CHAPTER 3 – MANAGING DEFENSES

DEFENSES

In this chapter, the reader will become familiar with defenses as they relate to DOE facilities. From that introduction, the reader will gain an appreciation of the importance of defenses in controlling events. The various categories or lines of defenses used in the industry and their relative dependability will be addressed. Most importantly, the reader will learn how to identify and eliminate latent organizational conditions in the system that weaken defenses by using a variety of available and familiar method (tools) that are introduced herein.

Defenses are extremely important in DOE facilities, because they are put in place to control a kind of invader, active human error—the primary hazard to the facility. Successful defenses prevent or mitigate the severity of events. Defenses and barriers are important to understanding and preventing accidents.

- An accident only occurs when one or more defenses have failed; either they did not serve their purpose or they were missing.
- Once the origin of an accident has been determined and the causes identified, defenses and barriers can be used as a means to prevent the same or a similar accident from taking place in the future.[1]

The Chernobyl Unit 4 nuclear reactor accident in the Ukraine on April 26, 1986, is a classic example of multiple failed or missing defenses—some resulting from design flaws and some from the errors of operators. The schedule that day called for a safety demonstration test to determine how long the turbines could provide electrical power from residual momentum alone in the event of a power loss.[2]

Operators failed in their role as the most important line of defense because they did the following.

(1) **Violated safe operating parameters –** Operators unwisely decided to continue the testing of the voltage generator, even though an initial operating error had caused the power level to fall to 7 percent of full power. The station operating procedures strictly prohibited any operations below 20 percent of full power. Operations at these low-power levels created a positive void coefficient in the reactor's core, which can lead to runaway reactivity. The operators should have aborted the test completely and returned the reactor to normal power to prevent this, but they did not.

(2) **Disabled engineered safety systems –** Operators subsequently disabled the emergency cooling and shutdown systems in order to complete the experiment by controlling the reactor themselves. That operators could physically disable these safety systems was indeed a flaw in the design of the system.

(3) **Retracted control rods beyond regulations –** When power dropped too low, operators forcibly raised power by retracting the control rods to an extreme level—much greater than that allowed by regulations. Here again a design flaw allowed such a manipulation. During the test, steam flow to the turbines was reduced. Thus, heat was not being carried away from the core as normal. When temperature in the core increased rapidly, giving rise to more boiling and

increasing reactivity, an operator attempted a manual scram. The operator likely did not understand the consequences of his actions. Rather than slow down reactivity, insertion of the graphite-tipped control rods caused quite the opposite effect. The power surge triggered multiple steam explosions. The reactor vessel head was blown off, and, in a second chemical explosion, the roof of the building was blown off.

(4) **Design flaw: No containment –** The RBMK reactor design did not include a steel- reinforced concrete containment structure present in all other reactor designs. The presence of a containment structure would have precluded the release of aerosolized fuel and fission products into the environment. Instead, there was a total meltdown of the fuel and fire in the reactor housing burned for 10 days, dispensing radionuclides into the atmosphere.

The Chernobyl accident took dozens of lives, completely destroyed the plant, and forced relocation of tens of thousands of people. Adverse impacts to the environment continue to this day.

Defenses comprise any human, technical, or organizational features that protect the facility and personnel against hazards.[3] In addition to human error, other hazards include radiation, industrial safety, hazardous chemicals, and various forms of energy, such as electricity and rotating equipment. Defenses can prevent a hazard, mitigate consequences, or warn. Defenses take the form of containments; physical interlocks; redundant equipment, power sources, and annunciators; personal protective equipment; procedure use; caution tags; and self-checking, among others

Defenses are built into our everyday lives. We will consider two examples—fire protection and driving a car. Take the defenses against a fire in your home. There are fire-resistant building materials (*exterior:* brick, stucco, or cement-based siding, metal or tile roofs, steel doors, and so on.; *interior:* metal studs, sheetrock walls and ceilings, ceramic tile flooring, and so on). Ground-fault interrupter (GFI) circuit breakers automatically cut off electricity when they sense shorts in the circuit. The above defenses guard against a fire starting or they slow its spread in the event of a fire. Smoke detectors and alarms warn of danger should a fire start. Fire extinguishers, fire hydrants and hoses, and the local firemen are defenses that control and put out a fire if it should break out.

There are many defenses associated with driving an automobile. Traffic lights signal drivers to proceed or stop at an intersection. Speedometers help drivers control vehicle speed. Drivers' licenses provide proof that people are qualified to operate an automobile. Seatbelts and air bags mitigate the effects of collisions. Ripples built into the edges of asphalt highways alert drivers with a rumbling noise when the vehicle is riding on the edge of the road. Likewise, defenses in the facility take the form of procedures; physical interlocks; redundant equipment, power sources, and annunciators; as well as those that rely on people, such as self-checking, peer-checking, three-way communication, reviews and approvals, and supervisory oversight.

Severity of Events

The significance, or severity, of a particular event lies in the *consequences* suffered by the physical plant or personnel, not the error that initiated the event.[4] The error that causes a serious accident and the error that is one of hundreds with no consequence can be the same error that has historically been overlooked or uncorrected. For a significant event to occur, multiple breakdowns in defenses or barriers must first occur. Whereas human error typically triggers an event, it is the number of defenses and the weaknesses of those defenses that dictate the severity of the event.

The existence of many flawed defenses is directly attributable to weaknesses in the organization or management control systems. Individual error-prevention practices are important and need to be implemented and maintained. However, to focus only on error reduction to prevent events is a bad strategy for this reason. Error reduction can only reduce the time between events. The greater successes in minimizing the occurrence of severe events are realized by focusing on defense-in-depth. Improving defenses will minimize severity. Therefore, one of management's top priorities must be verifying the integrity of defenses.

The Organization's Role in Defenses

Human performance occurs within the context of the organization—its processes, physical structures and culture. It is the organization that acquires, organizes, and makes use of resources (people, money, and equipment) in support of facility operations. When facility operations fail to accomplish what is intended, events are the results. Significant events triggered by human error are rightfully characterized as *organizational failures.* Significant events, excessive DOE oversight, and extended facility shutdowns are reflective of severe organizational failures. At the other extreme, facilities that demonstrate sustained operational excellence are managed by strong organizations that execute processes effectively and whose workforce adheres to high standards.

Defense Functions

Defenses serve various functions, including the following.[5]

- **Create Awareness** – understanding the risks and hazards and recognizing the presence of hazards. Examples include pre-job briefings, post-job reviews, risk assessments, procedures, component labeling, color-coding, self-checking, computer screen layout, logs, meetings, communication practices, danger tags, and radiological postings.
- **Detect and Warn –** alerted to the presence of off-normal conditions or imminent dangers. Examples include alarms and annunciators, equipment operator rounds, concurrent verification, peer-checking, supervision, confined-space entry requirements, self-checking, and problem-solving methodology.
- **Protect** – guarding people, equipment, and the environment from error or harm. Examples include personal protective equipment, supervision, equipment lockout, interlocks, shielding, and ventilation.

