2 A strategic approach

> Primum non nocere
>
> Thomas Sydenham (1624–1689)[1]

> Human rather than technical failures now represent the greatest threat to complex and potentially hazardous systems.
>
> James Reason[2]

Human error is likely the greatest source of variation in any human endeavor—an ever-present source of uncertainty that persists throughout your organization.[3] Dr. Reason said that "Wherever there are human beings, there will be human error."[4] When and where people will err cannot be known with absolute certainty—it's not an exact science. This introduces a substantial risk to any organization's operation. The International Organization for Standardization (ISO) describes risk as the "effect of uncertainty on objectives."[5] Therefore, you could conclude that managing the risk associated with the uncertainty of human error is strategic to your organization's long-term safety and prosperity. The word "strategy" (noun) is a plan, method, or series of maneuvers to attain a specific goal or outcome. On the other hand, the word "strategic" (adjective) describes something as essential to success in achieving a specific goal or outcome. I submit that managing the systemic risk of human error in complex, high-hazard operations is essential to preserving not only your people's health and well-being but also the long-term prosperity of your organization, its constituencies, communities, and surroundings.

Events/incidents/accidents happen when assets suffer harm—damage, injury, or loss, usually because assets were not adequately defended. Operational risks arise when people do things—work, using intrinsic hazards to produce products and services. Occasionally, people lose control of hazards through human error. Though human errors happen often, most are trivial, but some can be grievous. It's not important to "prevent" all human error (which is impossible anyway), just the ones that trigger serious negative events.

Events occur when assets suffer harm due to a loss of control of:

- transfers of energy
- movements of mass
- transmissions of information.

Today's high-hazard operations and their related management systems tend to be complex, possessing numerous interdependencies—cause-and-effect relationships—that can easily exceed any one person's capacity to comprehend them all. *Nothing is always as it seems*—there's always something hidden, unknown, incomplete, or otherwise obscure that could lead to trouble, even when in compliance with regulations and "approved" procedures. Consequently, those in direct contact with operational hazards and assets must be able to recognize and adapt (behavior choices) to changing risk conditions to protect assets—a key trait of resilience. The capacity to adapt is necessarily inefficient, but the safety improvements through resilience more than offset the costs in the long run.[6] Please do not misinterpret what I'm suggesting regarding the use of procedures. Technically accurate and usable procedures provide front-line workers the best tool for performing complex operations in high-hazard industries—the stakes are too high to leave the means of producing a work output to individual choice.[7]

Therefore, managers must understand how behavior choices of front-line workers on the shop floor emerge from the designs, functions, values, and norms of their management systems. Understanding and managing the flows and avenues of influence of the organization—the system—on the behavior choices of front-line workers is essential to properly aligning them to minimize the risk of harm and to achieve the business results you want.

> "…if you do not manage human error, human error will manage the organization, always at great cost and often at great danger."
>
> —James Reason
> Video Series, *Managing Human Error*

Human error cannot be left to chance during complex industrial operations. Therefore, I propose an approach that is (1) risk-based, (2) systemic, and (3) adaptive to managing workplace **Hu** during high-hazard operations—to recognize and control the specific **Hu** risks intrinsic in your operations and to verify assets are sufficiently defended should people still lose control. Since H&OP is about managing risk, let's focus on where the risk manifests itself—in the workplace.

Work and the workplace

What is work? From a physics perspective, work is simply the application of a force over a distance—something changes. Work is good when value is created. We enjoy our work when we realize purpose in it, and when we work hard and perform well, we feel the joy of accomplishment and gain a sense of personal

worth from it. When exchanged for a wage or salary, work allows an individual to provide for his/her own and help others in need—all good for society. But, occasionally, our work extracts value resulting in damage, loss, or injury.

In the marketplace, industrial operations involve the production of goods and services that are suitable for use or have economic value to a customer base—at a cost that is less than what they would pay to produce it themselves. A variety of processes and methods are used to transform tangible resources (raw materials, semi-finished goods, subassemblies) along with intangible ones (data, information, knowledge, expertise) from their natural, unprocessed state to a finished product state—creating value.[8] Operations associated with production processes require multiple and varied human actions—making, constructing, assembling, manufacturing, inspecting, communicating, operating, or handling material, parts, tools, machinery, and products. Other human activities—not directly involved in the transformation processes—include planning, scheduling, designing, testing, routing, shipping, dispatching, storage, etc. In the marketplace, *work is energy directed by human beings to create value*.

Since physical work involves the use of force during operations, front-line workers require the use of intrinsic (built-in) hazards, most of the time, in various forms of energy. Work—in the battery—occurs when either:

- *energy* is applied to raw materials or intermediate components to create a finished product or provide a service;
- *mass* is transported (whether solid, liquid, or gas) from one place to another;
- *information* is created, processed, stored, transmitted, or communicated to a receiver or recipient.

