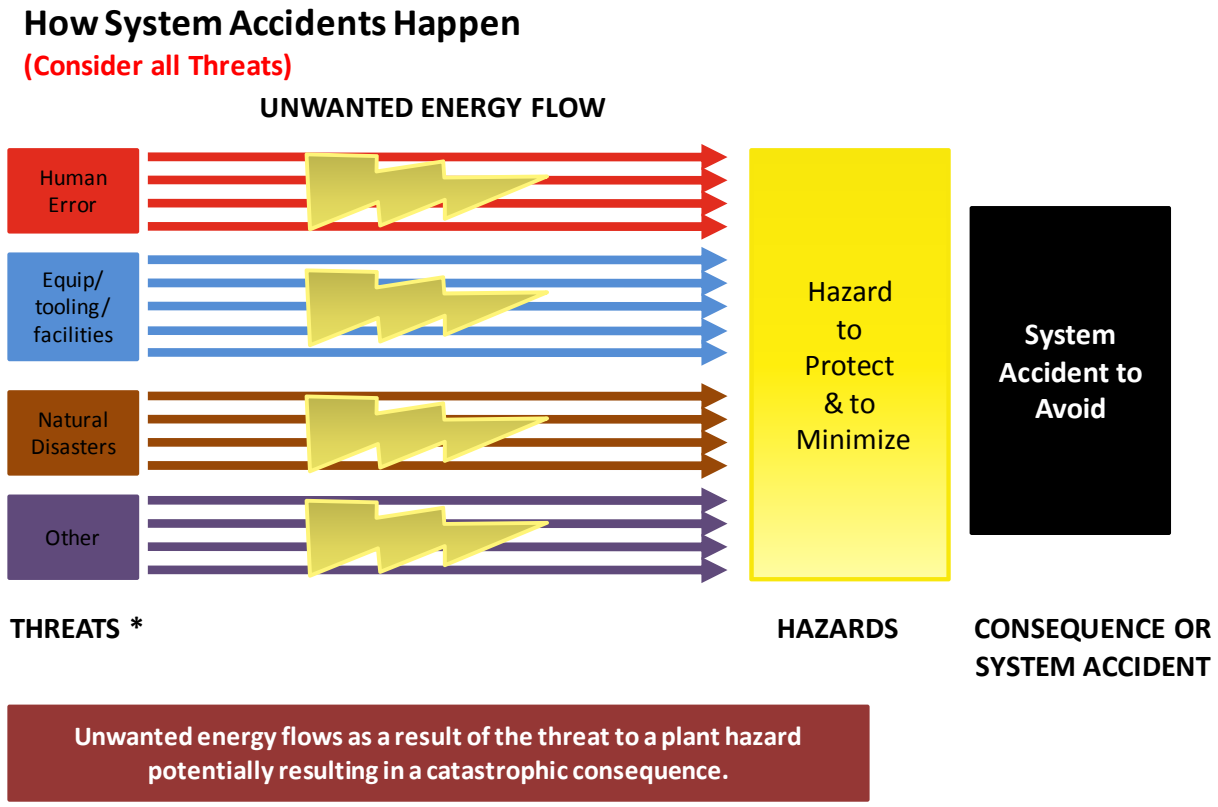


Figure 1-9: How System Accidents Happen

1.8.5 Preventing System Accidents

Figure 1-10 provides a simplistic view of how to prevent a system accident. Hazards can be energy in the form of leaks, projectiles, explosions, venting, radiation, collapses, or other ways that produce harm to the work force, the surrounding community, or the environment. The idea is that one wants to isolate these hazards from those things that would threaten to release the unwanted energy or material, such as human errors, faulty equipment, sabotage, or natural disasters such as wind and lightning through the use of preventive barriers. If this is done, work can proceed safely (accidents are avoided).

