Strengthening Defenses to Prevent Harm

WHY SHOULD HOSPITAL LEADERS BE AS CONCERNED ABOUT THE STRENGTH OF THEIR “DEFENSIVE” COMPETENCIES AS THEY ARE ABOUT THEIR “OFFENSIVE” COMPETENCIES?

Defenses, barriers, and controls save lives. When errors occur and hazards are activated, defenses, barriers, and controls provide the protective safeguards that keep patients safe from harm. “Not all of the errors result in patient harm. This is due to the fact that in health care, as in other industries, defenses are in place. Defenses are protective measures put in place to reduce the likelihood of negative outcomes resulting from an unsafe act” (Drews 2012, 332).

Defenses and barriers can be designed for either prevention or protection. “Barriers that are intended to work before a specific initiating event takes place, serve as a means of prevention. Such barriers are supposed to ensure that the accident does not happen. . . . Barriers that are intended to work after a specific initiating event has taken place serve as means of protection. These barriers are supposed to shield the environment and the people in it, as well as the system itself, from the consequences of the accident” (Hollnagel 2004, 76). Hospital leaders must understand the adequacy and effectiveness of the organization’s defenses and controls and their contribution to keeping patients safe.

Even high-performing organizations can suffer catastrophic failure when they do not maintain effective defenses and controls against harm. The following are a few examples:

• A nuclear power plant that failed to maintain effective defenses against human and system performance failures experienced a partial core meltdown that caused the release of radioactive gases into the atmosphere (Three Mile Island, 1979).
• A commercial airline that failed to maintain its defenses against human error and maintenance error went out of business shortly after one of its planes caught fire in midair and crashed, killing all 110 people on board (ValuJet, 1996).

• A wildland firefighting unit that failed to follow established safety defenses (8 out of 10 Standard Firefighting Orders were compromised) were trapped by a wildfire and died after they were overtaken by the fast-spreading blaze (South Canyon Fire, 1994).

• A major accounting firm that depended on the public’s trust in its integrity and strict adherence to accounting standards failed to maintain its defenses and controls, resulting in a conviction for obstruction of justice and criminal complicity that ultimately forced the company to surrender its licenses and right to practice before the US Securities and Exchange Commission (Arthur Andersen, 2002).

• The engineer of a commuter train in New York was found to have been the direct cause of the train’s derailment by going three times the mandated speed around a bend in the track, resulting in four passenger deaths and 61 injuries. The engineer had been suffering from sleep apnea, but the National Transportation Safety Board found that if a required safety defense mechanism had been installed (Positive Train Control), the accident could have been prevented (Spuyten Duyvil, 2013).

• A 10-year-old boy died on one of the world’s tallest waterslides at a theme park in Kansas City, Kansas, that was later found to have violated international design standards for safe operation and failed to repair and maintain necessary safety defenses such as the brake system (Schlitterbahn Waterpark, 2016).

An adage in professional football is that “defense wins championships.” The top-ranked defensive team during the regular season has won 17 Super Bowl championships, whereas the top-ranked offensive team has won only eight times. Forty-three (or 81 percent) of the 53 Super Bowls have been won by a top 10 defensive team. The winner of the 2019 Super Bowl, the New England Patriots, had the seventh-best defense out of 32 teams, while the losing Los Angeles Rams, who were held to just three points, had the twentieth-worst defense in the National Football League (ESPN 2019). Of course, great offensive teams have also had championship seasons. “We found that when it comes to winning a title, or winning in sports in general for that matter, offense and defense carry nearly identical weight. In virtually every sport, you need either a stellar offense or a stellar defense, and having both is even better” (Moskowitz and Wertheim 2012, 1). Excellence on both offensive and defensive provides an even greater chance of success.
What’s the point? Healthcare organizations—just like high-risk, high-reliability organizations, high-performing businesses, or championship-winning athletic teams—need to demonstrate defensive competence as well as offensive competence to excel. Offering the best clinical excellence in the world does not much matter if a healthcare system’s defenses and controls do not consistently and continuously protect patients from the inevitability of human error. In short, defense saves lives.

THE PURPOSE OF DEFENSES

Broadly, the term defenses comprises protections against hazards such as safeguards, barriers, and controls. The difference is semantic: When we design safeguards and barriers, we do so to guard against some action occurring—for example, a safeguard against patient falls or a barrier against the spread of infection. When we design controls, we do so to limit an action—for example, a control for a smart intravenous (IV) pump limits the free flow of medication or dosing level.

