Moving Risk Assessment Upstream to the DESIGN PHASE

By Bruce K. Lyon, David L. Walline and Georgi Popov

TO ERR IS HUMAN; TO PREVENT BY DESIGN IS DIVINE. For occupational serious injuries and fatalities (SIF) to be effectively and consistently reduced, safety must be designed into workplace facilities, systems and methods. Risk avoidance and elimination, the most effective risk treatment options, are generally only possible by design and redesign efforts.

A clear link exists between workplace fatalities and unsafe or error-prone designs. Studies in the construction industry indicate that more than 40% of fatalities are connected to the design aspect (Behm, 2005). In Australia, safety in design is an action area of the Australian Work Health and Safety Strategy. A Safe Work Australia (2014) study examined work-related fatalities that occurred from 2006 to 2011 and involved machinery, plant and powered tools. Its purpose was to assess the extent to which unsafe design contributed to the fatalities. Of these fatalities, 12% were identified to have been caused by unsafe design or design-related factors, while 24% were possibly caused by design-related factors.

In the medical field, the term *never events* is used to refer to fatalities, serious preventable events, medical errors and other incidents that are totally unacceptable to society (Morgenthaler & Harper, 2015). Never events, however, cannot be fully avoided where degraded "always conditions" exist. Always conditions are the elements within a system. When these always conditions are degraded with embedded hazards, flaws and undue complexity, a great risk of harm exists. Never events and degraded always conditions are incompatible, opposing forces, much like matter and antimatter. From the OSH perspective, SIFs are considered never events and the workplace systems are the always conditions.

Patterns of interactions between system elements (humans, tools, machinery, software, materials, procedures and environment) characterize human work. Such work is generally performed to achieve a purpose within system elements, conditions and environment over a period. Most interactions are intentional and inconsequential; however, some things do not always go as planned or intended. Human error represents system interactions that are unintended, but as Shorrock (2016) notes, there is almost always more to it than just an error on the part of the human. Always conditions designed into the system elements include human, organizational and societal factors. Degraded conditions might include confusing and incompatible interfaces, labels or controls that are difficult to read or distinguish, unserviceable equipment, missing tools and equipment, time pressure, inadequate staffing, prolonged work leading to fatigue and stress, varying levels of competence or different cultures.

For never events to be completely avoided, the always conditions that present hazards and risks that make them possible must be designed out of the systems. In the OSH world, this concept is known as prevention through design (PTD).

The Concept of PTD

In 2011, ANSI/ASSP Z590.3-2011(R2016), Prevention Through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes, was the first U.S. standard to address the need for incorporating safety into the design and redesign phase. A key element of ANSI/ASSP Z590.3 is that it provides guidance for life cycle risk assessments and a design model that balances environmental and OSH goals over the life span of a system (Figure 1). Systems such as facilities, equipment and products have a defined life cycle in which risks change. These points in the system's life cycle where new risks are introduced or existing risks may increase represent PTD risk assessment trigger points (Figure 2).

A stated goal of the PTD standard is to educate designers, manufacturers, OSH professionals, business leaders and workers in the principles so that those principles can be designed into new and existing facilities, processes, equipment, tools and methods. Fundamentally and practically, it makes the most sense to avoid a problem rather than allow it to exist and try to manage it.

Manuele (2014) states that "over time, the level of safety achieved will relate directly to whether acceptable risk levels are

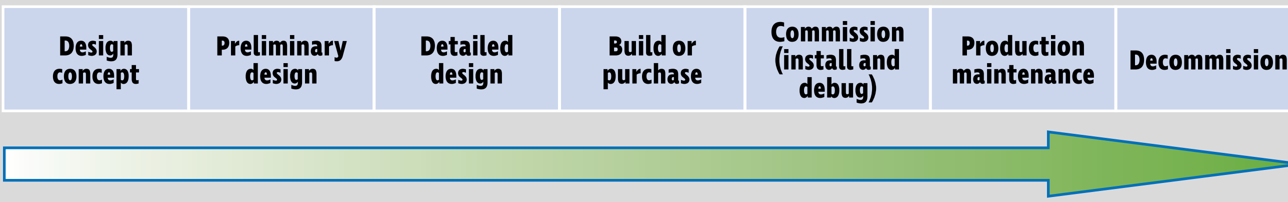
KEY TAKEAWAYS

- **Studies indicate that gaps found in design are significant contributors to workplace serious injuries and fatalities (SIFs), which points to the need for prevention through design (PTD) concepts.**
- **The greatest opportunity to avoid, eliminate and reduce risk to an acceptable level and prevent SIF events is upstream in the design and redesign of processes, equipment, facilities, tools and work methods.**
- **The primary goal of safety and risk management is to achieve and maintain a level of risk that is as low as reasonably practicable while accomplishing the organization's objectives. OSH professionals have a vital role to play in PTD and design safety reviews.**
- **This article provides OSH professionals a practical approach to establishing a method for anticipating, recognizing, avoiding, eliminating and minimizing operational hazards and risks before they are introduced into the workplace.**