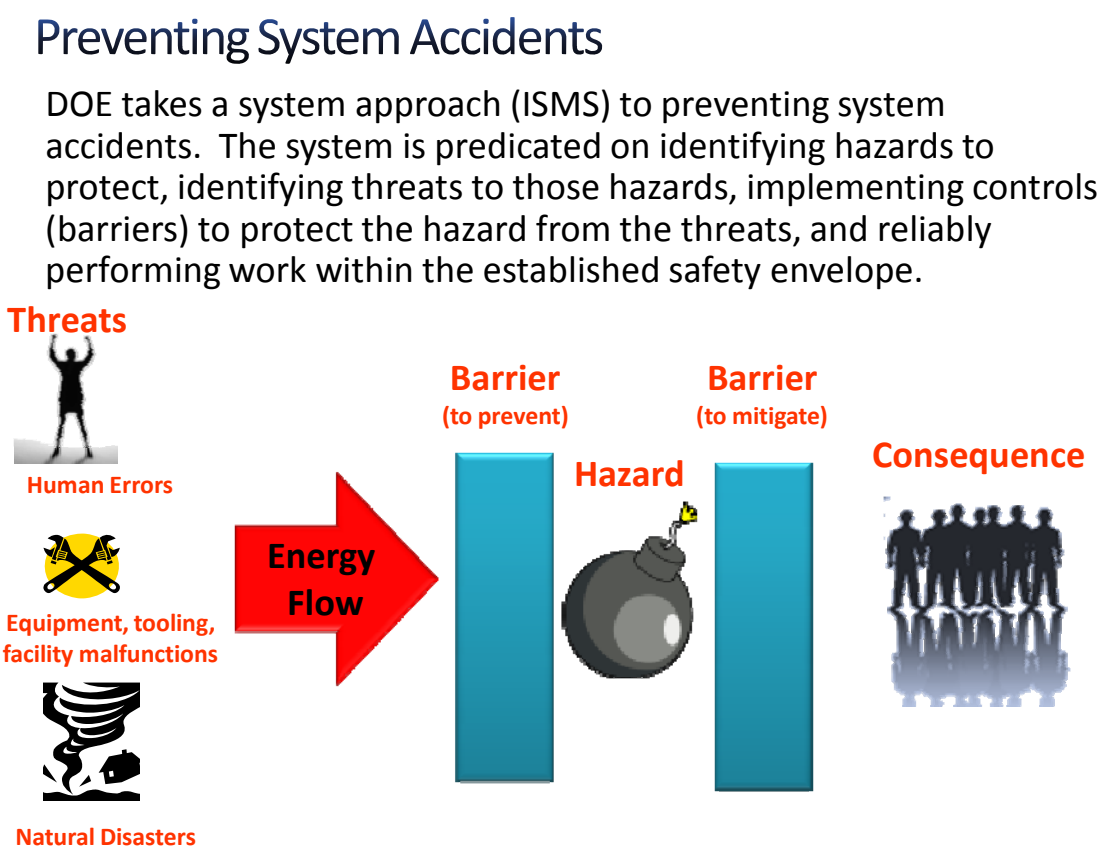


Figure 1-10: Prevent a System Accident

1.9 Diagnosing and Preventing Organizational Drift

Recognizing the hazards or risks and establishing and maintaining the barriers against accidents are continuous demands on organizations at all levels. Work, organizations, and human activity are dynamic, not static. This means conditions are always changing, even if only through aging, resource turnover, or creeping complacency to routine. Similarly to the Second Law of Thermodynamics—the idea that everything in the created order tends to dissipate rather than to coalesce – organizations left untended trend in the direction of disorder. In the safety literature this phenomena is referred to as **organizational drift**. Organizational drift, if not halted, will lead to weakened or missing barriers.

In order to recognize, diagnose and hopefully to prevent organizational drift from established safety systems (ISMS), models (mental pictures) are needed. Properly built models help investigators recognize aberrations by providing an accepted reference to compare against (i.e., a mental picture of how the organization is supposed to work). Models in combination with an understanding of organizational behavior also allow investigators to extrapolate individual events to a broader organizational perspective to determine if the problem is pervasive throughout the organization (deeper organizational issues).

Three levels of models are introduced in this section to aid the investigators putting their event into perspective.

- Level I at the employee level,
- Level II at the physics level - Break-the-Chain Framework (BTC),
- Level III at the organization or system level.

1.9.1 Level I: Employee Level Model for Examining Organizational Drift -- Monitoring the Gap – "Work-as-Planned" vs. "Work-as-Done"

The Employee Level Model provides the most detailed examination of organizational drift by comparing "work-as-done" on the shop floor with how work was planned by management and process designers. At this level, the effect of organization drift could result in an undesirable event because this is where the employees contact the hazards while performing work.

DOE organizations develop policies, procedures, training etc. to provide a management system envelope of safety within which they want their people to work. This safety envelope is developed through the ISMS "Define the Scope of Work, Analyze the Hazards, and Develop and Implement Hazard Controls" and can be referred to as "work-as-planned." The way work is actually accomplished under ISMS "Perform Work within Controls," referred to as "work-as-done", can be compared to the work-as-planned. Every organization's goal is to have "work-as-done" to equal work-as-planned (i.e., actual work performed within the established safety envelope – left side of Figure 1-11).

There will always be a performance gap between "work-as-planned" and "work-as-done" work performance gap (ΔWg) because of the variability in the execution of every human activity (right side of Figure 1-11). When the ΔWg becomes a problem because an accident or an information-rich, high-consequence or reoccurrence event occurs, a systematic investigative process helps to understand first "what" the variation is and second, determine "why" the variation exists. Figure 1-11 illustrates the comparison of the ideal or desirable organizational work performance goal on the left side, with the more likely or realistic work performance gap on the right. Recognizing and reducing the gap is the objective of "Provide Feedback and Continuous Improvement" activities.

Within this handbook, the term "physics of safety" is used to represent the science and engineering principles and methods used to assure the barriers designed into the systems are effective against the nature of the threats and hazards. Only with sound "physics of safety" basis behind the purpose of the barriers can management truly rely on a "work-as-planned" safety performance envelope. A typical gap analysis must explore weaknesses in the "work-as-planned" and the "work-as-performed."

Because the "work-as-planned" truly represents the requisite safety/security/quality process that management wants their employees to follow; the investigative process reduces the gap ΔWg by

systematically addressing the broadest picture of what went wrong, and focuses the Judgments of Need and Corrective Actions to reduce the gap.

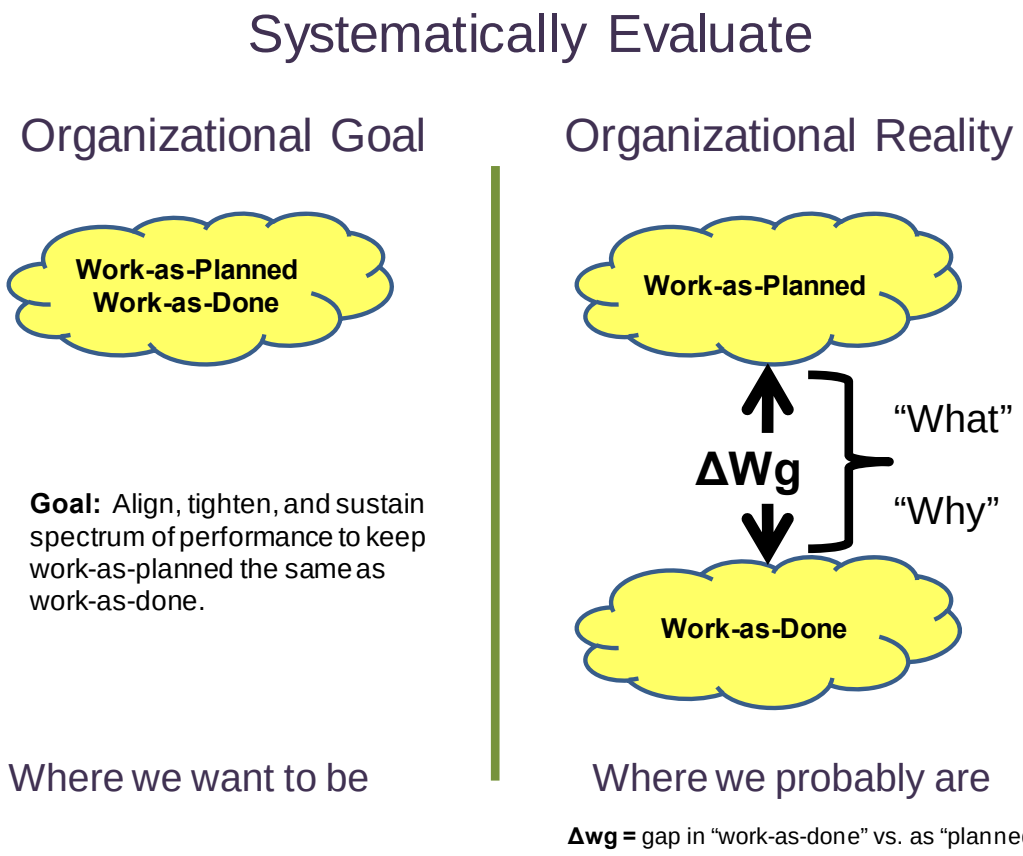


Figure 1-11: Level I - "Work-as-Done" Varies from "Work-as-Planned" at Employee Level