Notice that these situations are intrinsically associated with normal, everyday work. Transfers, movements, and transmissions occur via various means or pathways initiated by human operators. With today's complex technologies, these pathways tend to be physical in nature—such as the movement of oil through a pipe, heat through an exchanger, flow of electricity through a wire, or delivery of data over electronic and radio networks.

When work occurs—force applied over a distance—something has to change. If work is not performed under control, the change is not what you want; work can inflict harm. Though most hazards are identified before starting work, some appear without warning, which have to be managed in real time. Job hazard analysis, procedures, policies, expectations, training, automation, and facility and equipment designs are ways you use to reduce and control uncertainty and variation in **Hu**. Uncertainty and variation, however, can never be totally eliminated.

If you listed all the hazards you could encounter during your commute to work each day, you would note a few you know are always present (e.g., speed and proximity of other vehicles), but you would also realize that many cannot be anticipated—they are surprises. In the real world, over time, people and things change, knowledge and skills decay, tools and equipment wear out, and assumptions about the environment and local work conditions become

increasingly invalid. All along the way, people touch things and with each touch there is the potential to cause harm.

Bottom line: *Work involves the use of force under uncertainty.*

The Hu risk

Generally, safety is the freedom from an unacceptable risk of harm. But, harm to what? Every organization possesses multiple assets, but some are more important than others—people, property, and product as a minimum. Assets and their limitations define the boundaries of harm and what constitutes an event, when those limitations are exceeded. Strategically, it is important to protect your most important assets from harm. Events and accidents are always defined in terms of harm to one or more assets, without which there is no event, except in the case of a serious near-miss (near-hit).

It's crucial for managers of operations to realize an important facet of H&OP relative to the causes of an event. It's not the error that triggers an event that you should be most concerned about. It's the harm to assets that results from error—a loss of control. Harm involves a detrimental change in the state of assets or a serious degradation or termination of the organization's ability to accomplish its mission. Just as human error is unintentional and usually a surprise to the individual, the events that ensue are likewise surprises from an organizational perspective. Managers should not be as concerned with the occurrence of human error as with protecting assets from harm that ensues after the error. Protecting assets from harm motivates the desire to control workplace **Hu**. Ultimately, you want to avoid both (1) losing control and (2) suffering the harm, but each is managed differently.

Let's arrange these elements together in a conceptual model—a way of thinking about risk—that will help you manage the uncertainty of human error in the workplace, to avoid events. Whenever work is performed, as illustrated conceptually in Figure 2.1, three things are present:

- **assets—**things important, of high value, to an organization;
- **hazards**—intrinsic sources of energy, mass, or information used to create value;
- **human beings**—work by fallible people during value-creation processes.

The relationships between **assets**, **hazards**, and **humans** form what I call the "**Hu Risk Concept**." For the remainder of this book, each word used in the **Hu Risk Concept**, including the **Hu Risk Management Model** discussed in a few more pages, is denoted with a bold font as an ongoing reminder of each element's principal role in managing the risk of human error in operations. The **Hu Risk Concept** enhances the recognition of what to manage. The presence of uncertainty due to **human** interactions with **assets** and **hazards** produces risk—risk of harm—an **event**. Because of the potential impact on the organization and the systemic uncertainty that human error poses to your operations, a strategic risk exists. Therefore, managing human error in

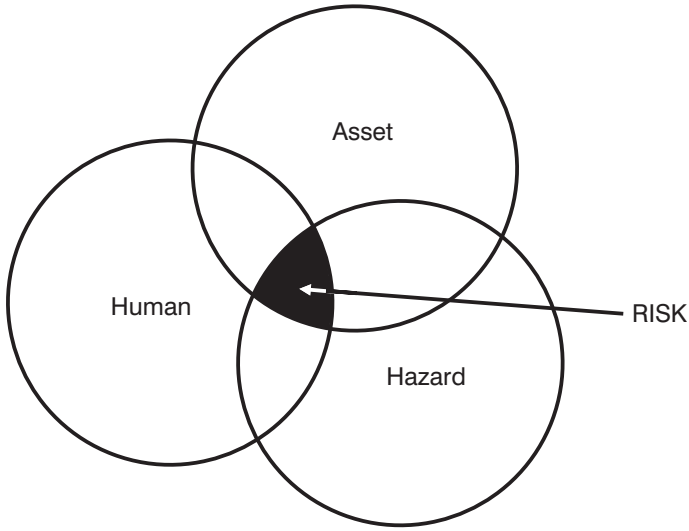

Figure 2.1 The **Hu Risk Concept** illustrates the primary elements demanding attention in managing the risk that human fallibility poses to operations. The interfaces (overlaps) of these elements introduce risk: losing control of an intrinsic **hazard** and harming an **asset**—an **event**

operations becomes as important as managing production—both must be managed together, not separately. Let's look at each element in more detail.