Three types of defenses will be discussed in this chapter: physical defenses, administrative defenses, and human defenses. Understanding how these types of defenses and controls function and how to effectively develop, deploy, monitor, and improve them is critical to a hospital’s efforts to keep patients safe from the potentially harmful effects of human error or system weaknesses. Every member of the patient care team, as well as the leadership team that supports their delivery of safe care, should build the following steps into their patient care practices (DOE 2012, 1-19):

1. Clarify the scope of work. Make sure that work expectations are clear and understood by the entire patient care team and that the necessary resources (e.g., supplies, equipment, competent staff) are readily available.
2. Analyze the hazards. Identify, analyze, and categorize the hazards associated with the task or process being undertaken.
3. Develop and implement defenses and controls. Identify, activate, and implement the defenses and controls that are appropriate for a situation, either to prevent a hazard from causing harm or to mitigate, contain, or divert the harmful effects of a hazard.
4. Perform work with activated defenses. Perform work safely with defenses and controls activated and working as designed.
5. Offer feedback for improvement. Assess the adequacy of the defenses and controls applied in a particular process or procedure, openly consider whether the defenses were circumvented, or identify the need for new or revised defenses.
Organizational drift from the desired safe care practices of high-reliability health-care organizations is determined by monitoring the gap between work as planned and work as performed. Achieving harm-free healthcare is contingent on making sure that work as performed reflects the work as planned defined in steps 1–3.

Defenses serve two main purposes—to prevent harm or to mitigate harm. Serious safety events that result in an injury to, or death of, a patient unfold in a five-step dynamic. First, an initiating error or action activates an existing hazard that may lead to patient harm. Second, flawed defenses and controls fail to protect the patient against hazards. Prevention barriers or defenses are designed to block potentially harmful actions from activating a hazard.

Third, error precursors—unfavorable conditions in the patient care environment—create error-likely situations or error traps. Mitigation barriers or defenses are designed to contain or reduce the impact of a hazard once it has been activated. For example, suppose that a surgeon and surgical team failed to follow the four-count standard protocol to prevent retained foreign objects and left a retained sponge—Gossypiboma—inside the patient. The application of a final preventive defense—scanning the patient using a radio frequency identification wand—was successful, and the retained sponge was removed before final suture. Another example of a mitigating defense is the sprinkler systems in hospitals that are designed to contain the hazard of fire.

Fourth, latent organizational weaknesses create conditions in the patient care environment that provoke errors or contribute to the deterioration of defenses and controls. Deficiencies in management policies, staff training programs, and norms, attitudes, and beliefs that do not reflect a culture of safety are examples of latent organizational weaknesses.

Lastly, when an initiating action by an individual is in error or a rule violation, and flawed defenses, error precursors, and latent organizational weaknesses align, patient harm is a probable outcome of the care process. James Reason defines defenses as follows (Reason and Hobbs 2003, 91):

Defences, barriers, and safeguards are features of the system that have been put there to help the system cope with unplanned and untoward events that have happened in the past, or have been imagined by the system designers. Unfortunately, gaps in defences may only become apparent after an accident has occurred. These gaps may involve defences that have failed to perform as intended or defences that were inadequate or entirely absent.

Defenses are designed to minimize the potential negative effects of errors—errors that may provoke a hazard and cause harm.
Many preventive defenses in healthcare employ technological barriers to block the effects of errors and avoid triggering a hazard. For example, the use of computerized provider order entry (CPOE) has improved communications among patient care teams, expanded the availability of information, and increased the speed of order processing. CPOE defensive controls help prevent the use of inappropriate medications, administration of the wrong dose of a drug, or administration of a drug at the wrong frequency. CPOE defensive controls also aid with monitoring the medication management process, eliminating confusing and illegible handwriting, and reducing the risk of look-alike/sound-alike drug errors (Wachter 2012, 211).

Bar-code medication administration (BCMA) is another excellent example of a physical and technological barrier designed to protect patients from receiving the wrong medication or the wrong dose or frequency of a medication. The BCMA defense requires nurses to swipe the bar code on the medication, the patient’s wristband, and their own badge, thereby establishing a three-way cross-check before the medication can be administered. “Effective use of BCMA technology can substantially reduce medication dispensing errors” (Wachter 2012, 214, 217).

Dr. Robert Wachter, chief of medical services at the University of California, San Francisco Medical Center, cites research by Eric Poon and colleagues (Poon et al. 2010) showing that multiple defenses provide layers of protection. In one case, a closed-loop system that combined CPOE, BCMA, and an electronic medication administration record led to a 50 percent decrease in drug administration errors and potential adverse drug events. High-reliability organizations refer to this strategy as defenses-in-depth.

DEFENSES-IN-DEPTH

Defenses and controls are designed, implemented, and strengthened over time to provide a protective barrier between human or system errors and patients. “High-hazard operations attempt to minimize vulnerability from human fallibility by using redundant systems, processes, and employees. Redundancy helps achieve reliability through duplication and overlap of effort” (B&W Pantex 2008, 20). Because any one defense may not be adequate to protect patients from harm, safe systems should build in multiple layers of defenses—defenses-in-depth—to create redundant, overlapping, and complementary defensive functions to block errors from causing patient harm.