1.9.2 Level II: Mid-Level Model for Examining Organizational Drift – Break-the-Chain

The Mid-Level Model for examining organizational drift focuses on the Break-the-Chain (BTC) framework. Based on the simplistic representation displayed in Figure 1-12, the BTC framework provides a broader, more complete model to help organizations avoid the threat potential of catastrophic events posed by the significant hazards, dynamic tasks, time constraints, and complex technologies that are integral to ongoing missions. And, when an event does occur, it also provides a logical and systematic framework to diagnose the event to determine which step in the process broke down to allow focusing corrective actions in only those areas found deficient. The BTC model is designed to stop the system accident as shown in Figure 1-10 but

can be applied equally to individual accidents. The BTC model is nothing but a logical, physics-based application of the ISM core functions. The six basic components of the BTC model are:

Step #1 – Focus on the System Accident (Pinnacle/Plateau Event) to Avoid: The first step focuses on the last link of the chain, the consequences of the system accident that the organization is trying to prevent. Once the catastrophic consequences have been identified, they should be listed in priority order. This prioritization is important for four reasons:

- It serves as an important reminder to all employees of the potential catastrophic consequences they must strive to avoid each day.
- It pinpoints where defensive barriers are most needed; as one would expect, the probability of an event and the severity of the consequences will drive the number and type of barriers selected.
- It ensures that the defensive barriers associated with the highest priority consequences will receive top protection against degradation.
- It encourages a constant review of resources against consequences focusing attention on making sure the most severe consequences are avoided at all times.

Prioritization is a critical organizational dynamic. Efforts to protect against catastrophic consequential events should be the first priority. Focus must be maintained on the priority system accidents to assure that the needed attention and resources are available to prevent them.

Step #2 – Recognize and Minimize Hazard: Identify and minimize the physical hazard, while maintaining production. After identifying the hazard, there are two approaches to minimize it. First, actions are taken to reduce the physical hazard that can be impacted by the threat (for example minimizing the amount of combustible material in facilities). Second, attempts are made to reduce the interactive complexity and tight coupling within the operation or, conversely, to increase the response time of the organization so an event can be recognized and responded to more quickly. The intent of these two approaches is to remove or reduce the hazard so that the consequences of an accident are minimized to the extent possible.

Step #3- Recognize Threat Posed by Human Errors, Failed Equipment, Tooling or Facilities, Mother Nature (i.e., natural disasters) or Other as of yet Unknown Things: A key component of consequence avoidance is identifying and minimizing all significant knowable threats that could challenge the hazard (i.e., allow the flow of unwanted energy). Note the use of the word "all." The intent is that if not all threats are identified and addressed; the organization is vulnerable to failure. Organizations should ensure the system event does not occur, not hope it does not occur (i.e., they prove operations safe). The categories of threats from human error and failed equipment, tooling or facilities, and natural disasters have been adapted from a combination of MORT, DOE Guide (G) 231.1-1 and TapRoot®.

Step #4 – Manage Defenses: Based on the threats identified, one must ensure the right barriers are identified to prevent or to reduce the probability of the flow of energy to the hazard (red, blue, brown, and purple barriers in Figure 1-12) or if that fails to mitigate the consequences of a

system accident (shown by granite encasement around system event box in Figure 1-12). The type and number of barriers and the level of effort needed to protect them are dictated by level of consequence and type of hazard associated with the operation. The decrease in the number of threats or probability of occurrence as a result of the application of various barriers or defenses is indicated in Figure 1-12 by the reduction in the number of colored arrows that can reach the hazard.

Step #5 – Foster a Culture of Reliability: Steps 1 through 4 make the operational hazard less vulnerable to threats. To execute these steps successfully and consistently without observable signs of degradation or significant events, requires an army of trained and experienced personnel who conscientiously follow the proven work practices. These workers must maintain their proficiency through continuous hands-on work and be trained so they can make judgment calls on the shop floor that will reflect the shared organizational values. They also need to have the authority to make time-critical decisions when situations require this action. They must be part of an organization that has a strong culture of reliability.

Step #6 – Learn from Small Errors to Prevent Big Ones: Gaps between "work-as-planned" by the process designer and "work-as-done" by the employees exist in every operation and reflects the challenges an organization will face sustaining the BTC framework (Figure 1-12). The fact that these gaps exist should be of no surprise, they exist in every organization. The problem occurs when the organization is unaware of the gaps or does not know the magnitude or extent of the gaps across the operation. Because of the importance of DOE sites remaining within the established safety basis (ISMS), the investigation process as described in this document places special emphasis on evaluating and closing the gap between "work-as-planned" and "work-as-done".

BTC parallels and complements the ISMS functions. The levels of formality or rigor to which the six process components (or process steps) are applied are proportional to the complexity and consequences of the operations (e.g., for nuclear operations where the potential consequences are severe, the full rigor of 10 Code of Federal Regulations (CFR) Part 830, nuclear safety is employed). Detailed application of this process can be found in Volume II, Chapter 1.