Assets—*what to protect from harm*

Assets include people, product, property, facilities, reputation, equipment—anything of value and important to the organization's reason for being—its mission. Whatever is essential or key to its (1) safety, (2) profitability, (3) reliability, (4) environment, (5) community, and (6) even reputation is of utmost importance to the members of a responsible and honorable organization.

For a business or organization to be sustainable, the **assets** used to create or deliver the company's outputs must be protected. For a commercial airline, the primary **assets** are passengers and its aircraft. Secondary **assets** include schedule reliability and quality of service. For a hospital, **assets** include patients, staff, medications, and its facilities. For a biotech company, it is the drug substance. For a nuclear power plant, it is the reactor core. **Assets** essential to an organization's survival are the rightful focus of H&OP. What happens to **assets** drives the organization.[9]

"If you value it, you will protect it unless you're willing to replace it."
—Dorian Conger
Incident Investigation Expert

In the U.S. Navy Submarine Service, submarines and their various subsystems, including their nuclear reactors, are carefully operated within specific constraints to optimize their safety and reliability, such as depth and speed. Collectively, operators refer to these constraints as the Safe Operating Envelop (SOE). The SOE for any **asset** is the multi-dimensional space of parameters and other conditions under which the **asset** is considered safe. For example, the SOE of a car tire includes wall condition, tread depth, air pressure, temperature, speed, among others. When one or more critical parameters associated with the SOE of an **asset** are exceeded, the likelihood and/or severity of the harm from existing **hazards** increases.[10] Critical parameters are the vital signs of the health or illness of equipment and processes. A fragile **asset** is one that can be easily harmed by handling, jostling, stress, contact, collision, abruptness, neglect, etc. Using more robust **assets** reduces the potential for harm, but may be more expensive. **Assets** are generally protected from harm during operations by ensuring certain critical parameters remain within the confines of their SOE (design bases) using procedures and built-in defenses.

Anything that can harm or damage key **assets** must be taken seriously by the organization's managers at every level—as part of its everyday core business processes. Examples of undesirable business outcomes include various forms of the following:

- products or services that harm customers;
- people killed, disabled, injured, or infected with a disease;
- product or property lost, defective, damaged, or destroyed
- environment contaminated, spoiled, or ruined;
- reputation defamed or tarnished;
- information lost, corrupted, or stolen (intellectual property or trade secrets);
- value lost due to excess waste or scrap and late deliveries.

Obviously, a company that continues to experience any of these problems—**events**—for extended periods will not stay in business very long.

Hazards—*built-in sources of harm*

Various types of **hazards** are intrinsic to industrial operations—built-in sources of energy, mass, and information that are associated with a particular domain of operations. They are necessary to accomplish the organization's work. Intrinsic physical **hazards** used in industrial operations make harm a real possibility. Generally, **hazards** are intrinsic either to the material or to its conditions of use. For example, in the maritime industry, intrinsic **hazards** can include water, deep water, rocks and shoals, corrosion, currents, tides, and the presence of other vessels. Deep-draft merchant vessels cannot operate safely in shallow water near shoals. In aviation, they include gravity, elevation, weather, terrain, and other aircraft. The following list of energy forms (with examples in parentheses) shows some of the more common intrinsic **hazards** used in operations:[11]

- electricity (power sources (potential), electrostatic charges);
- kinetic (rotating machinery, flywheels, moving equipment, flow, velocity);
- chemical (acids, corrosion, fire, dust, lead);
- gravity (elevated work, bulk storage at heights, hoisting and rigging);
- thermal energy (steam, fire, hot surfaces, bright lights);
- compressed fluids (high pressure gases, hydraulics, vertical columns);
- toxic or inert gases (phosgene, carbon monoxide, confined space);
- explosives (hydrogen, natural gas, gasoline fumes);
- acoustic (noise and vibration);
- radiation (x-rays, ionizing, lasers);
- biological (viruses, bacteria, fungi, animals, insects);
- information (defective software updates, out-of-date prints, unsecured networks, missing or inaccurate procedures, corrupt data, lax security protocols);
- people (fallible decisions, imprecise actions and movements).

Safety and control of hazards depends on the recognition of hazardous conditions, so as to prevent unexpected energization, startup of equipment and machinery, or the release of stored energy that could injure workers. This means people should possess an in-depth technical knowledge of the technology they work with, and be able to recognize various hazardous energy sources, their types, and magnitudes present.

"If it has the capacity to do work, it has the capacity to do harm."

—Dorian Conger
Incident Investigation Expert

We tend to assume **hazards** are stable—that they are always present and knowable in advance. Most are, some aren't. Occasionally, unanticipated **hazards** encountered during work appear gradually or unexpectedly, not unlike the normal rise and fall of sea levels or from storm surges spawned by earthquakes and distant storms. To sustain the safety of your **assets** over the long term, front-line workers have to be capable of managing the surprise **hazards** when they occur—able to adapt.