NOSTAL6IE/ISTOCK/GETTY IMAGES PLUS

FIGURE 1

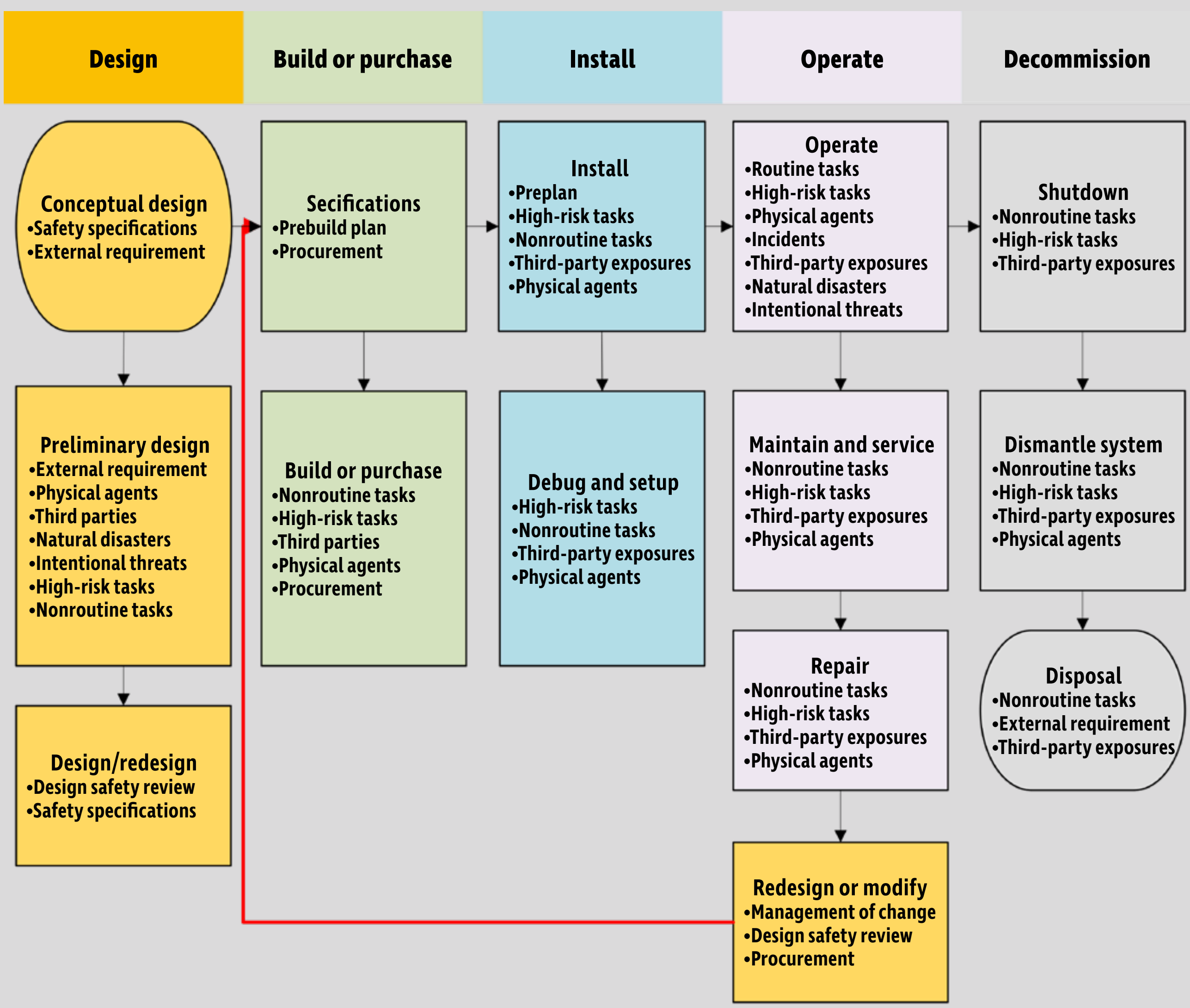
LIFE CYCLE PROCESS



Note. Adapted from Prevention Through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes [ANSI/ASSP Z590.3-2011(R2016)] by ANSI/ASSP, 2016, Park Ridge, IL: ASSP.