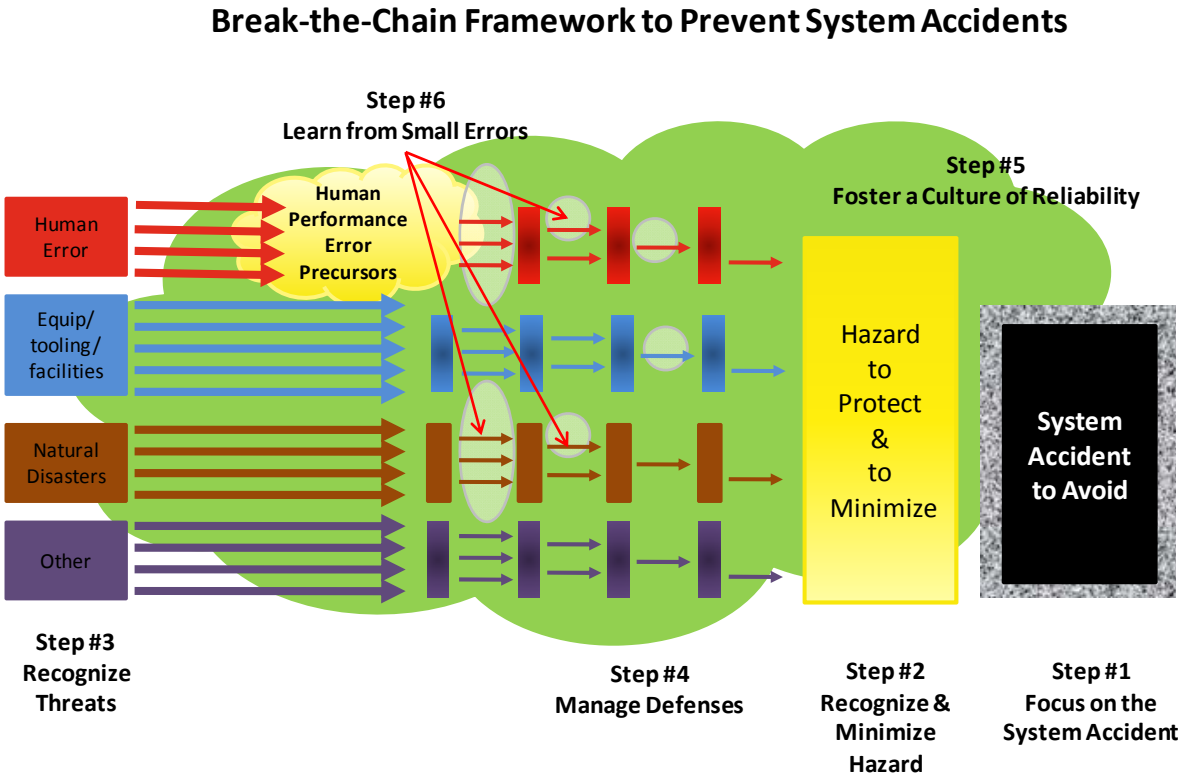


Figure 1-12: Level II - Physics-Based Break-the-Chain Framework

1.9.3 Level III: High Level Model for Examining Organizational Drift

The High Level Model for examining organizational drift, shown in Figure 1-13, was adapted from work by the Institute of Nuclear Power Operations (INPO)[vii]. It is intended to represent a systematic view for analysis of both individual and system accidents. The model breaks down work into four sequences that one typically finds at DOE sites: 1) Organizational Processes & Values; 2) Job Site Conditions (work-as-planned); 3) Worker Behaviors ("work-as-done"); 4) Operational Results. An explanation of each category of work can be found in Figure 1-13.

Also shown in Figure 1-13 are the quality assurance checks (green ovals) that take place before transitioning from one sequence of work to the next sequence of work. These process check points are additional examples of barriers put in place to ensure readiness to go the next sequence of work. DOE uses many similar quality assurance readiness steps in both its high hazard nuclear operations and industrial operations.

[vii] INPO Human Performance Reference Manual, INPO-06-003.

The later in the work sequence the process barriers fall, noted by higher highlighted grey numbers, the more significant or important the barrier is in preventing the undesired event because it represents one of the last remaining barriers before a consequential event.

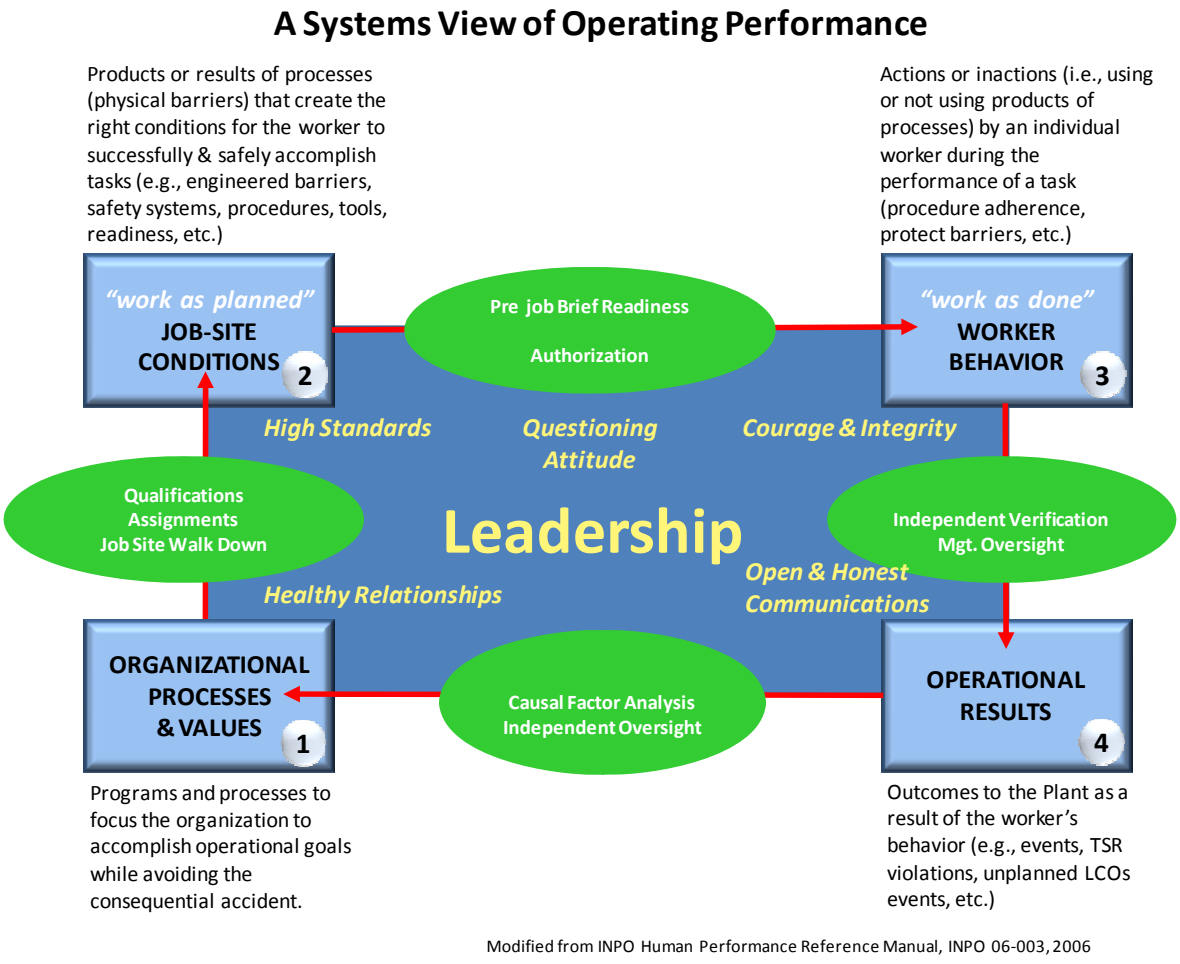


Figure 1-13: Level III - High-Level Model for Examining Organizational Drift

1.10 Design of Accident Investigations

The organizational basis for the causes of accidents requires the accident investigators to develop insights about organizational behavior, mental models and the factors that shape the environment in which the incident occurred. This develops a better understanding of "what" in the organizational system failed and "why" the organization allowed itself to degrade to the state that resulted in an undesired consequence. The investigation progresses through the events in the opposite order in which they occurred, as shown schematically in Figure 1-14.