Events—*harm to* assets

Events have many names, such as incident, accident, deviation, nonconformance, etc. In other contexts, the term "**event**" can refer to everyday occurrences such as a birthday party, a wedding, a concert, or a baseball game. Here, I refer to the negative meaning of the word **event**—an undesirable occurrence involving harm (injury, damage, or loss) to one or more **assets** due to uncontrolled (1) transfers of energy, (2) movements of mass, or (3) transmissions of information, as noted earlier. **Events** are not entirely unpredictable—unpredictability resides in their timing and location, not so much their causes.[12] I believe that causes of **events** that have not happened can be found and eliminated.

> "Day after day, year after year, nothing much goes wrong, lulling managers and workers into a sense of security and a belief that what they do day after day is safe. Events are always surprises."
>
> —Derek Viner
> Author: *Occupational Risk Control* (2015)

The anchor point in any **event** occurs at a point in time when control is lost over the damaging properties of energy, mass, and information—when the destructive potential of intrinsic **hazards** is unleashed uncontrollably because of a loss of control or the absence of adequate protection.[13] In every **event**, defenses had to fail in some way or were circumvented. See Figure 2.2. An **event's** severity is not so much a result of the worker's error, it is more a function of the amount of energy absorbed by an **asset**. An **event's** severity is measured in terms of the degree of injury, loss, or damage to one or more **assets**—a function of the magnitude, intensity, or duration of the **hazard's** damaging release. For example, an automobile accident triggered by the same driver's error in either case is more severe at high speeds than at low speeds. It should be apparent that the robustness of defenses—barriers and safeguards—determines how bad, or how benign, outcomes are after an error.

The harm that ensues after a loss of control, is more the result of ineffective defenses, where the barriers or safeguards were either missing, ineffective, or by-passed. As illustrated in Figure 2.1, the **Hu Risk Concept**, sustaining safety in operations is essentially a control problem—control of (1) human variability during high-risk activities, and (2) the intrinsic hazardous processes used during work.[14]

Human fallibility—potential for losing control

The occurrence of an **event**—the onset of injury to, damage to, or loss of one or more **assets**—strongly indicates that control over the damaging properties of

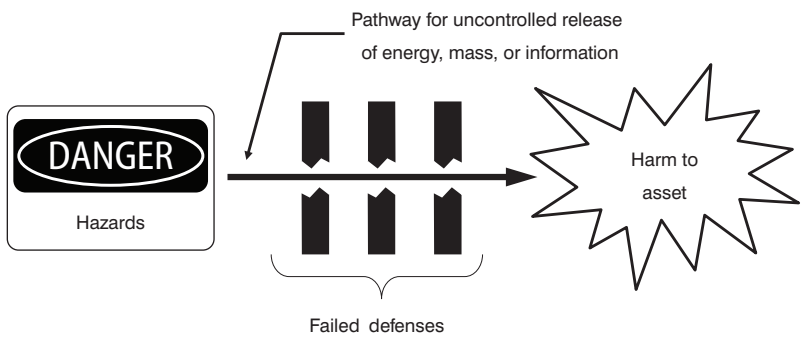

Figure 2.2 An **event** occurs due to an "uncontrolled" transfer of energy, movement of mass, or transmission of information—failures in defenses—that allows harm to occur to an **asset**. (Adapted from Figure 1.1 in Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate.)

intrinsically hazardous processes was lost—usually triggered by some human failing at the controls.[15] Variations in behavior, due to human error, lead to variations in results. The notion of human error is explored more deeply in Chapter 3.

Yes, people are **hazards**, but they are also heroes. Creativity and fallibility are two sides of the performance coin. Through creativity, people possess the ability to adapt to unexpected risky situations. Because of this innate human characteristic, people are able to create safety for **assets** in situations not previously anticipated by either managers or designers. Creativity springs from technical expertise. Expertise and the ability to adapt are important features of RISK-BASED THINKING, which will be addressed more fully in Chapter 4.

In the healthcare industry, the overarching, guiding principle is to "first, do no harm." That's exactly the mindset that managers and leaders need in high-hazard operations. In the following paragraphs, I describe a management model—derived from the **Hu Risk Concept** that helps you and your organization "do no harm." A model-based approach to managing risk provides managers with the means to be proactive in avoiding harm, by helping them understand how their systems influence performance and its defenses. An event-based approach—learning late by reactive reporting and **event** analysis—will only get you so far.

Hu risk management model

The battery of **Hu**—the confluence of **assets**, **hazards**, and **Hu** illustrated conceptually in Figure 2.1 occurs during work. Using the **Hu Risk Concept** as a springboard, a more practical form, depicted in Figure 2.3, suggests more specifically what to manage—**pathways** and **touchpoints**. It is a simple, highly transferable model that helps pinpoint the work-specific interfaces (or combinations) to pay attention to in order to avoid an **event**.