Again, an analogy to football works here. Think about the functions of a football team’s defensive squad: The collective goal of the defense is to stop the forward progress of the opposing force (in healthcare, the potential harm-producing effects of error). Members of the defense have individual roles to play, but they
also complement the defensive efforts of their teammates, and their efforts are often redundant—for example, multiple defensive players might tackle an opposing offensive player. The defense comprises three layers: (1) the front line of defense—that is, the defensive line; (2) the linebackers, who defend against anything that gets past the front line; and (3) the defensive backs in the “secondary” defensive area of the field of play. On each team, two defensive players in the secondary have the responsibility of safeties, meaning that they are the last line of defense against the opposing force.

Who are your safeties? Football teams with excellent defenses-in-depth usually excel at winning games. Hospitals with strong defenses-in-depth win by keeping patients safe from the harmful effects of error and organizational weaknesses. “The presence of sophisticated system or component redundancy, also called defenses-in-depth redundancy, has changed the character of industrial accidents more than any other factor, making modern technological systems largely immune to isolated failures” (B&W Pantex 2008, 21).

**LESSONS FROM HIGH-RELIABILITY ORGANIZATIONS**

**Defenses-in-Depth: Nuclear Power Plants**

US nuclear power plants use a defenses-in-depth approach to minimize the possibility of releasing hazardous amounts of radioactive material into the environment. Nuclear power plants use three barriers to prevent the release of fission products into the environment: fuel rods, a reactor vessel and primary cooling system, and containment. While the chances of a single barrier or defense failing is unlikely, the chances of all three defenses failing simultaneously is extremely remote (FEMA 2019).

The US Nuclear Regulatory Commission (NRC) oversees the safety of the nation’s nuclear power industry. A defenses-in-depth approach has been a central tenet of the NRC’s safety regulations and requirements for nuclear power plants for many years. The defense-in-depth concept for protecting the public from the consequences of a nuclear reactor accident was first applied in the 1950s. “Defense-in-depth recognizes that our knowledge is imperfect. Although we plan for all conceivable accidents, the unexpected may still occur. Our design and operation of nuclear plants needs to be robust enough to compensate for this lack of knowledge” (Drouin 2016). Nuclear power plants implement multiple layers of defenses—defenses-in-depth—to
control the hazards associated with nuclear power generation, so that if one layer fails, the other layers of defense will compensate.

Hospitals should consider the three principles of defense-in-depth used by nuclear power plants when designing their hazard-specific defensive protections:

1. **Redundancy.** More than one component or element of the process should perform the same function—for example, having two or more sources of information to verify a patient’s identification or performing multiple checks before administering a high-risk medication.

2. **Independence.** The multiple components of a process rely on separate and distinct attributes to function—for example, the prescribing physician, pharmacist, nurse, and peer cross-checking nurse and the technological defenses of CPOE and BCMA all provide multiple independent verifications to minimize the possibility of a medication administration error.

3. **Diversity.** The multiple components of a process that perform the same function rely on different design features to operate—for example, backup power generation and batteries ensure that lifesaving support services such as ventilation and infusion pumps will continue to operate as required.

In the safe design of nuclear power plants and nuclear reactors, defenses-in-depth help (1) maintain reactor stability by limiting the ability of events to disrupt operation, such as seismically designed buildings; (2) protect the reactor if plant operations are disrupted with safety features such as emergency reactor core cooling with redundant pumps; (3) strengthen barrier integrity to guard against the release of radioactive material into the environment with, for example, leak-tight containment structures; and (4) protect the public if a release does occur through emergency preparedness plans (Drouin 2016).

**ADMINISTRATIVE DEFENSES**

Hazards can be identified and controlled by activating defenses. We know what the most prevalent, significant, and harm-producing hazards are in acute hospital settings. Despite this, hospitals collectively have not developed and implemented the defenses and controls necessary to neutralize these hazards and protect patients...
from potential harm. Chapter 5 summarized the top 10 threats to patient safety, which include patient falls, inpatient suicide, central line–associated bloodstream infections, and wrong-site, wrong-patient, or wrong-procedure surgery. Exemplar hospitals and healthcare systems in the United States have made great progress in designing defenses and controls to address these known hazards and to provide patient protections in error-likely situations.

For example, the Universal Fall Precautions implemented by hospitals include administrative defenses such as policies that require staff to familiarize patients with their environment and require patients to demonstrate their ability to use the call light. Physical or technical barriers and defenses against patient falls include having sturdy hand rails in patients’ rooms, bathrooms, and hallways and keeping hospital bed brakes in the locked position. Human defenses and controls include hourly rounding by staff to continuously check on patients and the physical environment to ensure the elements of the fall prevention precautions are in effect. An important human defense is making sure staff respond quickly to patients activating their call lights.