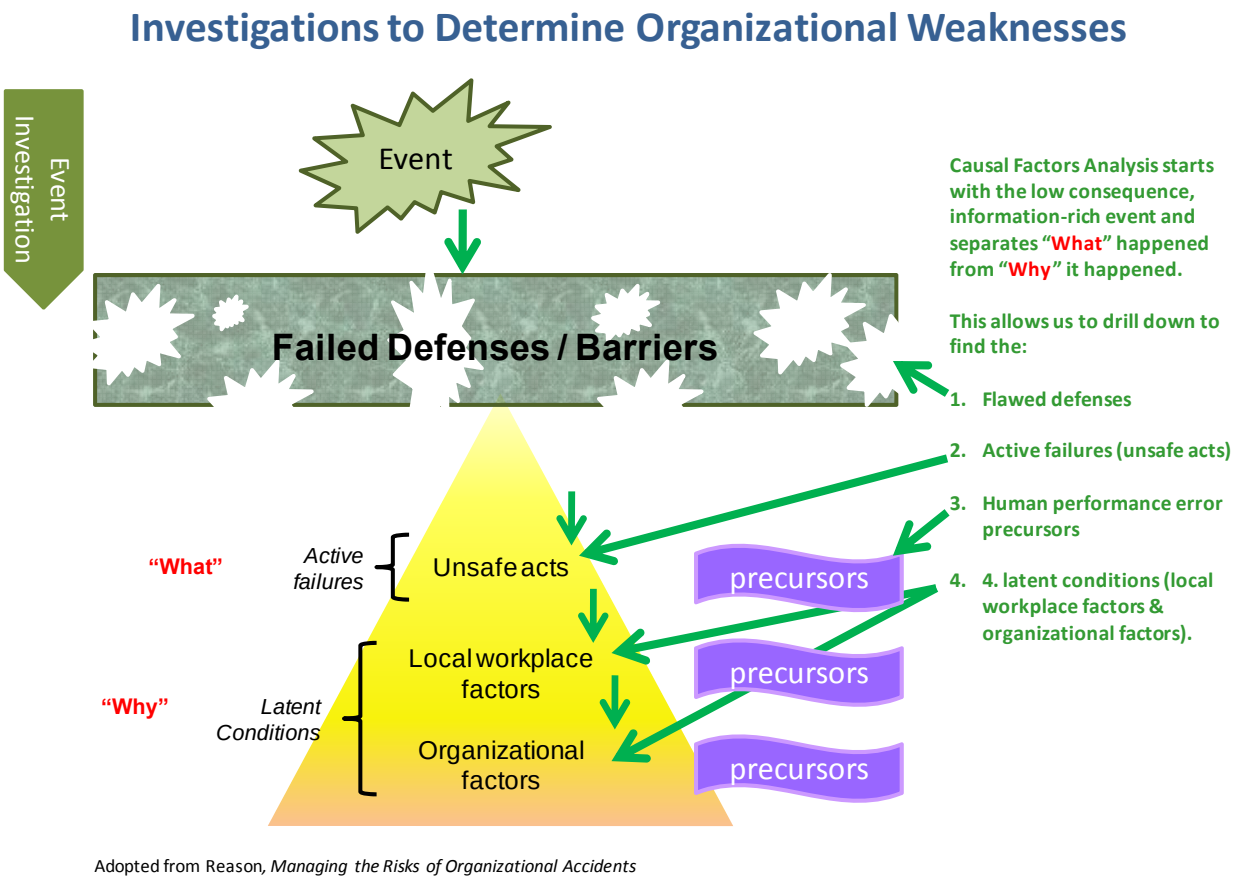


Figure 1-14: Factors Contributing to Organizational Drift

1.10.1 Primary Focus – Determine "What" Happened and "Why" It Happened

The basic steps and processes used for the Accident Investigation are:

- Define the Scope of the Investigation and Select the Review Team
- Collect the Evidence
- Investigate "**what happened**"
- Analyze "why it happened"
- Define and Report the Judgments of Need and Corrective Actions

The purpose of an accident investigation is to determine:

- The "**what**" went wrong beginning by comparing "work-as-done" to planned work. The purpose is to understand what was done, how it was planned, and identify unanticipated or unforeseeable changes that may have intervened. Establishing the "what" was done tends to result in a forward progression of the sequence of events that defines what barriers failed and how they failed.

- The "**why**" things did not work according to plan comes from a cultural-based assessment of the organization to understand why the employees thought it was OK to do what they did at the time in question. Establishing the "why" tends to be a backwards regression identifying the assumptions, motives, impetus, changes and inertia within the organization that may reveal weaknesses and inadequacies of the barriers, barrier selection, and maintenance processes. The objective is to understand the latent organizational weaknesses and cultural factors that shaped unacceptable outcomes.

Investigative tools provided in this handbook are designed to determine the "what" and the "why." These investigative tools allow investigation teams to systematically explore what failed in the systems used to ensure safety. Rooting out the deeper organizational issues reduces degradation of any system modification put in place.

1.10.2 Determine Deeper Organizational Factors

Having determined "what" went wrong, the investigation team must attempt to use the theory introduced in Chapter 1 to understand how extensive the issues discovered in the investigation are throughout the organization, how long they have been undetected and uncorrected, and why the culture of the organizations allowed this to occur. To answer these questions, the team needs to determine the extent of conditions and causes, attempt to identify the Latent Organizational Weaknesses (those management decisions made in the past that are now starting to set employees up for errors) and attempt to identify underlying cultural issues that may have contributed to these.