Pathways and touchpoints

Risk is managed at the interfaces between the three elements of our **Hu Risk Concept** (overlapping circles in Figure 2.1). The interfaces (interactions) are illustrated by the plus signs (+). The first + sign represents the establishment of

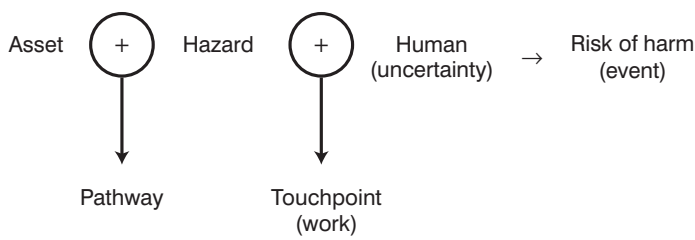

Figure 2.3 The **Hu Risk Management Model** pinpoints the two work-related interfaces—**pathways** and **touchpoints** (denoted by the plus (+) signs), that must be controlled to minimize the risk of harm during operations

a **pathway** for either the transfer of energy, movement of mass, or transmission of information between an operational **hazard** and an **asset**, where only one human action (or equipment failure) is needed to either create value (under control) or cause harm (out of control). A **pathway** for harm exists when a **hazard** is poised in such a way as to expose an **asset** to the potential for a change in state—a vulnerability for good or for bad. Remember, the original intent of these interfaces is to add value through work. However, whenever there is an opportunity to add value, there is an associated risk to do harm—to extract value. Derek Viner, in his book, *Occupational Risk Control*, refers to such exposures as "vulnerability **pathways**."[16] For example, a firearm that has a bullet loaded in the chamber, with the safety off and the hammer cocked is poised to discharge. A person would be exposed to death or severe injury if standing in the *line of fire* in front of the muzzle of a firearm in such a condition, especially if the firearm is wielded by another person with a finger on the trigger (a **touchpoint**). Other examples of potential **pathways** include the following situations:

- a toddler standing near the edge of the deep end of a swimming pool;
- the presence of fuel, oxygen, and a nearby ignition source, such as a match;
- an electrical potential (voltage) controlled by a single switch or circuit breaker;
- a person standing on the curb of a busy street;
- a vehicle parked on a steep hill secured only by the automatic transmission in Park (P) and with the front wheels aimed straight ahead;
- accessibility to proprietary information controlled by a simple password by the wrong persons;
- a digital control system (DCS) aligned to start a series of automated process sequences by an operator with a finger on mouse prepared to click "Go" or to depress the Enter key;
- a phishing e-mail message open on the screen of your personal computer with the cursor hovering over a link to a malicious website.

Recall the photo of the ironworkers in Figure 0.1. It vividly illustrates the elements of the **Hu Risk Management Model**. This photograph highlights the three distinct elements of risk: **asset**, **hazard**, and **human**. Obviously, the **assets** are the people, the ironworkers. What makes the photograph stunning is the obvious **hazard**—the beam the workers are sitting on is more than 800 feet about the streets below. The apparent absence of barriers (nets or body harnesses) to prevent them from falling makes it doubly fearsome, which is accentuated by the fact that people are fallible, including the photographer. **Pathways** are particularly important because the potential for harm is now dependent upon either a single human action or equipment malfunction (failure). Front-line workers must be wary of the creation and existence of **pathways**.

The second + sign represents a **touchpoint**. A **touchpoint** involves a human interaction with an object (whether an **asset** or a **hazard**) that changes the state of that object through work. **Touchpoints** involve a force applied to an object over a distance, using tools or controls of hazardous processes. After

performing a **touchpoint**, "things are different," and usually things can't be put back the way they were. The control of a **touchpoint** is most important when a **pathway** for energy, mass, or information exists between an **asset** and a **hazard**. A **touchpoint** includes all the following characteristics:

- *human action*—bodily movements, exerting a force;
- *interaction with an object*—physical handling—force applied to an object;
- *work*—force applied over distance;
- *change in state*—changes in parameters that define the state of the object.

Human beings possess the capacity to direct energy, to move things with their hands, feet, and body. Because of our innate human fallibility, **touchpoints** bring about uncertainty related to the actions performed—whether under control or out of control, and their outputs, whether for good or for bad. Quality Assurance people call this variation. In the photograph of the ironworkers in Figure 0.1, the **assets**, **hazard**, and **pathway** are clear. However, the all-important **touchpoint** may not be so apparent. They're sitting on them—their backsides. If the workers lean too far forward or backward, either way they could lose their balance and fall to their deaths.

Both the creation of **pathways** and the occurrence of **touchpoints** (work) are normal and necessary activities of everyday operations. The occurrence of **touchpoints** after creating a **pathway** tend to be critical to safety. If a **touchpoint** is performed in error, the performer loses control and harm—an **event**—is likely to occur. This suggests that defenses must be built into the facility design, production processes, procedures, and expectations to protect **assets** from errant operations, while **pathways** exist. Otherwise, harm is likely.