Administrative defenses and controls are not as reliable as physical or engineered controls because they rely on human training, judgment, and initiative to ensure that administrative policies and procedures are followed completely and correctly (DOE 2009, 3-6). Administrative defenses and controls that “significantly impact human performance” include the following (DOE 2009, 3-7):

- Strategic business planning, including goal setting, budgeting, priority setting, and resource allocation
- Organizational structure, including lines of authority and defined staff roles and responsibilities
- Processes and policies that define how work is to be conducted, including operations guidance, preventive maintenance, and work procedures
- Communications, including routine communications, meetings, and alarms
- Technical and administrative procedures, including human performance, safety, troubleshooting, records, self-assessment, and corrective action
- Training programs
- Personnel qualification standards that establish the physical, psychological, educational, and proficiency standards for each position
- Work management processes, including work initiation, prioritization, planning, and scheduling
- Human resource policies and practices, particularly related to staffing levels
• Human performance expectations and standards
• Information technology and information handling

Checklists are an effective administrative defense against the inherent hazards of complex, multistep processes and procedures, and they have been particularly effective in preventing errors of omission. In his book *The Checklist Manifesto*, surgeon and public health expert Atul Gawande (2009, 13) notes,

Avoidable failures are common and persistent. And the reason is increasingly evident: the volume and complexity of what we know has exceeded our individual ability to deliver its benefits correctly, safely, or reliably. The checklist is a different strategy to overcome our failures, builds on our experience, and takes advantage of our knowledge.

According to Gawande, checklists remind staff to follow the minimum necessary steps in a process and make the steps explicit. “You want people to make sure to get the stupid stuff right” (Gawande 2009, 51).

The application of checklists as a defense against active errors and latent conditions has been adopted as the Safe Surgery Checklist by the World Health Organization and has proven effective in reducing the rate of central line–associated bloodstream infections in US hospitals. Johns Hopkins developed a checklist of the necessary steps to avoid infections when inserting a central line: (1) wash hands with soap; (2) clean the patient’s skin with chlorhexidine antiseptic; (3) put sterile drapes over the entire patient; (4) wear a mask, hat, sterile gown, and gloves; and (5) put a sterile dressing over the insertion site once the line is in (Gawande 2009, 38). Gawande recommends that checklists must be quick and simple tools that are user friendly and modest in length and scope to be functionally useful in complex systems such as healthcare (Gawande 2009, 128).

**PHYSICAL AND TECHNICAL DEFENSES**

Physical and technical defenses are engineered controls such as hardware, software, and equipment that operate in the physical environment of care delivery. These defenses are designed to affect people’s behaviors, choices, and attitudes to avoid error traps, control hazards, and prevent harm (DOE 2009, 3-5). *Active controls* perform specific safety-related functions, such as universal barrier precautions to prevent infections, IV pumps to prevent medication errors, and round-tip surgical blades (scalpels) to prevent sharp injuries. *Passive controls* do not have to be
operated or maintained, which makes them more reliable since they do not require human involvement. Physical defenses and engineered controls provide the following advantages:

- Elimination of unnecessary human–machine interactions
- Error-tolerant designs that are used to mistake-proof human–machine interactions
- Interlocks to prevent improper operator actions
- Initiation of automatic protective actions when necessary
- Manager-initiated modifications to eliminate or minimize errors associated with work-arounds
- Resolution of deficiencies in the environment or working conditions to minimize their impact on performance

Physical defenses and barriers must be designed to counter and control the conditions that can contribute to safety events (DOE 2009, 3-6), such as inoperable equipment; poorly functioning controls, alarms, or indicators; work-arounds; temporary repairs; long-term modifications or alterations to the work space; nuisance alarms; excessive noise; missing labels; poor lighting; unusual work space or equipment conditions; cramped conditions; and awkward layout of equipment. In the handbook High Reliability Operations: A Practical Guide to Avoid the System Accident, B&W Pantex (2008, 137), the firm that contracts with the US Department of Energy (DOE) to oversee the safe storage of the country’s nuclear weapons stockpile, recommends:

Don’t hide those barriers! Safety barriers that employees don’t know about or understand are often violated and seldom effective. Don’t hide barriers from your employees [and] continually prompt employees to verify the effectiveness of barriers. Your employees need to understand which barriers are meant to defend against which hazards. After all, they have the most to lose if an ineffective or missing barrier leads to systemic failure.

Physical and engineered defenses can provide detection capability as well. Warning and alarm system defenses provide the patient care team with important health assessment and patient monitoring information, while electronic health records are designed with software lockouts that allow only one patient record to be opened at a time to avoid wrong-patient errors. Moreover, forcing function defenses provide hard-stop limits on the programming of smart IV pumps (Wetterneck 2012, 453).

Smart IV pumps provide an excellent example of engineered physical defenses and controls that suppress the hazards of wrong-dose, wrong-rate medication errors. The first programmable IV infusion pumps would accept any infusion rate and
programming entry errors—for example, entering the volume as the rate could result in a fatal dose. “Compared to medications delivered via other routes, IV medication errors are twice as likely to cause patient harm” (Vanderveen 2014). Beginning around 2004, smart IV pumps introduced a major defense against intravenous medication errors, the dose error reduction system. Wireless connectivity facilitated the integration of smart pumps with other systems and devices. These technological enhancements and safety defenses represented a major improvement in infusion safety that enhanced nursing productivity, aided clinical decision-making, improved patient monitoring, and reduced the variation in medication infusion processes (Vanderveen 2014).