- **Recover** – restoration from off-normal conditions and restoring the system to a safe state. Examples include independent verification, emergency procedures, eye wash stations, pre-established response procedures, continuity of operations plans, re-entry teams, and decontamination.
- **Contain** – restricting or limiting the accidental release of harmful energy or substances. Examples include double-shell storage tanks, glove boxes, remote manipulations, tank berms, piping and valves, and containment.
- **Enable Escape** – providing the means to flee from uncontrolled hazard. Examples include emergency plans, crash bars on doors, emergency lighting, and network installation management (NIM) routes.

DEFENSE-IN-DEPTH

Defenses themselves are not necessarily perfect. Multiple, overlapping defenses are needed to compensate for this reality. Defense-in-depth is achieved by imbedding defenses in an overlapping fashion into the organization, its culture, and the physical facility. Thus, if one defense fails or is ineffective, other systematically placed redundant defenses will fulfill the same defensive function. Controls include various devices, methods, or practices that make an activity or process go safely and predictably to protect key assets from human error. Four types of lines of defense—engineered, administrative, cultural, and oversight controls—work together to anticipate, prevent, or catch active errors from causing a significant event. An explanation of each of these four types of defense, as well as examples and common flaws associated with each follow.

Engineered Controls

Engineered design controls are all those hardware, software, and equipment items in the physical environment that affect people's behavior, choices, and attitudes, and are a result of engineering design. Engineered controls act either actively or passively. Active controls include equipment such as pumps or valves that perform a specific safety-related function. Passive controls include pipes, vessels, and berms that provide containment and generally do not have moving parts. The most reliable defense mechanisms are passive because they require no operational or maintenance support to remain effective, eliminating dependence on human involvement.

- Example: Engineered Controls

  The *human-machine* environment contains several opportunities to "control" human error. Human-centered designs consider human error and its potential consequences, eliminating or minimizing error traps with equipment. Consideration is given to the habitability and accessibility of the physical work environment. Unnecessary human interactions with facility equipment are either eliminated or automated. Otherwise, interlocks and error-tolerant designs have to be used to mistake-proof human-machine interactions, especially those with risk-important systems and critical components.

  Interlocks and protection systems are provided to prevent improper operator actions and to initiate automatic protective actions when necessary. Interlocks and

protection systems will not prevent all possible operator errors, but they can substantially reduce the risks if they are properly maintained. Supervisors initiate modifications to eliminate or minimize errors associated with workarounds and human-machine interface deficiencies. These actions are especially important at critical steps. Other important elements relevant to effective engineered controls include configuration control, material condition, foreign material exclusion (FME), and housekeeping practices. Problems with environmental conditions, labeling, accessibility, lighting, and habitability are resolved, if possible, to minimize their impact on performance, especially on risk-important equipment. These are administrative controls in support of the engineered controls.

- **Common Flaws with Engineered Controls**

  The following list highlights some of the more common equipment-related conditions that challenge worker performance and can contribute to facility events:
  - out-of-service equipment, controls, alarms, and indicators;
  - workarounds, temporary repairs, or long-term temporary modifications/alterations;
  - nuisance alarms and disabled annunciators;
  - excessive noise;
  - missing labels or labels oriented such that they cannot be seen or read easily;
  - poor lighting;
  - high temperatures or high humidity (heat stress factors);
  - unusual plant or equipment conditions; and
  - poor accessibility, cramped conditions, or awkward layout of equipment.

Administrative Controls

Administrative controls, such as procedures, inform people about what to do, when to do it, where it is to be done, and how well to do it, and are usually documented in various written policies, programs, and plans. Administrative controls rely on human judgment, training, and personal initiative to follow the direction contained in documents. Consequently, administrative controls are not as reliable as engineered controls.

- **Example: Administrative Controls**

  A wide range of management methods exists to ensure proper facility operations and to control various hazards. Administrative controls that significantly impact human performance include the following:
  - strategic business planning (goals, budgeting, priorities, plans, resource acquisition, and so forth);
  - formal organizational structure, lines of authority, roles, and responsibilities;
  - policies, programs, and processes for the conduct of production work activities (preventive maintenance, procedure development, modifications, configuration control, operations, and so forth);

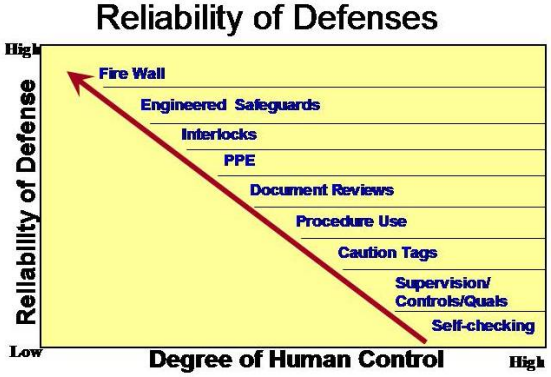
- communication methods (conversations, e-mail, logs, meetings, reports, newsletters, signs, postings, telephones, radios, alarms, and so on);
- technical and administrative procedures (clearances/tagging, foreign material exclusion, industrial safety, human performance, troubleshooting, records, parts and materials, self-assessment, corrective action, and so forth);
- training programs;
- work management processes (work initiation, prioritization, review and approval, planning, and scheduling);
- human resources policies and practices related to staffing levels, overtime, and discipline;
- human performance tools, expectations, and standards; and
- information technology and information handling.

- **Common Flaws with Administrative Controls**

  The following administrative conditions, among others, can be causes or contributing factors in facility events:
  - two or more actions embedded in one procedure step;
  - vague expectations and standards;
  - superficial document reviews or the lack of a "qualified reviewer" process for technical procedure development;
  - critical steps not identified in procedures and work packages;
  - excessive work package backlog that exceeds planner resources;
  - work packages planned without inclusion of operating experience;
  - unresponsive procedure revision process;
  - unavailable foreign material exclusion (FME) caps and covers;
  - excessive deferred preventive maintenance;
  - insufficient staffing leading to excessive overtime, workload, and fatigue;
  - routine authorization to exceed overtime limits (leading to chronic fatigue);
  - inadequate time for direct supervision of work in the field;
  - unclear qualification standards; and
  - incomplete or missing electrical load lists to aid in ground isolation.

Reliability of Defenses

As might be expected, some defenses are more reliable than others. Controls, barriers, or safeguards tend to be more reliable defenses when they are not dependent on people to carry out their protective functions. In general, physical defenses



tend to perform their intended functions despite human action or inaction. Engineered controls, such as physical interlocks and equipment design, are more reliable than administrative controls, such as procedures, human performance tools, and training programs. When the effectiveness of a defense mechanism relies on the performance of people—as do procedures, training, self-checking, and verifications—then it is less reliable. When plant safety and reliability are dependent on people during risk-important activities, the physical plant is more vulnerable to their errors. Reliability is related to the dependability of the defense or barrier to perform its intended function when needed. If it is imperative to prevent error, then physical, engineered controls are more appropriate.