A learning organization must determine "what" did not work by performing a compliance-based assessment and understand "why" the organization was allowed to get to this stage by performing a cultural-based assessment. In the Federally-led accident investigation the compliance based assessment is driven by DOE O 225.1B which requires the team investigate policies, standards, and requirements that were applicable to the accident being investigated and to investigate the safety management system that was to be in place to institutionalize the resulting work practices to allow safe work (DOE Policy (P) 450.4A, *Safety Management System Policy*). This is accomplished by reviewing work against the ISM Core Functions. The cultural-based assessment is accomplished by examining three principal culture shaping factors (leadership, employee engagement, organizational learning) which are developed from the ISM Principles.

This output of the deeper organizational issues is much more subjective than previous sections because it is based on the team assimilating information and making educated judgments as to possible underlying organizational causes. The following sections are provided to frame the deeper organizational part of the investigation and the results should be used in conjunction with

the organizational mental model introduced earlier (Figure 1-13: *Level III - High-Level Model for Examining Organizational Drift*).

1.10.3 Extent of Conditions and Cause

The team should determine how long conditions have existed without detection (hints that the organization's assessment and oversight processes are not very effective) and how extensive the conditions are throughout the organization (hints which point to deeper management system issues, indicating a higher level corrective action needed).

As part of this effort, the team should also capture the missed opportunities to catch this event in its early stages such that the event being investigated would not have occurred. A learning organization should be taking every attempt to learn from previous mishaps or near misses (including external lessons learned) and have sufficiently robust process to detect when things are going wrong early in the process.

1.10.4 Latent Organizational Weaknesses

Latent organizational weaknesses are hidden deficiencies in management control processes (for example, strategy, policies, work control, training, and resource allocation) or values (shared beliefs, attitudes, norms, and assumptions) that create workplace conditions that can provoke error (i.e., precursors) and degrade the integrity of defenses (flawed defenses). [Reason, pp. 10-18, 1997][14]

Table 1-1 is a guide, to help identify latent organizational weaknesses - those factors in the management control processes or associated values that influence errors or degrade defenses. Consider work practices, resources, documentation, housekeeping, industrial safety, management effectiveness, material availability, oversight, program controls, radiation employee practices, security work practices, tools and equipment use, training and qualification, work planning and execution, and work scheduling. For an expanded list of examples, see Attachment 1, *ISM Crosswalk and Safety Culture Lines of Inquiry*.

Table 1-1: Common Organizational Weaknesses

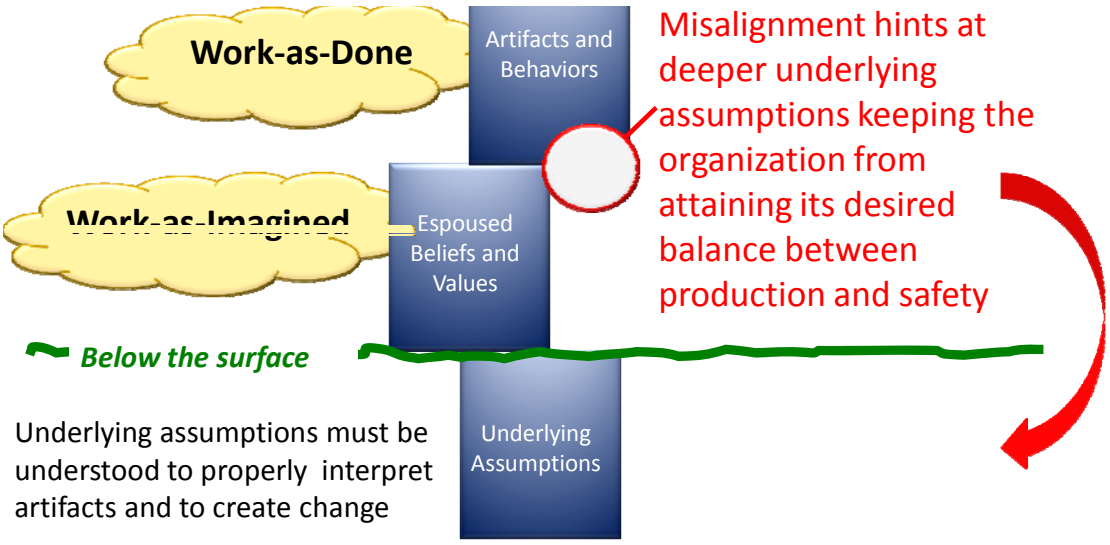
Category	Weakness
Training	Effectiveness of training on task qualification requirement for skill-based tasks. Focus is on lower level of cognitive knowledge. Failure to involve management in training. Training is inconsistent with company equipment, procedures, or process.
Communication	Reinforcement of use of the phonetic alphabet in critical steps to preclude misunderstanding of instructions. Failure to reinforce use of 3-way communications. Failure to use specific unit ID numbers in procedures Unclear priorities or expectations. Unclear roles and responsibilities.
Planning and Scheduling	Provision for contingencies for failures. Failure to consider that multiple components may be out of service. Failure to provide required materials or procedures. Over scheduling of resources. Failure to consider incorrect operation or damage to adjacent equipment. Specific type of work not performed. Specific type of issue not addressed Inadequate resources assigned.
Design or Process Change	Involvement of users in design change implementation. Inadequate training. Inadequate contingencies in case a procedure goes wrong
Values, Priorities, Policies	Management policies on line input into adequacy of procedures or safety features. Too high a priority is placed on schedules. Willingness to accept degraded conditions or performance. Management failure to recognize the need for or importance of related program.
Procedure Development or Use	Consideration of human factors in procedural development and implementation. Failure to perform procedural verification or validation. Failure to reference procedure during task performance. Assumptions made in lieu of procedural guidance. Omission of necessary functions in procedures.

Category	Weakness
Supervisory Involvement	Performance of management observations and coaching. Failure to correct poor performance or reinforce good performance. Unassigned or fragmented responsibility and accountability. Inadequate program oversight
Organizational Interfaces	Interfaces for defining work priorities. Lack of clear lines of communications between organizations. Conflicting goals or requirements between programs Lack of self-assessment monitoring. Lack of measurement tools for monitoring program performance. Lack of interface between programs.
Work Practices	Reinforcement of the use of established error prevention tools and techniques (human performance tools).

1.10.5 Organizational Culture

Insights about safety culture may be inferred by considering aspects of leadership, employee engagement and organizational learning. Observations about culture should be captured reviewed and summarized to distill indicators of the most significant culture observations. These are phrased as positive culture challenges in the report.