According to Dr. Tim Vanderveen, smart IV pumps have significantly improved IV medication safety by (1) fostering the development of drug dose limits, (2) promoting the standardization of concentration and dosing units, (3) providing a treasure trove of infusion data, (4) documenting many “good catches” of prevented programming errors, (5) uncovering a high degree of variation in infusion pump practices, (6) identifying human factors–related issues that provide opportunities for better design, and (7) promoting wireless connectivity with server applications.

**HUMAN DEFENSES**

Nurses or other caregiving staff may sometimes be the cause of human error that threatens a patient’s safe care experience. At the same time, however, they are often the last line of defense against a hazard becoming a harm. The knowledge, skills, and abilities of the patient care team members are influenced by their past experiences, decision-making abilities, education, and training—all of which serve as a potent defense against human error and latent organizational weaknesses.

Human defenses are also driven by the cultural norms, values, beliefs, and attitudes of the organization and staff. “Culture is defined by people’s behavior, and safe behavior is value-driven. The true values of an organization are reflected in the observed acts of its people” (DOE 2009, 3-8). Thinking about their important role as “safeties”—the last line of defense—nurses and other caregivers at the sharp end of patient care must constantly consider the errors that could occur at each step in critical care processes and the hazards that create error-likely situations.

Performing this defensive function requires situational awareness and the application of readily available reminders of the human performance improvement tools that provide an additional defense against preventable harm. Human defensive actions include (1) pre-job briefings, (2) questioning attitude, (3) self-checking, (4) peer checking, (5) eliminating error precursors at the job site, (6) stopping when unsure, (7) adherence to procedures, (8) second-person verifications, and (9) attention and
alertness. These safe care practices and communication techniques were discussed in chapter 3.

**FACTORS THAT DEFEAT DEFENSES AND CONTROLS**

The Institute of Nuclear Power Operations (INPO) maintains safety standards for the nation’s 102 nuclear power plants and conducts routine safety inspections of nuclear facilities. During its many years of oversight of this high-reliability industry, the INPO identified several warning signs reflecting common weaknesses that contribute to the degradation of defenses and controls (DOE 2009, 3-25). Hospital leaders and performance improvement staff should consider these factors and use them to assess the effectiveness of the hospital’s defenses:

- **Overconfidence.** Staff are living on past successes and therefore do not recognize low-level problems and remain unaware of hazards.
- **Isolationism.** Benchmarking is seldom done, and best practices are not implemented; therefore, the organization lags others in the industry in many areas of performance and may be unaware of it.
- **Adversarial relationships.** Within the organization, employees are not involved and are not listened to, and they are not encouraged to raise concerns about safety. Adversarial relationships hinder open communications.
- **Informal operations.** Operational standards, formality, and discipline are lacking. Special projects and initiatives overshadow a focus on operations.
- **Weak engineering.** A loss of talent and lack of alignment with operational priorities causes weak engineering and design.
- **Production priorities.** Important equipment problems linger and repairs are postponed—safety is assumed and not explicitly emphasized in staff interactions and communications.
- **Inadequate change management.** Organizational changes are implemented before their impacts are fully considered—processes and procedures do not support strong performance following management changes.
- **Serious safety 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, and communicate poorly. Managers lack knowledge about the organization and lack operational experience. And senior leaders are not involved in operations, do not exercise accountability, and do not follow up.
• Lack of self-criticism. Self-assessment processes, such as management observation programs, do not find problems or do not address them—if a problem is identified, the results are not acted on in time to make a difference.

In conducting a thorough analysis of the causes of wrong-site, wrong-patient, and wrong-procedure surgeries, The Joint Commission’s Center for Transforming Healthcare identified 29 main causes that stemmed from the organization’s culture or occurred during the scheduling process, during the time the patient was in the preoperative holding area, or during surgery. For the wrong-site surgery cases reviewed in the project, controls and defenses were either absent, circumvented, or inconsistently applied. For example, during the scheduling process, unapproved abbreviations, cross-outs of information, and illegible handwriting were identified as event precursors. The inconsistent use of surgical site marking, time-out processes that were inconsistently used or not used at all, and inadequate patient verification by the team because of time pressures or distractions were causal factors in the preoperative holding area. Cultural contributions to surgical mistakes reflect an organization that has an inconsistent focus on patient safety and does not empower staff to voice their safety concerns (Joint Commission Center for Transforming Healthcare 2011).