Cultural Controls – Values, Beliefs, Attitudes

An effective safety culture engenders the belief that when production and safety conflict, safety will prevail. Cultural controls include those leadership practices that teach (consciously or unconsciously) people how to perceive, think, feel, and behave toward challenges to safety.[6] Culture is defined by people's behavior, and safe behavior is value-driven.[7] What an organization says its values are may not be reflected in its behavior. The true values of an organization are reflected in the observed acts of its people, especially its managers.[8] What an organization says its values are may not be reflected in its behavior. For instance, when procedures are vague or incomplete, people tend to default to what they think is important for success as they define it. The true values of an organization are reflected in the observed acts of its people, especially its managers.

Organizational culture comprises a set of *shared* assumptions, values, and beliefs that characterize the choices and behaviors of the members in an organization. Culture is for the group what character and personality are for the individual. Because of the special nature of hazards present at DOE facilities, organizations that work in these facilities need a *strong* safety culture. "Strong" implying the extent to which the organization's members adopt or internalize such values and behaviors. More will be said about culture in Chapter 5.

Values What managers place importance on and what is considered "high priority" becomes valued in the organization, whether this is publicly espoused or not. Key management values are usually visible at the site or at the facility in meeting rooms and conspicuous, high-traffic areas (both in the facility and outside the facility) where everyone sees them. When workforce behaviors become consistent with management's espoused values over the long term, then the organization has truly internalized those values.

Beliefs What people believe (or perceive) to be true tends to drive their attitudes and behavior. A belief is an acceptance of and conviction in the truth, existence, or validity of something, including assumptions about what will be successful. People erroneously believe they can always maintain control whenever and wherever. Typically, this is the case when people decide to take shortcuts or violate a safety policy. This belief changes as people understand the realities associated with human performance. The following beliefs have a significant positive impact on event-free performance.

- Absolutely safe environments do not exist.

- Human beings are fallible.
- People want to do a good job.
- Human error is normal.
- There is no such thing as a "routine" task or activity.
- Significant events are organizational failures.
- Error presents an opportunity to learn and improve organizational effectiveness.

Attitudes An attitude is a state of mind, or feeling, toward an object or subject. Importantly, attitudes affect people's choices and behaviors toward safety and error prevention. Positive feelings follow safe behaviors when people experience positive and consistent feedback from supervisors and peers and they understand why the feelings are important. If people experience negative feelings when they use safe behaviors (pain, fear, anxiety, frustration, humiliation, embarrassment, boredom, or discomfort) they will tend to avoid those behaviors and practices. The following attitudes promote safe work behaviors.

- **Uneasiness toward human fallibility** – individuals acknowledging their capacity to err, to make a mistake or slip at any time, and being wary of conditions conducive to error; tending to follow procedures carefully and applying human performance tools rigorously.
- **Questioning attitude** – maintaining vigilant situation awareness toward surrounding working conditions to detect error-likely situations, unsafe or hazardous working conditions, or otherwise unusual conditions; not proceeding in the face of uncertainty and basing decisions on facts
- **Conservative approach** – taking actions or making decisions that err in the direction of safety rather than production, especially when doubt exists; exhibited by placing systems, equipment, or the facility in a safe condition before stopping an activity.
- **Avoiding "unsafe" attitudes** – being aware of and avoiding attitudes and practices detrimental to high levels of reliability, such as Pollyanna, summit fever, heroic, pride, fatalism, and invulnerability to error

Work Group Norms

A person's peer group is the largest, single determinant of an individual's behavior on the job. Norms tell people what they are supposed to do, wear, say, and believe; what is acceptable and what is unacceptable; what to look for; what to ignore; how to see things; and how to interpret what they see and hear. Norms are passed on by word of mouth and are enforced by how a person's peers respond when a norm is broken.[9] If work group members think one person is working too hard, they may make jokes and unkind remarks to the person until he/she adopts the group's norm for what is considered an appropriate level of effort. In extreme cases, the peer group may shun or attack the person until he or she complies with the group's "rules."

Leadership Practices

Nothing drives a culture more than management's style and response to various challenges or opportunities. Management, through the following leadership practices as described in Chapter 5, "Culture and Leadership," tends to shape the culture of the staff through the following:

- facilitating communication;
- promoting teamwork;
- coaching and reinforcing expectations;
- eliminating latent organizational weaknesses; and
- valuing the prevention of error.

Common Flaws with Cultural Controls

Sometimes it is easier to know when a culture is unhealthy by observing the practices, choices, interactions, and decisions of the organization's personnel. The following examples illustrate some flawed cultural controls:

- placing importance on personal judgment;
- being overly confident in one's own abilities to solve problems;
- being reluctant to challenge the decisions of others;
- relying only on one's own resources;
- applying human performance tools carelessly;
- lacking correction or coaching of at-risk practices, or using human performance tools improperly;
- having inconsistencies between what managers say they want and what they reward or pay attention to;
- making uncritical observation comments so as to not offend those observed;
- initiating disciplinary action for honest mistakes;
- providing bonuses based solely on productivity measures; and
- proceeding to the next action or step before signing off concurrent verification.

Oversight Controls

Vulnerabilities with defenses can be found and corrected when management decides it is important enough to devote resources to the effort. The very nature of latent conditions is such that they will not self-reveal, they must be discovered. The fundamental aim of oversight is to improve facility resilience to significant events triggered by active errors in the workplace—that is, to minimize the severity of events. Oversight controls provide opportunities to see what is actually going on in the facility, to identify specific vulnerabilities or performance gaps, to take action to address those vulnerabilities and performance gaps, and to verify that they have been resolved.

Senior Management Team Focus on Human Performance

Since human error is one of the greater sources of risk to the facility, the senior management team must give it careful and regular consideration. Instituting a standing working group structure to monitor human performance has proven successful. This structure promotes management awareness of current challenges to human

performance and their effects on performance. This group establishes the vision, strategy, and processes for managing human performance toward a vision of event-free operations. The members of the senior management team, as an example, may serve on a *Human Performance Steering Committee.*

The steering committee or equivalent promotes accountability for human performance at the department-manager level using various measures of human performance, self-assessments, the corrective action program, and other sources of feedback. Managers closely monitor human performance events and trends, evaluate their causes and contributors, and communicate the results to personnel to increase their understanding and awareness. This system of accountability helps verify that human performance processes and changes are implemented as intended, consistent with the organization's purposes, resources, and goals; that expectations are performed to stated standards; and that performance gaps are identified and closed.

Performance Improvement Processes

Systematic performance improvement processes promote continuous improvement. However, weaknesses with oversight and performance improvement have contributed to long-term poor performance. The following flawed oversight controls tend to degrade this line of defense.