The risk of an **event** is managed through the prudent deployment of controls, barriers, and safeguards to (1) lessen the chance of human error at important **pathways** and **touchpoints**, and (2) protect **assets** from harm. This assumes no modifications or alternatives exist to the **assets** and **hazards** used during operations. As mentioned earlier in the Introduction, the scope of this book is limited to managing H&OP with what you have.

The building blocks of H&OP

Strategically, what should managers "control?" As stated earlier, H&OP is all about managing the risk human error poses to an organization's operations. In light of the **Hu Risk Management Model**, the building blocks of H&OP suggest specifically what managers should pay attention to and what to do. As illustrated in Figure 2.4, H&OP involves three core operational functions and three management support functions. The core operational functions that involve daily risk management include:

1 *Risk-Based Thinking*—adapting to real-time risks in the workplace.
2 *Critical Steps*—ensuring the right things go right at critical phases of work.
3 *Systems Learning*—detecting and correcting ineffective defenses and related system weaknesses.

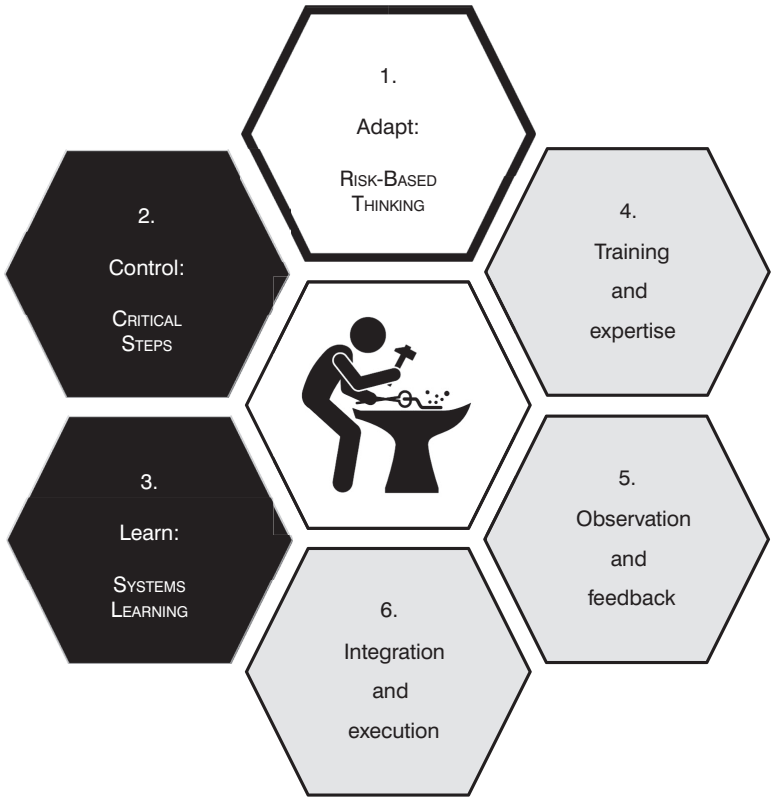

Figure 2.4 The Building Blocks of Managing H&OP. Adapt: Risk-Based Thinking; Control: Critical Steps; and Learn: Systems Learning serve as the core risk-management functions of H&OP (black hexagons). However, without direct line manager engagement, H&OP will not work: Training and expertise, Observation and feedback, and Integration and execution (gray hexagons)

Cells 4, 5, and 6 are important management practices that support the effectiveness of cells 1 through 3. These include:

4 *Training and expertise*—ensuring front-line personnel possess technical knowledge and skill to exercise Risk-Based Thinking and to recognize and control Critical Steps.
5 *Observation and feedback*—managers spending time on the shop floor, creating learning opportunities for both workers and themselves.
6 *Integration and execution*—enabling Risk-Based Thinking as a way of doing work, and promoting managerial accountability for the follow-through of all H&OP functions.

Collectively, the six functions form the building blocks of H&OP, which are described individually in more detail in the following paragraphs and chapters.

1 *Adapt*—Risk-Based Thinking. This function focuses on enhancing the organization's and its people's capacity to adjust—in real-time—to changing risks, whether expected or unexpected. On most occasions work is guided by procedures, policies, checklists, supervision, expertise, and work norms. But, in some unforeseen cases, front-line workers and their supervisors may run into surprising work situations. Therefore, front-line personnel will have to "think on their feet" to make adjustments to such surprises to keep **assets** within their SOEs, and, if they can, still accomplish their organization's purposes.