ANALYZING THE STRENGTH OF DEFENSES THROUGH BARRIER EFFECTIVENESS ANALYSIS

Defenses and barriers should be routinely analyzed to determine their status (present or absent, activated or ignored) and their effectiveness at preventing patient harm. Each barrier or defense should be analyzed to (1) clarify the hazard that the defense is designed to control, (2) determine the threat that the defense is meant to protect against, (3) determine the effectiveness of the defense against the intended threat, and (4) assess the significance of identified weaknesses in the defense and their possible contribution to system safety events (B&W Pantex 2008, 139). High-reliability organizations reduce variability and improve the safety of performance by minimizing hazards, reducing the negative influences of complex interactivity, minimizing human error, and employing redundant independent barriers as backup measures (B&W Pantex 2008, 29).
A thorough barrier effectiveness analysis will reveal five defensive states—six if the hospital is still routinely harming patients—that indicate the effectiveness of the organization’s safety defenses:

1. Defense was in place, was activated, and was effective at controlling the hazard and preventing patient harm.
2. Defense was in place, was activated, but was penetrated (ineffective), allowing the hazard to cause harm.
3. Defense was in place but was not activated (possible act of omission).
4. Defense was circumvented (possible act of commission).
5. Defense was not in place and was not required.
6. “What is a defense?” (ignorance of the effective use of defenses, barriers, and controls leads to patient harm).

Barriers and defenses can be assessed retrospectively as part of a root cause analysis to determine how the designed defenses and controls worked, how they might have failed, and how they could be strengthened to provide greater protection from harm in the future. “Investigators use barrier analysis to identify hazards associated with an accident and the barriers that should/could have prevented it” (DOE 2012, 1-21). The effectiveness of defenses can also be assessed prospectively through scenario testing and concurrently by the patient care team and the patient safety coach. Being mindful of the emerging situation as patient care team members or caregivers work through a safety-critical process or procedure should include an awareness of the safety defenses that are supposed to control process-specific hazards and an assessment of their activation and effectiveness. A sample barrier effectiveness analysis for fall-related defenses is outlined in exhibit 11.1.

Barrier effectiveness analysis considers five elements (DOE 2012, 2-64):

1. Hazard identification—identify the targeted hazard that the defense is supposed to control.
2. Barrier identification—identify each barrier that is supposed to target and control the identified hazard.
3. Barrier performance—assess how the barrier or defense actually performed, whether the barrier was in place or not, and whether the barrier failed to perform as designed.
4. Causes of barrier failure—identify the probable causes of the barrier’s failure.
5. Consequences—evaluate the consequences of the barrier’s failure and contributions to a safety event.
Hazard: Falls
Target: Patients
Event: Patient fell while trying to ambulate alone to access the bathroom; suffered a bruised hip and shoulder, which extended the patient’s hospitalization two days.

Defense/Barrier
(Analysis is performed for each defense that is designed to control each hazard.)
Have sturdy handrails in patient rooms, bathrooms, and hallways (the fifth defense of the 12 Universal Fall Precautions).

Defense Purpose
(prevention or mitigation)
Prevention defense

Defense Type
(physical, administrative, or human)
Physical

How did the defense/barrier perform?
This defense was not activated because other defenses failed first; therefore, handrails were never used. Staff failed to respond to repeated call light requests for assistance to go to the bathroom, and the defense of hourly nurse rounding was not performed.

Why did the defense/barrier fail?
This defense did not fail; it was never activated because other layers of defense failed first.

What effect did the defense/barrier have on the serious safety event?
None.

Should the defense/barrier be strengthened in any way?
Not at this time.
In support of the barrier effectiveness analysis, hospitals should also develop a safety case for every major error-provoking and harm-producing hazard. The safety case (1) identifies a claim or concern about a safety-critical process or procedure; (2) makes a structured argument to support the claim; and (3) provides evidence that demonstrates the validity of the argument (e.g., facts, research, test data, expert opinion).

For example, a safety case for IV infusion pumps should include a hazard analysis to identify related hazards and provide “an argument that hazards caused by the device have been adequately addressed. This is accomplished through a thorough analysis of hazards and implementation of adequate controls to address the hazards” (FDA 2014, 10–11). The safety case for infusion pumps should make a claim about the safety of the pump, clarify the patients and conditions for which the pump is intended, and establish that effective defenses and controls have been implemented to prevent or mitigate the potential harmful effects of the hazard.

Industrial safety expert Erik Hollnagel (2004, 97–98) has defined a set of “pragmatic criteria” that can be useful for assessing the adequacy and effectiveness of a hospital’s patient safety defenses, barriers, and controls:

- **Efficiency or adequacy**—how efficient the barrier is expected to be in achieving its purpose
- **Resources required**—the resources needed to design, develop, implement, and maintain the barrier
- **Robustness (reliability)**—how reliable and resistant the barrier is—for example, how well it can withstand the variability of the environment, including working practices, degraded information or noise, unexpected events, and wear and tear
- **Delay in implementation**—the time from conception to implementation of a barrier
- **Applicability to safety-critical tasks**—safety-critical tasks play a special role in sociotechnical systems
- **Availability**—whether the barrier can fulfill its purpose when needed
- **Evaluation**—whether a barrier works as expected and is available when needed
- **Dependence on humans**—the extent to which a barrier depends on humans to achieve its purpose
LESSONS FROM HIGH-RELIABILITY ORGANIZATIONS

Safety Management in Air Traffic Control

Each day, the Air Traffic Organization (ATO), the operational arm of the US Federal Aviation Administration, guides more than 50,000 flights through 30.2 million square miles of domestic and international airspace. The ATO’s mission is to ensure that every flight departs and arrives safely. During the 12-year period ending in 2015, 50 fatal accidents related to air traffic management occurred in the US National Airspace System; only one involved a commercial air carrier. In three of the last five years ending in 2015, no fatal accidents related to air traffic management occurred.