- Senior management oversight of the human performance is inadequate.
- Meetings of the Human Performance Steering Committee are held irregularly.
- Self-assessments are not focused on important attributes, or are not formally performed or tracked.
- The measurement and trending of risk-important processes are insufficient or are not performed.
- Root cause analyses are shallow and focus on individual errors without addressing organizational contributors to events.
- There is a lack of rigorous observations of work in the field.
- Managers are unaware of current human performance challenges in their organizations.
- Performance indicators of human performance are ineffective or are not in place.
- Expectations for change management are inadequate.

Human Performance Improvement Plans

Human performance improvement plans (HPIP) provide management with a systematic approach for correcting identified problems. Without plans, improvement is unlikely and rework is probable. An ongoing HPIP addresses the latest challenges to safety related to human performance. The HPIP, a living plan that is updated as new issues emerge, is reviewed during every Human Performance Steering Committee meeting to verify improvement is actually occurring.

PERFORMANCE MODEL

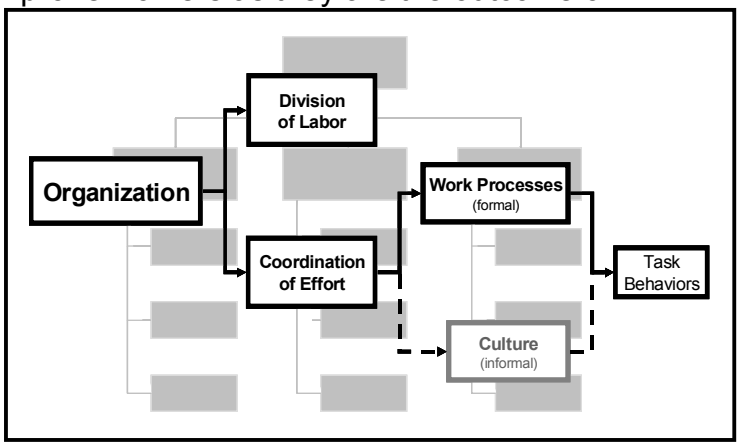
Human Performance –A system is a network of elements that function together to produce an outcome. A facility contains numerous systems, among them, the electrical system, the water circulation system, the work process system, the telephone system,

the fire suppression system, and the heating, ventilation, and air conditioning (HVAC) system. There are also numerous intangible systems that function in the facility environment. For instance, the social system, the organizational system, incentives and disincentives systems, and belief systems are examples that typically function behind the scenes. *Human performance can also be considered a system.*

Understanding organizational systems and the impact of facility processes and values and leadership dynamics on performance is important to improving human performance. Systems- thinking involves pondering the multiple causes and effects, the variables that come to bear on the worker at the point of touching equipment in the facility.

An organization is defined as a group of individuals, including managers, supervisors, and workers, with a shared purpose or mission and means (processes) to efficiently apply resources toward the safe and reliable (values) design, construction, operation, and maintenance of the physical facility. Recall that the third principle of human performance states: *individual behavior is influenced by organizational processes and values.* Thus, human performance does not take place in a vacuum. Rather, performance occurs within the confines of the organization. No matter how well work is organized, how good procedures are, how well equipment is designed, or how well teamwork is achieved, people will never perform better than what the organization will support.[10]

Workers are not "free agents" mentally in the workforce. Procedures, policies, programs, training, and even culture influence worker behavior. The organization affects all of these. As illustrated in the *Anatomy of an Event,* (Chapter 1), organization and the associated management control systems are the prevalent origins of events. Events are not so much the result of error-prone workers as they are the outcome of error-prone tasks and error-prone work environments, which are controlled by the organization.[11]



There is a direct cause-and-effect relationship between the organization and the individual performer. It is the organization that determines the division of labor and the coordination of effort—what people do, when they do it, under what conditions it is accomplished, and how well it is to be done.[12] Roles and responsibilities have to be clearly determined.

Organizational Effectiveness

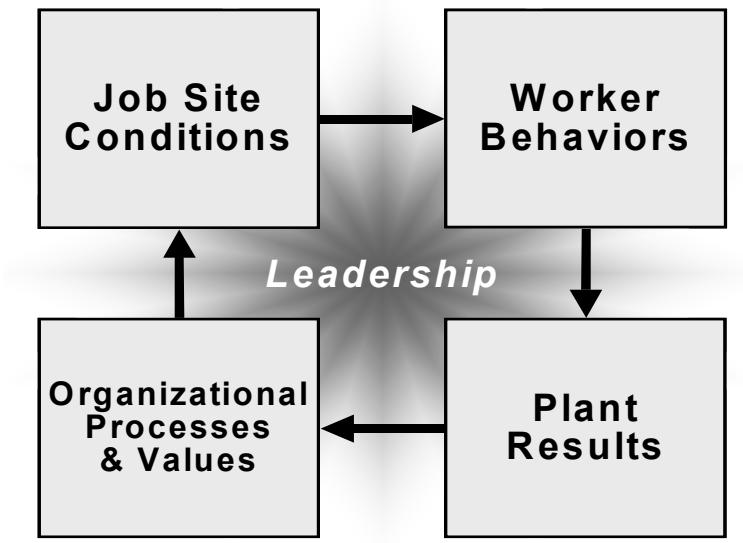
Organizational effectiveness is the ability of an organization to accomplish its goals efficiently. To achieve organizational effectiveness, the management team must organize it resources, especially its people. Organizing involves determining the *division of labor* and *coordinating the effort* as shown in the graphic on organization. Establishing functions, goals, roles and responsibilities, structure, and job assignments

determines the division of labor. Managers pay attention to the tools of the organization—things typically written on paper (the administrative control system). They use formal policies, business plans, priorities, directives, goals and objectives, programs, processes, planning and scheduling, action plans, and expectations and standards to provide direction and controls to accomplish the facility's mission. The purpose of controls is to make processes (or tasks) go smoothly, properly, and according to high standards.[13]

Managers shoulder the responsibility for overall facility performance. To discharge their responsibilities, managers use work processes as the primary mechanism to coordinate work.[14] Functions carried out by managers to establish work processes include:

- deciding the administrative and functional structure needed to establish a standardized sequence of tasks to be accomplished;
- developing and approving procedures to direct workers production and maintenance tasks;
- training people to do the work, specifying what, how, why, and when they are expected to accomplish their tasks;
- establishing processes that provide feedback and identify opportunities for improvement; and
- setting priorities of the organization.

The effectiveness of work processes is improved when managers communicate clear expectations to the workers, when they promote open communication, and when they strive for quality procedures and make use of an effective corrective action program.



The *Performance Model* in the box is a simple, cause-and-effect model of these interdependencies that shows the organizational nature of human performance. The individual boxes in the model represent either conditions or action, and arrows indicate influence or causality.

Organizational Factors

Organizational Factors have a strong influence on human performance. Organizational factors encompass all the ways management uses to direct and coordinate the work of the facility, which together shape the behavior of the people performing their jobs.[15] Collectively, they are the hub of all that goes on at the facility. Organizational factors reveal themselves in engineered controls, administrative controls, cultural controls, and oversight controls (corporate and independent). Some of the more important organizational factors known to impact performance are the following:[16]

- communication methods and practices
- management styles and degree of workforce participation
- tools and resources
- procedure development and review
- cleanliness of the work environment
- layout of facilities and structures
- staffing levels
- experience level of the workforce
- design and modification
- work processes
- management visibility
- human resources policies and practices
- training programs
- priorities (production and safety)
- expectations and standards
- emphasis on health and safety
- work planning and scheduling

For specific jobs or tasks, organizational factors create a unique array of job-site conditions (work environment)—good or bad—that set people up for either success or failure.