An organization's culture, if not properly aligned with safety requirements, could result in ignored safety requirements. A healthy culture exists when the "work-as-done" (culture artifacts and behavior) overlap the "work-as-planned" (espoused beliefs and values) indicating an alignment with the underlying assumptions (those factors felt important to management). A misalignment between actual safety behavior and espoused safety beliefs indicates an unhealthy culture or one in which the employees are not buying into the established safety system or one in which the true underlying assumptions of management is focused on something besides safety (Figure 1-15).



Schein, Organizational Culture and Leadership, 2004

Figure 1-15: Assessing Organizational Culture

Safety culture factors offer important insights about event causation and prevention. Although in-depth safety culture evaluations are beyond the doable scope of most accident investigations, the DOE (with the help of EFCOG) has determined that examining three principal culture shaping factors (leadership, employee engagement, organizational learning) will help to identify cultural issues that contributed to the event. These factors were developed from the ISM Principles by the EFCOG Safety Culture Working Group in 2007.

Leadership

Leadership and culture are two sides of the same coin; neither can be realized without the other. Leaders create and manage the safety culture in their organizations by maintaining safety as a priority, communicating their safety expectations to the workers, setting the standard for safety through actions not talk (walk the talk), leading needed change by defining the current state, establishing a vision, developing a plan, and implementing the plan effectively. Leaders cultivate trust to engender active participation in safety and to establish feedback on the effectiveness of their organization's safety efforts.

- Leaders assure plans integrate safety into all aspects of an organization's activities considering the consequences of operational decisions for the entire life-cycle of operations

and the safety impact on business processes, the organization, the public, and the environment.

- Leaders understand their business and ensure the systems employed provide the requisite safety by identifying and minimizing hazards, proving the activity is safe, and not assuming it is safe before operations commence.

- Leaders consider safety implications in the change management processes.

- Leaders model, coach, mentor, and reinforce their expectations and behaviors to improve safe business performance.

- Leaders value employee involvement, encourage individual questioning attitude, and instill trust to encourage raising issues without fear of retribution.

- Leaders assure employees are trained, experienced and have the resources, the time, and the tools to complete their job safely.

- Leaders hold personnel accountable for meeting standards and expectations to fulfill safety responsibilities.

- Leaders insist on conservative decision making with respect to the proven safety system and recognize that production goals, if not properly considered and clearly communicated, can send mixed signals on the importance of safety.

- Leadership recognizes that humans make mistakes and take actions to mitigate this.

- Leaders develop healthy, collaborative relationships within their own organization and between their organization and regulators, suppliers, customers and contractors.

Employee/Worker Engagement

Safety is everyone's responsibility. As such, employees understand and embrace the organization's safety behaviors, beliefs, and underlying assumptions. Employees understand and embrace their responsibilities, maintain their proficiency so that they speak from experience, challenge what is not right and help fix what is wrong and police the system to ensure them, their co-workers, the environment, and the public remain safe.

- Individuals team with leaders to commit to safety, to understand safety expectations, and to meet expectations.

- Individuals work with leaders to increase the level of trust and cooperation by holding each other accountable for their actions with success evident by the openness to raise and resolve issues in a timely fashion.

- Everyone is personally responsible and accountable for safety, they learn their jobs, they know the safety systems and they actively engage in protecting themselves, their co-workers, the public and the environment.

- Individuals develop healthy skepticism and constructively question deviations to the established safety system and actively work to avoid complacency or arrogance based on past successes.

- Individuals make conservative decisions with regards to the proven safety system and consider the consequences of their decisions for the entire life-cycle of operations.

- Individuals openly and promptly report errors and incidents and don't rest until problems are fully resolved and solutions proven sustainable.

- Individuals instill a high level of trust by treating each other with dignity and respect and avoiding harassment, intimidation, retaliation, and discrimination. Individuals welcome and consider a diversity of thought and opposing views.

- Individuals help develop healthy collaborative relationships within their organization and between their organization and regulators, suppliers, customers and contractors.

Organizational Learning

The organization learns how to positively influence the desired behaviors, beliefs and assumptions of their healthy safety culture. The organization acknowledges that errors are a way to learn by rewarding those that report, sharing what is wrong, fixing what is broken and addressing the organizational setup factors that led to employee error. This requires focusing on reducing recurrences by correcting deeper, more systemic causal factors and systematically monitoring performance and interpreting results to generate decision-making information on the health of the system.

- The organization establishes and cultivates a high level of trust; individuals are comfortable raising, discussing and resolving questions or concerns.

- The organization provides various methods to raise safety issues without fear of retribution, harassment, intimidation, retaliation, or discrimination.

- Leaders reward learning from minor problems to avoid more significant events.

- Leaders promptly review, prioritize, and resolve problems, track long-term sustainability of solutions, and communicate results back to employees.

- The organization avoids complacency by cultivating a continuous learning/improvement environment with the attitude that "it can happen here."

- Leaders systematically evaluate organizational performance using: workplace observations, employee discussions, issue reporting, performance indicators, trend analysis, incident investigations, benchmarking, assessments, and independent reviews.

- The organization values learning from operational experience from both inside and outside the organization.

- The organization willingly and openly engages in organizational learning activities.

1.11 Experiential Lessons for Successful Event Analysis

A fundamental shortcoming of some investigative techniques is that they do not address where the physics could fail, based on perceptions of improbability due to lack of recent evidence (it has happened before). People, equipment, and facilities only get hurt or damaged when energy flows to where it does not belong. Investigations must determine where the physics could fail in order to prevent potential bad consequences.

"System Optimism" is the belief that systems are well designed and well maintained, procedures are complete and correct, designers can foresee and anticipate every situation, and that people behave as they are expected to or as they were taught. This is the "work-as-imagined" by the organizational management culture. In this view, people are a liability and deviation from the "work-as-imagined" is seen as a threat to safety that needs to be eliminated. In other words, this is the perception that errors are caused by the individuals who made them; correct or remove the errant individual and the problem is fixed.

"System Reality" is the belief that things go right because people learn to overcome design flaws and functional glitches, adapt their performance to meet demands, interpret and apply procedures to match conditions, and can detect and correct when things go wrong. In this view, people are an asset and the deviation from the "work-as-imagined" is seen as how workers have to adapt to successfully complete the work within the time and resources constraints that exist for that task. In other words, if the worker is adapting incorrectly, the fault is in the conditions and methods available to adapt.