It's not "if" people adapt; it's "when" they adapt—they must adapt. And, most people are able to adapt because of the knowledge and expertise they have developed in their jobs over several years. Risk-Based Thinking is a form of resilience—something a system does to verify/ensure safety exists. Research in resilience engineering has identified the following cornerstone habits of thought that characterize successful organizations: (1) anticipate, (2) monitor, (3) respond, and (4) learn.[17] Collectively, I refer to these cornerstones or patterns of thought as Risk-Based Thinking. *Although you cannot anticipate every possible harmful scenario, you can be ready for almost anything through Risk-Based Thinking.* This is a bold assertion, but it's the strength of a resilient workforce. When Risk-Based Thinking is integrated into the DNA of an organization's way of doing business, people will be ready for most unexpected situations. All safety-oriented practices, including **Hu** tools, have their foundations in one or more cornerstone habits of thought.

Its cousin-in-thought, "chronic uneasiness," enhances people's respect for the technology they work with and their mindfulness of **pathways** between **assets** and **hazards** and impending transfers of energy, movements of mass, and transmissions of information. Top performers think before acting to prove to themselves that an **asset's** safety exists before doing work. Chapter 4 explores this building block in greater depth.

2 *Control*—Critical Steps. This function focuses people on ensuring the right things indeed go right the first time, every time. A Critical Step is a human action that will trigger immediate, irreversible, intolerable harm to an **asset**, if that action or a preceding action is done improperly. The more work, the more **touchpoints** in a given time means more errors occur for the same period—more shots on goal. It is likely more **events** will occur. The more errors, the more often **events** occur. As you can see, the tempo of work activities tends to drive the frequency of events; the number of people required, how often people do work, the amount of time involved, and the number of human actions.

Events are triggered at Critical Steps. Identifying and controlling **Hu** at Critical Steps, minimizes unwanted variation in **Hu**—avoiding a loss of control. Specifically, managers would do well to help workers and supervisors become keenly aware of Critical Steps and related error traps that aggravate the potential for error during those actions. Workers and supervisors know what to pay close attention to and what to do to

exercise positive control of these critical **touchpoints** that trigger transfers of energy, movements of mass, and transmissions of information during operations. Chapter 5 explores this building block in great detail.

3 *Learn*—Systems Learning. The safety of any system depends on the presence, integrity, and robustness of its defenses. Systems Learning involves the detection and correction of weaknesses in an organization's system that diminish the integrity, presence, or robustness of defenses, weakening the control of **Hu**, and/or inhibiting the protection of **assets**.

Error prevention has been the traditional focus of managers wanting to "improve **Hu**." However, I hope that you are realizing that the emphasis on error prevention is overblown. Only defenses (barriers and safeguards) built into systems, processes, structures, and components minimize the severity of **events**.[18] The severity of **events** is not a result of the trigger mechanism—human error. It's a result of the marshalling of energies, an **asset's** susceptibility to harm, and the integrity of defenses built into the system. Finding and correcting faulty defenses and eliminating hidden **hazards** in the workplace tend to minimize the severity of **events**. Not doing so leaves the system vulnerable and, therefore, unsafe—even though **events** may not be occurring.[19] Systems Learning is effective only when line managers are accountable for the ongoing discovery and elimination of system weaknesses that inhibit the effectiveness of defenses.[20] A deep dive on Systems Learning happens in Chapters 6 and 7.

4 *Training and expertise*. Training, experience, and proficiency builds expertise—intimate understanding and skill associated with a technology, combined with a *deep-rooted respect* for the dangers of that technology. Training also informs people of their capabilities and limitations as human beings as well as a means to moderate their fallibility. Risk-Based Thinking and chronic uneasiness are integrated into technical training programs. Expertise is the bedrock of Risk-Based Thinking. Knowledge and skill is perishable—it has a half-life. Therefore, training must be ongoing—not a one-and-done activity. Training is discussed in Chapter 8.

5 *Observation and feedback*. Because of its importance and usefulness to line managers as a Systems Learning tool, observation and feedback is called out separately. Observation provides opportunities for two-way feedback via face-to-face interactions between line managers and front-line personnel. Through observation and feedback, managers see firsthand what is happening in real time and what front-line workers have to work with—what they inherit from the system, including unworkable and ineffective procedures, tools, and expectations. Managers see with their own eyes what workers do to accomplish work, whether according to expectations or otherwise. Workers and supervisors receive feedback about their performance in the workplace, and managers receive feedback about their systems. Chapters 7 and 8 discuss the importance and conduct of observation and feedback.

6 *Integration and execution*. Eventually, Risk-Based Thinking, Critical Steps, and Systems Learning are incorporated into all facets of operations and the

organization. It becomes part of the daily core business—it is not optional. Safety and production go hand-in-hand—they're not separate activities. Safety occurs while you work. Integration enables Risk-Based Thinking in various organizational functions as well as operational tasks and work processes—it becomes a way of thinking and doing work. Execution is a systematic and disciplined management process of getting things done.[21] Managers can't simply hope front-line personnel will use **Hu** tools (see Appendix 3) to avoid errors—the risks must be properly managed. Implementing H&OP and Risk-Based Thinking requires management, leadership, commitment, and accountability. Chapter 9 is devoted to this building block.