Job-Site Conditions

These factors define the unique set of conditions for a particular worker about to perform a specific task or action. The job site is that location or place where behavior occurs during task performance and can be characterized by either environmental or individual factors. Environmental factors (overarching both from the organization and the work environment) include conditions external to the individual and often beyond his or her direct control, such as procedure quality, component labeling, human-machine interface, heat, and humidity. Individual factors include conditions that are a function of the person assigned the task, some of which are also beyond his or her direct control, such as knowledge, skills, experience, family problems, and color blindness.

Workplaces and organizations are easier to manage than the minds of individuals workers. You cannot change the human condition, but you can change the conditions under which people work.

Dr. James Reason Human Error

A special subset of job-site conditions that provoke human error are called error precursors (described in Chapter 2). When such conditions cause a significant mismatch between the task environment and the individual, an active error is likely to occur. The individual's capabilities and limitations (mental, physical, or emotional) may or may not match well with the environmental factors for the work as planned. In summary, job-site conditions shape worker behavior, for good or for bad. More detail is provided in the section on the Behavior Engineering Model.

Worker Behaviors

Worker behaviors include all the actions (or inactions) by an individual at the job site. Examples are component manipulations, use of human performance tools and other work practices, calculations, tool use, verbal exchanges, and procedure use. The effect of individual behavior is a change in the state of facility structures, systems, and/or components—plant results—for good or bad.

Plant Results

This element of the performance model represents the outcomes to the physical plant—good or bad. Examples of facility results include productivity, rejections, non-conformances, forced shutdowns, equipment reliability, safety-system availability, and outage effectiveness, as well as injuries, overexposures, spills, and damage. The quality of facility performance depends on the presence, integrity, and effectiveness of both processes and defenses.

MANAGING DEFENSES – Performance Improvement Model

It is a commonly held belief that people are always able to distinguish right from wrong and that people lack proper motivation when they act carelessly or without clear judgment.[17] This is a faulty assumption. Error-prone tasks and work environments are usually created by latent organizational weaknesses. These are undetected deficiencies in organizational processes or values or equipment flaws that create workplace conditions that provoke error (error precursors) or degrade the integrity of defenses (flawed defenses). Undetected organizational deficiencies plague human performance.

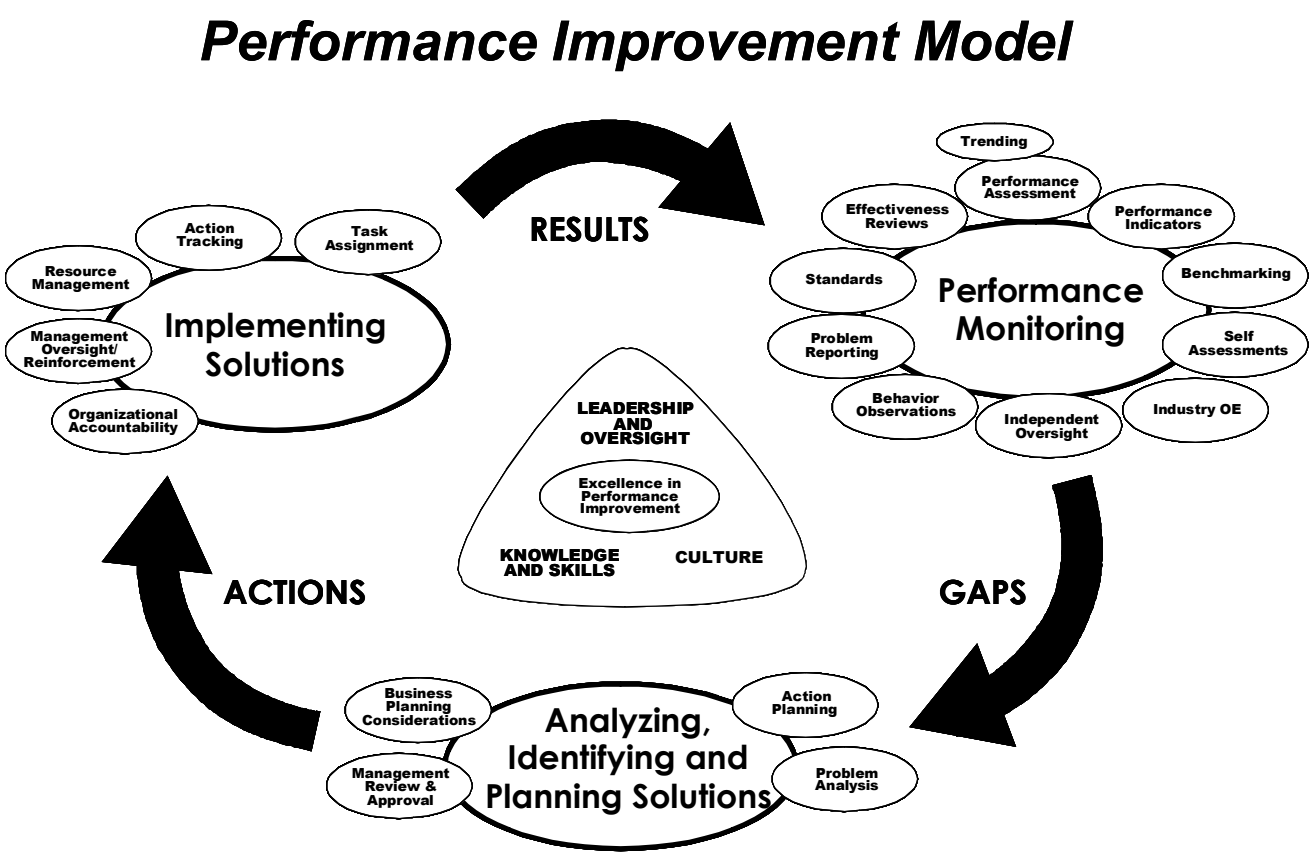
Latent errors or conditions are difficult to prevent. Once they are created they do not fade away but rather they accumulate in the system. Because of their hidden characteristic, it is management's primary challenge to *limit the time these vulnerabilities exist*. Managers should aggressively identify and correct vulnerabilities with defenses at the earliest opportunity. A more significant contribution to safety can be expected from efforts to decrease the duration of latent errors than from measures to decrease their basic frequency.[18]

"Managing" is the ongoing act of planning, directing, or controlling activities and resources toward accomplishing or achieving a purpose. Because significant events are few in number, less information is available about the presence of flawed controls and defenses. This means that performance information has to be gathered from other sources. Luckily, these sources are pre-existing and are known to managers, supervisors, and staff. Typically, reliance is placed on field observations, self-assessments, benchmarking, apparent cause evaluations, and trending to provide management with information needed to improve performance and to eliminate vulnerabilities to facility events. See Appendix A for a list of factors known to defeat defenses.