Rather than simply judging a decision as wrong in retrospect, the decision needs to be evaluated in the context of contributing factors that explain why the decision was made. If the investigation stops with worker's deviation as the cause, nothing is corrected. The next worker, working in the same context, will eventually adapt in a similar fashion and deviate from "work-as imagined." Performance variability is not limited to just the worker who triggers the accident. People are involved in all aspects of the work, including variation in the actions of the co-workers, the expectations of the leaders, accuracy of the procedures, the effectiveness of the defenses and barriers, or even the basic policies of the organization can influence an outcome. This is reflected in the complex, non-linear accident model where unexpected combinations of normal variability can result in the accident. Failure to follow up with lessons-to-be-learned and validations of corrective actions and Judgment of Needs can certainly lead to a recurrence of an event.

Glossary

Accident: An unwanted transfer of energy or an environmental condition that, due to the absence or failure of barriers or controls, produces injury to persons, damage to property, or reduction in process output.

Accident Investigation: The systematic appraisal of unwanted events for the purpose of determining causal factors, subsequent corrective actions, and preventive measures.

Accident or Emergency Response Team: A team or teams of emergency and accident response personnel for a particular site. This team may be composed of a number of teams from the site, such as local police and firefighter units, emergency medical personnel, and hazardous material teams.

Analysis: The use of methods and techniques for arranging data to: (a) assist in determining what additional data are required; (b) establish consistency, validity, and logic; (c) establish necessary and sufficient events for causes; and (d) guide and support inferences and judgments.

Analytical Tree: Graphical representation of an accident in a deductive approach (general to specific). The structure resembles a tree—that is, narrow at the top with a single event (accident) and then branching out as the tree is developed, and identifying root causes at the bottom branches.

Appointing Official: A designated authority responsible for assigning Accident Investigation Boards for investigations, with responsibilities as prescribed in DOE O 225.1B.

Barrier: Anything used to control, prevent, or impede energy flows. Common types of barriers include equipment, administrative procedures and processes, supervision/management, warning devices, knowledge and skills, and physical objects.

Barrier Analysis: An analytical technique used to identify energy sources and the failed or deficient barriers and controls that contributed to an accident.

Board Chairperson: The leader who manages the accident investigation process, represents DOE in all matters regarding the accident investigation, and reports to the appointing official for purposes of the accident investigation.

Board Members: A group of three to six DOE staff assigned to investigate an accident. This group reports to the Board Chairperson during the accident investigation.

Causal Factor: An event or condition in the accident sequence necessary and sufficient to produce or contribute to the unwanted result. Causal factors fall into three categories:

- Direct cause
- Contributing cause
- Root cause.

Cause: Anything that contributes to an accident or incident. In an investigation, the use of the word "cause" as a singular term should be avoided. It is preferable to use it in the plural sense, such as "causal factors," rather than identifying "the cause."

Chain of Custody: The process of documenting, controlling, securing, and accounting for physical possession of evidence, from initial collection through final disposition.

Change: Stress on a system that was previously in a state of equilibrium, or anything that disturbs the planned or normal functioning of a system.

Change Analysis: An analytical technique used for accident investigations, wherein accident-free reference bases are established, and changes relevant to accident causes and situations are systematically identified. In change analysis, all changes are considered, including those initially considered trivial or obscure.

Conclusions: Significant deductions derived from analytical results. Conclusions are derived from and must be supported by the facts, plus results from testing and analyses conducted. Conclusions are statements that answer two questions the accident investigation addresses: what happened and why did it happen? Conclusions include concise recapitulations of the causal factors (direct, contributing, and root causes) of the accident determined by analysis of facts.

Contributing Cause: An event or condition that collectively with other causes increases the likelihood of an accident but that individually did not cause the accident.

Controls: Those barriers used to control wanted energy flows, such as the insulation on an electrical cord, a stop sign, a procedure, or a safe work permit.

Critical Process Step: A step in the process where potential threats could interact with the hazard that could be released. For accident analysis, the absence of hazards or threads in a process step makes it a non-critical step.

Direct Cause: The immediate events or conditions that caused the accident.

DOE Accident Investigator: An individual who understands DOE accident investigation techniques and has experience in conducting investigations through participation in at least one Federal investigation. Effective October 1, 1998, DOE accident investigators must have attended an accident investigation course of instruction that is based on current materials developed by the Office of Corporate Safety Programs.

DOE Operations: Activities funded by DOE for which DOE has authority to enforce environmental protection, safety, and health protection requirements.

DOE Site: A tract either owned by DOE, leased, or otherwise made available to the Federal government under terms that afford DOE rights of access and control substantially equal to those it would possess if it held the fee (or pertinent interest therein) as agent of and on behalf of the government. One or more DOE operations/program activities carried out within the boundaries of the described tract.

Energy: The capacity to do work and overcome resistance. Energy exists in many forms, including acoustic, potential, electrical, kinetic, thermal, biological, chemical, and radiation (both ionizing and non-ionizing).

Energy Flow: The transfer of energy from its source to some other point. There are two types of energy flows: wanted (controlled—able to do work) and unwanted (uncontrolled—able to do harm).

Event: An occurrence; something significant and real-time that happens. An accident involves a sequence of events occurring in the course of work activity and culminating in unintentional injury or damage.

Events and Causal Factors Chart: Graphical depiction of a logical series of events and related conditions that precede the accident.

Eyewitness: A person who directly observed the accident or the conditions immediately preceding or following the accident.

Fatal Injury: Any injury that results in death within 30 calendar days of the accident.

Field Element: A general term for all DOE sites (excluding individual duty stations) located outside the Washington, D.C., metropolitan area.

General Witness: A person with knowledge about the activities prior to or immediately after the accident (the previous shift supervisor or work controller, for example).

Hazard: The potential for energy flow(s) to result in an accident or otherwise adverse consequence.

Heads of Field Elements: First-tier field managers of the operations offices, the field offices, and the power marketing administrations (administrators).

Human Factors: The study of human interactions with products, equipment, facilities, procedures, and environments used in work and everyday living. The emphasis is on human beings and how the design of equipment influences people.

Investigation: A detailed, systematic search to uncover the "who, what, when, where, why, and how" of an occurrence and to determine what corrective actions are needed to prevent a recurrence.

Investigation Report: A clear and concise written account of the investigation results.

Judgments of Need: Managerial controls and safety measures necessary to prevent or minimize the probability or severity of a recurrence of an accident.

Lessons Learned: A "good work practice" or innovative approach that is captured and shared to promote its repeated application. A lesson learned may also be an adverse work practice or experience that is captured and shared to avoid recurrence.