The primary benefit of systemwide deployment of H&OP is sustained periods of success. A declining trend in the frequency and severity of **Hu events**, the reduction of costs and risks to the organization, and the ever-increasing adoption of safe practices, among others, are manifestations of H&OP. Applying Risk-Based Thinking and reducing the occurrence of errors at Critical Steps tends to drive down the frequency of **events**. The severity of the **events** that still occur are minimized by ensuring barriers and safeguards are in place and effective in protecting the organization's **assets**.

I believe that institutionalizing H&OP will not only save lives through improved safety and reliability, but it will also save livelihoods by improving the organization's productivity (production/unit time) in the near term, and profitability (production/unit cost) over the long run.

Things you can do tomorrow

1 Discuss with colleagues or your management team what is meant by "safety." Discuss how safety is managed. Ask your colleagues or management how they know safety exists if no **events** are occurring.
2 Do managers believe that **events** are unanticipated, sudden, surprising, unpredictable, and "caused" by "unsafe" worker behavior? Such beliefs foster resistance to the idea that **events** can be prevented.
3 During any production-focused meetings, observe whether safety is separate or part of the conversation. Do meetings start with a "safety moment," followed by the "real work?" Or, is protection of assets part and parcel with talk about the production objectives?
4 Using a frequent high-risk operation as an example, discuss with the management team how the risk of human error could be better managed using the **Hu Risk Management Model**.
5 Identify operations or work activities on the current schedule that are high-risk or potentially costly if control is lost. Consider means to avoid losing control. Identify contingencies, "STOP-work" criteria, and ways to protect assets if control is lost.

Notes

1 "First, do no harm." The medical maxim is commonly and mistakenly thought of as the Hippocratic Oath. This specific maxim and its Latin phrase was attributed to the English physician Thomas Sydenham (1624–1689) in a book by Thomas Inman. See Inman, T. (1860). Hays, I. (ed.) "Book review of *Foundation for a New Theory and Practice of Medicine.*" *American Journal of the Medical Sciences*, Philadelphia, PA: Blanchard and Lea (pp.450–458).
2 Reason, J. (1995). Understanding Adverse Events: Human Factors. *Quality in Health Care,* 4.2:80-89. DOI: 10.1136/qshc.4.2.80.
3 Flin, R., O'Connor, P. and Crichton, M. (2008). *Safety at the Sharp End: A Guide to Non-Technical Skills*. Farnham: Ashgate (p.1).
4 A quote associated with Dr. James Reason in his video series, "Managing Human Error."
5 International Organization for Standardization (2009). ISO 31000. "Risk Management."
6 Van Dyck, C., Frese, M., Baer, M. and Sonnentag, S. (2005). Organizational Error Management Culture and Its Impact on Performance: A Two-Study Replication. *Journal of Applied Psychology*. Vol. 90. No. 6. (pp.1228–1240). DOI: 10.1037/0021-9010.90.6.
7 Marx, D. (2009). *Whack-a-Mole: The Price We Pay for Expecting Perfection*. Plano, TX: By Your Side Studios (p. 67).
8 Retrieved from http://www.businessdictionary.com/definition/production.html#ixzz3q3cbPuXq
9 Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate (p.3).
10 Corcoran, W.R. (August 2016). An Inescapable of the Safe Operating Envelope (SOE). *The Firebird Forum*. Vol. 19, No. 8.
11 Viner, D. (2015). *Occupational Risk Control: Predicting and Preventing the Unwanted*. Farnham: Gower (pp.70–72).
12 Ibid. (p.27).
13 Ibid. (p.46).
14 Leveson, N. (2011). *Engineering a Safer World*. Cambridge, MA: MIT (pp.67, 75).
15 Viner, D. (2015). *Occupational Risk Control: Predicting and Preventing the Unwanted*. Farnham: Gower (p.112).
16 Ibid. (p.43).
17 Hollnagel, E. and Woods, D. (2006). Epilogue: Resilience Engineering Precepts. In Hollnagel, E., Woods, D. and Leveson, N. (eds.). *Resilience Engineering: Concepts and Precepts*. Farnham: Ashgate (pp.349–350) and (2009) *Resilience Engineering Perspectives, Vol. 2*. Farnham: Ashgate (pp.117–133).
18 Idaho National Engineering and Environmental Laboratory (March 2002). "Review of Findings for Human Contribution to Risk in Operating Events," (NUREG/CR-6753). Washington, DC: U.S. Nuclear Regulatory Commission.
19 Retrieved from www.fra.dot.gov/downloads/safety/ANewApproachforManagingRRSafety.pdf
20 Reason, J. and Hobbs, A. (2003). *Managing Maintenance Error, A Practical Guide*. Farnham: Ashgate (pp.91, 96).
21 Bossidy, L. and Charan, R. (2002). *Execution: The Discipline of Getting Things Done*. New York: Crown (pp.21–30).