Performance improvement involves three primary activities.

- **Performance monitoring** – activities that assess current performance, identifying gaps between current and desired levels of performance or results
- **Analyzing, identifying, and planning solutions** – activities that determine actions needed to close the gaps.
- **Implementing solutions** – the collective activities that result in applying the chosen solutions and verifying their effectiveness to close the gaps

These three activities are depicted in the Performance Improvement Model below.



METHODS (Tools) FOR FINDING LATENT ORGANIZATIONAL CONDITIONS

- self-assessments
- trending
- operating experience
- behavior observations
- problem (causal) analysis
- surveys and questionnaires
- corrective action program
- performance indicators
- benchmarking
- independent oversight
- problem reporting
- management oversight, involvement, and reinforcement
- event investigation

Self-Assessments

The organization can identify gaps in performance by comparing the present performance for a given work activity to the expected performance (based on standards). The difference between actual and expected performance is referred to as the "performance gap." An analysis of this gap in performance yields information about conditions and circumstances needed to determine corrective action. Improvements can then be targeted to reduce the performance gap. This same process can be used to compare actual processes and methods to expected, desired processes and methods. The self-assessment outcome may show shortfalls in worker knowledge, skill, attitudes and experience or in actions or behaviors caused by human fallibilities. It is

more likely, however, to indicate deficiencies in job-site conditions related to task demands and the work environment or inadequate processes or weak organizational values that have influenced worker performance. The results of recurring self-assessments will yield patterns of weaknesses in defenses.

Behavior Observations

Field monitoring of individual performance is an excellent technique for gathering information about how well the organization supports job-site performance. The purpose of an observation is not to criticize or to judge people, but to review the quality and effectiveness of work preparation, policies, and work practices, as well as their implementation.

An important purpose of observations is to identify opportunities to improve the organization of work, not just worker practices. The scope of behavior observations should include the whole job, not just worker behavior. Not only is it important to pay attention to worker practices but also to monitor the job-site context, potential hazards, and the controls relevant to the work activity. Results should be recorded for trending purposes to help identify strengths and weaknesses. Behavior observations can flush out organizational weaknesses that may not be obvious by other means, especially when this data is included with other information.

The quality of behavior observations is important to gathering accurate performance data. Managers and supervisors must be willing to be critical during an observation. Effective observations are planned, involve watching specific activities and critical steps, require feedback, and are recorded. Observers should be able to model expected behaviors. Their knowledge of human performance tools and at-risk practices must be sharp and exact. Behavioral checklists, such as scorecards or coaching cards, can be used to remind managers and supervisors what to watch for. For specific tasks, knowledge of critical steps, potential errors specific to the task, and targeted worker weaknesses are included within the scope of the observation.[19]

Error rates decrease when managers and supervisors are in the field with workers. Error rates tend to decrease when they monitor work in the field.[20] The following in-field supervisory practices contribute to fewer errors by the workforce:

- checking that workers accurately perceive the risks and priorities associated with the task;
- observing work practices at critical steps;
- reinforcing people appropriately when they exhibit proper and effective work practices;
- correcting people on the spot for at-risk and unsafe practices and coaching performance that otherwise does not meet expectations; and
- solving production problems and removing performance obstacles for the work team or individual.

Problem Reporting

Finding and eliminating latent weaknesses improve dramatically when worker feedback and communication are encouraged. Workers are in the best position to provide the

feedback to help identify latent organizational weaknesses. Managers need to optimize related work processes that support work in the field to facilitate worker reporting issues. Workers are the beneficiaries of what the organization provides them, and they are keenly aware of its shortcomings.

Feedback via post-job reviews provides a credible and fresh source of information. The fundamental purpose of information gained from this review is to improve the organization of work as it supports worker performance at the job site—procedures, work packages, training, supervision, workarounds, and so forth. Such information will help improve productivity, identify opportunities to strengthen defenses against error and events, and eliminate error precursors embedded in the task. To promote the use of post-job reviews on a routine basis, they should be easy and quick to do, and the worker must see appropriate changes in response to his or her feedback.

Benchmarking

Benchmarking is a powerful management tool that should be considered in strategic organizational improvement planning. Best practices are strategies and techniques employed by top performers. Since top performers are not generally "best in class" in every area, it is important to know exactly the areas being targeted in the top performing organization. Those areas should be matched to areas in the home organization where improvement has been shown to be necessary. From detailed gap analyses, organizations can implement action plans that include benchmarking to address performance shortfalls. Comparison of facility practices with the practices of other like operations that are considered "best in class" is an ongoing effort. The implementation of changes resulting from benchmarking should include an overall strategy to disseminate the need, urgency, methodology, and responsibilities for changing a facility process to match that of a benchmarked organization. Adopting a new process should be carried out with specific objectives in mind that are tied to eliminating identified weaknesses in the pre-existing process.

Performance Indicators and Trending

Performance indicators allow for the identification of undesirable trends. They are tools to help managers focus actions on pressing issues in order to drive continuous improvement. Managers must measure what is important not just what is easy to measure. The following are representative of indicators used at DOE facilities:

- event rate (count of event-free days between events);
- error rate (number of errors from all problem reports submitted during a period of time);
- changes in employee survey parameters from survey to survey;
- industrial safety accident rate;
- document revision requests;
- indices (weighted calculation of several other indicators related to human performance; for example, events, industrial safety, security, radiological);
- procedure compliance;
- observations (scoring of work performance and coaching feedback);

- re-work (amount of maintenance-related work that results in delays or additional costs over a given period);
- out-of-service errors (error rates associated with lockout/tagout activities);
- repeat events;
- workarounds; and
- backlogs

The Pareto principle, or 80/20 rule, states that 80 percent of the consequences stem from 20 percent of the causes. This naturally occurring pattern helps identify the "big hitters," so that limited resources can be concentrated on resolving or improving the issues that comprise 80 percent (more or less) of all the problems. Once the big-hitter categories have been identified, analysts can plot each category over time, and they can then be addressed. Corrective actions can be implemented to address apparent causes of those issues. Analysts can plot data over time for these categories to see how each category trends over time.

Operating Experience

There is a natural tendency for people to think "It can't happen here" or "That won't happen to me." As was discussed in Chapter 2, humans underestimate risk and overestimate their ability to maintain control. This sense of invulnerability is an unsafe attitude. The use of operating experience (using feedback acquired from previously operating equipment or a system, both internal and external to the facility) has proven effective in improving performance and keeping facilities safer. Operating experience helps ground individuals to the risks and vulnerabilities associated with specific activities. This must be a relentless pursuit of leadership. Operating experience is most effective when the right information is communicated to the right people in time to make a difference. Lessons learned can be reinforced during various training forums and through day-to-day activities such as pre-job briefings, coaching and reinforcement by supervisors, and through engineering design reviews.