In 2015, air traffic operations totaled 132.1 million flights. Air traffic operations experienced only 19 high-risk events in that year, reflecting a safe performance rate of 99.99451 percent. The US air traffic control system is an exemplary high-reliability organization, operating in an extremely high-risk environment while experiencing very few events. The ATO maintains a comprehensive Safety Management System, which received more than 15,000 reports in 2015 through its Voluntary Safety Reporting Programs—the largest of its kind in the world. The reporting system “allows those on the frontlines of safety—such as controllers, technicians, and flight crews—to document incidents, concerns, and potential solutions without the fear of reprisal” (FAA 2015, 4).

The ATO’s primary measure of safety-related performance is the system risk event rate, a 12-month rolling rate that reflects the frequency of serious airborne losses of separation per 1,000 reported events. In September 2015, the rate was 2.62 serious losses for every 1,000 reported losses, well below the ATO’s target of 20.

The ATO assesses safety incidents through a rigorous Risk Analysis Process, regardless of whether the event occurred in the air, on an airport surface, or in one of the ATO’s technical systems. Assessments are performed by a panel of experts that includes pilots, controllers, and human factors specialists. Significant hazards include runway incursions, degradation of equipment that could affect the safety of air traffic or flight information services, and loss of separation in the air. The most persistent safety problems reported through the ATO’s voluntary reporting systems are
(1) safety culture, (2) procedural deficiency, (3) equipment design or function, (4) interface with other facilities, (5) compliance with directives, (6) organizational policy, and (7) delegation of work.

A significant safety concern is the growing complexity and congestion of the National Airspace System, which is particularly apparent in the airfield environment. The ATO has enhanced its defenses and controls through the Runway Safety Program, which involves integrating multiple layers of surface surveillance and alerting technology, redesigning problematic runway and taxiway layouts, and improving safety aids such as runway lighting and signage.

Over the 10-year period ending in 2015, improvement in runway-related safety defenses and in the Runway Safety Program overall resulted in a 44 percent decrease in serious runway incursions (incorrect presence of an aircraft, vehicle, or person in a protected area for takeoffs and landings) and prevented damage and injuries from runway excursions (when an aircraft veers off the runway or overruns the runway).

The ATO’s Risk Analysis Process involves assessment of the severity and likelihood of recurrence of safety events and assessment of the National Airspace System’s defensive layers and barriers. These defenses and barriers represent the “controllability” of the situation. The analysis reviews the systemic factors and human errors that contributed to a safety event and the likelihood that those factors will align again in the future.

The ATO’s barriers “fall into three categories: air traffic control, pilot, and [National Airspace System] technology infrastructure. Each category is composed of many discrete barriers designed to prevent a loss of required separation from occurring (termed resolution barriers) or prevent a loss of separation from becoming a collision (recovery barriers)” (FAA 2016, 9). Examples of ATO technology defenses include alerts, advisories, and surveillance systems. Examples of organizational defenses include planning, communications, and supervisory interventions. Examples of human (pilot) defenses include situational awareness, execution, and “See and Avoid.” Each defense and barrier is scored for effectiveness. Those scores allow safety analysts “to inspect the effectiveness of barriers and the factors that influence their performance at different locations and at different levels of specificity. We can identify trends in individual or composite barrier performance, which, in turn, help us understand the conditions that contribute to vulnerabilities or successes” (FAA 2016, 10).
PATIENTS DEFENDING THEIR OWN SAFETY

Clearly, no one is more invested in patient safety than the patient. Patients must be encouraged, empowered, and fully engaged as active members of the patient care team in the hospital setting. “Research shows that when patients are engaged in their health care, it can lead to measurable improvements in safety and quality” (AHRQ 2013). According to the Agency for Healthcare Research and Quality’s “Guide to Patient and Family Engagement in Hospital Quality and Safety,” hospitals should promote better communication among patients, family members, and healthcare professionals beginning at admission and throughout the patient’s stay. “When patients speak up—and when health care professionals engage and empower them to do so and then understand and act on what we hear—we strengthen the health care team. We know that successful organizations that are serious about shared decision making and focused on safety encourage patients to” (Brady and Gandhi 2018):

- Ask questions to make sure they understand their diagnosis, treatment options, and care plans
- Speak up about the risks and problems they see or may encounter
- Express their values

Indeed, “patients themselves can help to safeguard their own wellbeing and promote change” (Health Foundation 2013, 3). When patients actively participate in their care, they are involved in decisions about their care plan and kept informed about what is happening to them or about to happen to them. When patients participate, the quality and safety of care improves. Research indicates that greater levels of patient participation are associated with fewer adverse events (Health Foundation 2013, 15).