Managers must make effective use of operating experience tools (Operating Experience Summaries and the DOE Lessons Learned Program[21]). Managers routinely provide relevant operating experience information to workers at the time they have a need for it. The pre-job briefing is an excellent venue in which to share the operating experience. The challenge is to get workers to internalize the lessons learned and to apply them where appropriate to their upcoming job. Supervisors should ask individuals with key responsibilities in the work activity to explain how they will avoid specific errors committed in the events described. Supervision then considers appropriate defenses to avoid or mitigate errors and the consequences suffered in the described event. Supervisors should elicit work history experiences from individuals experienced with the task and assigned to the present job. They will usually have pertinent information, notably about latent weaknesses that hampered previous job performance and what will prove very useful to the other assigned workers.

Independent Oversight

It is common for people to forget to be afraid of the risks and threats and to become complacent about latent weaknesses or flawed defenses, especially when they are anxiously engaged day in and day out with their project or activities. Is this condition symptomatic of a lack of "situation awareness"—the accuracy of a person's current knowledge and understanding of working conditions compared to actual conditions at a given time? Or, is it the absence of "mindfulness," the presence of a certain "mindset," or the existence of some unexplainable "blind spots"? How is it that an individual from another operation visiting in the facility can readily spot a process weakness, an unsafe practice, an error-likely situation, or a weakness in a defense that has gone unnoticed by resident workers and staff? It is because the outsider brings a fresh set of eyes, perceptions based on an ideal mental model of what should be and expectations that unencumbered by local culture, experience and constraints. It is exactly this disparity between insiders and independent observers in their ability to recognize degraded conditions that makes independent oversight such a powerful tool.

Reviews of facility activities by outside organizations provide an opportunity to reveal "blind spots" to facility management that otherwise would remain hidden or latent in the system. Quality Assurance departments, corporate oversight groups, DOE oversight and assistance groups, and independent assessment groups, such as the Defense Nuclear Facility Safety Board (DNFSB) oversight, provide opportunities to identify latent conditions. With an emphasis on nuclear safety, DOE evaluations and DNFSB reviews identify conditions, processes, and practices that fall short of expectations for safety and industry best practices that can possibly lead to degraded system performance if uncorrected.

Problem Analysis

Problem analysis—using tools or combinations of tools such as root or apparent cause analysis, and common cause analysis—uncovers the underlying causes of problems or adverse trends, commensurate with their significance. It is not the intent of this handbook to describe these analysis tools in detail.

Analysts conducting root cause analysis of significant plant events should focus on what could have prevented the event rather than simply concentrating on who caused an event. It is also important to determine what defenses worked to keep the event from being more severe. When causal analysis is fixated on individual culpability, finding effective corrective actions will be elusive at best, as it is unlikely the analyst will identify the real causes of the event.[22] An effective investigation focuses on discovering the latent weaknesses embedded in the organization, its culture, and the physical plant, rather than simply singling out one or two individuals for counseling or training.

"Inattention to detail" and "not following procedures" are not root causes even though these are still commonly cited as such in the DOE complex. A root cause is the cause that, if corrected, will prevent recurrence of the event. Human error cannot be eliminated completely—inattention will continue to occur despite our best efforts to eliminate it.

Investigations of events triggered by active error are usually distorted by hindsight—the analyst's knowledge of facts after the event that were not known, or knowable, by the

principal individuals before the event. Hindsight predisposes the analyst to search for data that confirms the apparent shortcomings of the individual(s). Also, explaining what people could have or should have done explains nothing about why they did what they did. The challenge for the analyst is to determine why actions of the individuals made sense to them at the time. An analyst can build that context by identifying the following for each individual: [23]

- what they were trying to accomplish (goals);
- what they were paying attention to (focus); and
- what each person knew at critical points in the sequence of events (knowledge and situation awareness).

This information is obtainable from the individuals involved, through interviews and by a review of the job-site conditions for each individual (procedures, recorder traces, logs, computer printouts, review of the workplace, equipment, and so forth). The answers to the bulleted questions become the starting point for further investigation into the causes of the event.

The *Anatomy of an Event* model, introduced in Chapter 1, offers another structured approach to analyzing human performance issues. Working backward through the model from the event consequences to the organizational weaknesses that stimulated the event, helps explain the context of performance. Four major areas of fact need to be uncovered: (1) the specific consequences; (2) initiating actions (active errors) and error precursors that provoked the active errors; (3) flawed defenses that either failed to prevent the active errors or failed to prevent or mitigate the event consequences; and (4) the organizational weaknesses that contributed to every factor previously mentioned.[24] In the end, the analysis should clearly show the causal links (line of sight) from the organizational weaknesses to the event consequences.

Management Oversight

Fundamentally, management must have assurance that the risk of human error is minimized and controlled, especially during risk-important activities. A system of accountability helps verify that challenges to human performance are aggressively identified and addressed. Management verifies that expectations are performed to standards, that performance gaps are identified and closed, that corrective actions are completed effectively, and so on. See *Human Performance Steering Committee* earlier in this chapter to review one way the senior management team can perform its oversight responsibilities.

Surveys and Questionnaires

Monitoring changes in employee attitudes via periodic surveys identifies trends in values and beliefs. Workforce responses to surveys and standard questionnaires enable comparison of attitudes, values, and beliefs across an organization and detection of changes over time.[25] Survey results help managers determine where their time and effort can be applied most effectively to address misunderstandings and inappropriate values that impact the organizational culture. Questionnaire and survey questions must be carefully designed, tested and tied to specific organizational realities to be effective. Be careful not to ask for input and then fail to do anything constructive with it. There is a tendency in management to ask for input from workers and then not

to act on it. When people are uninformed of the results and changes derived from the information gathered, they will become doubtful of management's sincerity in wanting improvement, and will be uncooperative with future surveys.

Corrective Action Program

DOE's Corrective Action Management Program (CAMP) is a comprehensive tool to help management identify, document, evaluate, and trend performance issues to facilitate the development and implementation of appropriate actions to correct problems.[26] CAMP provides management with a tool to systematically adjust defenses and performance.

Briefly, the four steps of the program include:

- identifying and reporting problem findings from operational events, internal or external assessments or investigations, observations during daily work performance and worker safety concerns;
- evaluating each problem finding and developing appropriate corrective actions and corrective action plans;
- closing and implementing corrective actions to resolve findings delineated in the corrective action plan; completion and implementation status is tracked and reported to ensure timely and adequate resolution of each finding; and
- completion of all corrective actions for the findings listed in the corrective action plan and an independent follow-up assessment to verify closure.

Change Management

Change management is a methodical process that enables managers to establish the direction of change, align people and resources, and implement the selected modifications throughout the organization. Regardless of the scope of the change, it should be managed. Typically, change management has been reserved for large-scale organizational change and is not considered for day-to-day activities. However, most daily management activity involves some degree of change, such as changes in crew composition, outage schedule, policies, procedures, and equipment. More specifically, schedule changes are a common contributor to facility events.

Experience has shown that change fails most often when it implemented without developing a plan that includes:[27]

- defining the problem;
- determining the current condition;
- determining the desired final condition—a vision of what is expected;
- sufficiently considering the new values, attitudes, and beliefs needed to accommodate the change;
- identifying who is responsible to ensure the change is successful;
- describing the process to achieve the desired change, including consulting with all the people affected by the change;
- establishing a schedule for implementation;

- providing positive reinforcement of new behaviors by supervision and management; and
- specifying the actions planned to verify that the change has been successful.

Effective change management reduces the potential of error by managers when they change things. Without a structured approach to planning and implementing change, the error potential of managers and the support staff is higher. Organizations that have been successful with change have used a systematic process driven by quality leadership as well as excellent management.[28]

APPENDIX A: Warning Flags—Factors that Defeat Defenses

The Institute for Nuclear Power Operations (INPO), with the help of several utility executives, conducted a study of utilities that experienced extended plant shutdowns. The results of the study identified several common weaknesses with organization and management. INPO concluded that these latent conditions are conducive to the degradation and accumulation of flawed defenses and human-performance-related events. If not responded to aggressively, these weaknesses could lead to permanent facility shutdown and possible closure. INPO refers to these common weaknesses as "warning flags." [29]

- **Overconfidence** – The "numbers" are good, and the staff is living off past successes. Consequently, the staff does not recognize low-level problems and remains unaware of hazards.
- **Isolationism** – There are few interactions with other utilities, INPO, and industry groups. Benchmarking is seldom done or is limited to "industrial tourism," without the implementation of good practices learned. As a result, the plant lags the industry in many areas of performance and may be unaware of it.
- **Defensive and Adversarial Relationships** – The mind-set toward the NRC or INPO is defensiveness or "do the minimum." Internal to the organization, employees are not involved and are not listened to, and raising problems is not valued. Adversarial relationships hinder open communication.
- **Informal Operations and Weak Engineering** – Operations standards, formality, and discipline are lacking. Other issues, initiatives, or special projects overshadow plant operational focus. Engineering is weak, usually through a loss of talent, or lacks alignment with operational priorities. Design basis is not a priority, and design margins erode over time.
- **Production Priorities** – Important equipment problems linger, and repairs are postponed while the plant stays on line. Nuclear safety is assumed and is not explicitly emphasized in staff interactions and site communications.
- **Inadequate Change Management** – Organizational changes, staff reductions, retirement programs, and relocations are initiated before their impacts are fully considered. Recruiting or training is not used to compensate for the changes. Processes and procedures do not support strong performance following management changes.
- **Plant Events** – Event significance is unrecognized or underplayed, and reactions to events and unsafe conditions are not aggressive. Organizational causes of events are not explored in depth.
- **Ineffective Leaders** – Managers are defensive, lack team skills, or are weak communicators. Managers lack integrated plant knowledge or operational experience. Senior managers are not involved in operations and do not exercise accountability or do not follow up.
- **Lack of Self-Criticism** – Oversight organizations lack an unbiased outside view or deliver only good news. Self-assessment processes, such as management observation programs, do not find problems or do not address them; or the results are not acted on in time to make a difference

REFERENCES

[1] Hollnagel. Accidents and Barriers, Linkoping, Sweden. p.1; eriho@ikp.liu.se.

[2] Reason. *Managing the risks of Organizational Accidents,* 1998, pp. 76-77; http://en.wikipedia.org/wiki/chernobyl_accident.

[3] Maurino, Reason, Johnston, Lee. *Beyond Aviation Human Factors*, 1995, p.10.

[4] INPO. *Significant Event Evaluation and Information Network (SEE-IN) Program Description* (INPO 94-001), 1994, p.7.

[5] Maurino, Reason, Johnston, Lee. *Beyond Aviation Human Factors*, 1995, pp.11-13.

[6] Schein. *Organizational Culture and Leadership,* 3rd edition, 2004, p. 246.

[7] International Society for Performance Improvement. *Handbook of Human Performance Technology: Improving Individual and Organizational Performance Worldwide*, 1999, p.338.

[8] Porras. *Stream Analysis, A Powerful Way to Diagnose and Manage Organizational Change*, 1987, p.57.

[9] Porras. *Stream Analysis, A Powerful Way to Diagnose and Manage Organizational Change*, 1987, p.57.

[10] Maurino, Reason, Johnston, and Lee. *Beyond Aviation Human Factors*, 1995, p.xi.

[11] Reason. *Managing the Risks of Organizational Accidents*, 1998, pp.127-129.

[12] Schein. *Organizational Psychology*, 1994, pp. 12-15.

[13] Drucker. *Management: Tasks, Responsibilities, Practices*, 1974, p.218.

[14] Apostolakis. "A Structured Approach to the Assessment of The Quality Culture in Nuclear Installations." A paper presented at the American Nuclear society International Topical Meeting on Safety Culture in Nuclear Installations, Vienna, Austria, April, 1995, p.2.

[15] Porras. *Stream Analysis, A Powerful Way to Diagnose and Manage Organizational Change,* 1987, pp.35-40.

[16] United Kingdom Health and Safety Executive. *Reducing Error and Influencing Behaviour*, 1999, p.44.

[17] Wickens. *Engineering Psychology and Human Performance*, 1992.

[18] Reason. *Human Error*, 1990, pp. 179-80.

[19] Geller. *The Psychology of Safety*, 1998, pp. 194-212.

[20] After Entergy implemented its management observation program, which emphasized coaching time, it experienced a significant reduction in problem reports related to human error. 2000, as cited in INPO. *Human Performance Reference Manual,* 2006, endnote 21, p. 108. Entergy is a New Orleans based utility that provides electrical power to nearly three million customers in Arkansas, Louisiana, Mississippi and Texas.

[21] The DOE Corporate Operating Experience Program is at www.hss.energy.gov/csa/analysis/oesummary/index.html. The DOE Corporate Lessons Learned Program is at www.hss.energy.gov.csa.analysis/11/.

[22] Maurino, Reason, Johnston, Lee. *Beyond Aviation Human Factors*, 1995, p. 34.

[23] Dekker. *The Field Guide to Human Error Investigations*, 2002, pp. 77-99.

[24] Maurino, Reason, Johnston, Lee. *Beyond Aviation Human Factors*, 1995, p.66.

[25] Rothwell, Sullivan, & McLean. *Practicing Organization Development,* 1995, pp. 149-152.

[26] The Corrective Action Management Program meets requirements of DOE Order 414.1C. *Quality Assurance* (6/05). Corrective Action Program Guidance is provided in DOE G-414.1-5. The Corrective Action Tracking System (CATS) is on the web at www.hss.energy.gov.CSA/CSP/CAMP.

[27] Interaction Associates. *Facilitative Leadership* (course notebook), 1990.

[28] Kotter. *Leading Change*, 1996, p. 20.

[29] INPO. *Human Performance Reference Manual,* 2006, pp. 95-96.