Patients can engage in three broad behaviors to contribute to their own safety: (1) making sure that their treatment is appropriate for them, (2) making sure that treatment is given as planned and according to appropriate protocols, and (3) helping to identify and reduce problems and risks within healthcare systems (Health Foundation 2013).

AN INTERESTING THOUGHT—MAYBE NOTHING MORE

Our current metrics and measures for evaluating individual job performance are mostly offensive performance measures; however, performance evaluations should also include individuals’ defensive contributions to patient care. Leading hospitals
assess staff performance against behavior-based expectations, encouraging staff to take personal responsibility for safe care practices and actively report safety concerns. By doing so, they reinforce the hospital’s culture of safety and commitment to zero patient harm.

In professional basketball, the key statistical metric for players is their “efficiency” rating—a measure of both the player’s offensive production and defensive performance. This rating reflects the player’s overall performance. This measure is critically important, since the same five players on the court must excel on both offensive and defensive—just like the frontline “players” who provide care to patients in a hospital.

In professional hockey, players perform in either offensive or defensive positions, but they all have defensive responsibilities while on the ice. All players receive a “plus/minus” rating for their performance during each game. Players receive +1 for every goal the team scores while they are on the ice and –1 for every goal the team gives up while they are on the ice. A player’s plus/minus statistic correlates with excellent overall performance and contribution to winning games, both offensively and defensively.

Here’s an interesting idea: Every day a member of the patient care team is involved in an event-free day, they get a +1, and every day that the team experiences a safety event, all the team members receive a –1. Hospitals and patient care teams often recognize and celebrate when they have not experienced a central line–associated bloodstream infection, ventilator-associated pneumonia, catheter-associated urinary tract infection, patient fall, or other serious safety event over a long period of time. Providing teams and team members with a “Patient Safety Plus/Minus Score” could provide recognition and reinforcement of new safety behaviors and their impact on saving lives!

THE PARITY ZONE

Psychologist James Reason, in his book Managing the Risks of Organizational Accidents, describes the dynamic, often competing tensions and motivations in a high-hazard industry—or almost any organization—between production and protection. An organization’s resources are generated through the production of goods and services, which makes the funds available for the organization’s protections. “Since production creates the resources that make protection possible, its needs will generally have priority. . . . This is partly because those who manage the organization possess productive rather than protective skills” (Reason 1997, 4).

Reason explains that the prioritization of production over protection (the organization’s defenses against patient harm) is partly attributable to the fact
that production information is clear, direct, and readily understood, whereas protection-related information is indirect, discontinuous, and “indicated by the absence of negative outcomes.” Reason’s assessment of the organizational leader’s bent toward production over protection is concerning if it holds true for healthcare executives. If an organization fails to invest in adequate protections (i.e., adequate defenses and barriers against serious safety events), its production will suffer as a result of waste, rework, low patient satisfaction, low morale, and loss of community trust. “In an ideal world, the level of protection should match the hazards of the productive operations—the parity zone. The more extensive the productive operations, the greater is the hazard exposure and so also is the need for corresponding protection” (Reason 1997, 3). Hospital leaders should assess their organization’s parity zone to establish the right balance between production and protection and to ensure that the entire organization understands that balance. As a hospital or healthcare system leader, what are your protection skills, and how can they be strengthened?

CONCLUSION

Chapter 11 describes the safe care practices that will strengthen a hospital’s defenses to protect patients from harm. Even high-performing organizations can suffer catastrophic failure when they do not maintain effective controls and defenses against harm. Three types of defenses are discussed in this chapter: physical defenses, administrative defenses, and human defenses. Understanding how these defenses and controls function and how to effectively develop, deploy, monitor, and improve them is critical to a hospital’s efforts to keep patients safe from the potentially harmful effects of human error and system weaknesses.

CHAPTER 11 SAFE CARE PRACTICES

1. Understand the adequacy and effectiveness of the organization’s defenses and controls and their contribution to keeping patients safe.

2. Encourage every member of the patient care team, as well as the leadership team that supports their delivery of safe care, to build the following steps into their patient care practices: clarify the scope of work, analyze the hazards, develop and implement defenses and controls, perform work with activated defenses, and offer feedback for improvement.
3. Build safe systems that include multiple layers of defenses—defenses-in-depth—to create redundant, overlapping, and complementary defensive functions to block errors from harming patients.

4. Consider the factors that defeat defenses and controls and use them to assess the effectiveness of the hospital’s defenses.

5. Assess the organization’s “parity zone” to establish the right balance between production and protection and to ensure that the entire organization understands that balance.

REFERENCES