FIGURE 2

PREVENTION THROUGH DESIGN DURING SYSTEM'S LIFE CYCLE



Note. Adapted from *Risk Management Tools for Safety Professionals*, by B.K. Lyon and G. Popov, 2018, Park Ridge, IL: ASSP.

achieved or not achieved in the design and redesign processes." His statement is in accordance with the hierarchy of controls model found in ANSI/ASSP Z590.3 (Figure 3). The PTD model promotes the use of higher-level controls—avoidance, elimination, substitution and engineering—upstream in the design phase as the most effective and economical. Most agree with this concept; however, in practice, few organizations take full advantage of incorporating safety into the preoperational phase. This presents a major opportunity for OSH professionals equipped with the skills and desire to advise and guide organizations through the process of identifying hazards and reducing risk during design and redesign (Popov, Lyon & Hollcroft, 2016).

The greatest opportunity for advancing OSH lies within the practice of PTD. This article provides OSH professionals a practical approach to establishing a method for anticipating, recognizing, avoiding, eliminating and minimizing operational hazards and risks before they are introduced into the workplace.

System Safety Roots

PTD concepts are rooted in system safety. Stephans (2004) describes system safety as the effort to make things as safe as is practical by systematically using engineering and management tools to identify, analyze and control hazards. The 15 tenets of system safety that Stephans describes (Table 1) align with those found in risk management and PTD standards, notably ANSI/ASSP/ISO 31000-2018, Risk Management: Guidelines, and ANSI/ASSP Z590.3.

A review of the tenets of system safety reveals that strong correlations exist between system safety and PTD. System safety tenets strongly reflect the concepts of risk reduction through assessment, treatment and designing safety into system elements, as do PTD principles.

Hazardous Energy Control

A critical area to be considered in design is the control of hazardous energy. A prominent theory developed by William Haddon Jr., known as Haddon's energy release theory, establishes a relationship between incident causation and risk control methods. Haddon's model relates well to engineers and can be applied systematically. It includes 10 sequential control strategies that should be considered in the design of new products and systems:

1) Prevent stored energy.
2) Reduce stored energy.
3) Prevent energy release.
4) Reduce rate of release.
5) Separate energy release from humans and assets by space or time.
6) Separate energy release from humans and assets by physical barriers.
7) Modify contact surfaces.
8) Strengthen susceptible structures.
9) Increase detectability and prevention of harm.
10) Prevent further damage.

As Haddon's strategies indicate, the most effective control is accomplished when it is incorporated into the design. Special attention to the potential for hidden energies in products and systems is warranted. Table 2 provides a simple list of energy types and hazards that should be considered during a design safety review (Popov, Lyon & Hollcroft, 2016).

Barriers to PTD

The concept of addressing safety during design seems logical and desirable; however, the practice of doing so occurs far too rarely. For many organizations, OSH professionals are not invited to the design table or included in the design and redesign processes. The reasons are many.

Recently, one of the authors participated in the planning for a new manufacturing facility to be built in the U.S. The project planning session was to determine the work breakdown structure, specific steps and tasks, resources and time frames over the 18 months leading up to operations. The planning team included regional and local management, engineering, production, maintenance, quality, human resources, and safety, health and environment staff.

As the team worked through the steps it became apparent to the author that a risk review of the new facility's design had not been discussed. When it was suggested that a risk assessment of the designs would be beneficial, there was hesitation from team members. Most of the members did not see this as a feasible time for an assessment and indicated that risk assessments would be performed once the facility was operational. Two safety representatives explained that it would be difficult to identify hazards and assess risks without the physical structures, equipment and employees in place. It was the group's belief that the corporate design and engineering departments were addressing all necessary requirements including safety and code compliance issues in the design. As a result, no formal safety review of the design was scheduled. The author continued to work with team members as the designs and construction progressed, identifying and addressing hazards and concerns. However, embedded problems were introduced into the new facility including:

•Emergency shower and eyewash stations placed directly in front of or near electrical panels. Specifically, these stations were located in the forklift recharging bays at each of the organization's similarly designed facilities.

•Lack of ventilation and local exhaust systems. As part of the quality assurance process, a destructive testing laboratory performs tests including chemical reactions, grinding, cutting, braz-

FIGURE 3

ANSI/ASSP Z590.3 PTD RISK REDUCTION HIERARCHY OF CONTROLS MODEL

	Controls
Most preferred	**Risk avoidance:** Prevent entry of hazards into a workplace by selecting and incorporating appropriate technology and work methods criteria during the design processes.
	Eliminate: Eliminate workplace and work methods risks that have been discovered.
	Substitution: Reduce risks by substituting less hazardous methods or materials.
	Engineering controls: Incorporate engineering controls/safety devices.
	Warning: Provide warning systems.
	Administrative controls: Apply administrative controls (e.g., the organization of work, training, scheduling, supervision).
Least preferred	**PPE:** Provide PPE.

Note. Adapted from Prevention Through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes [ANSI/ASSP Z590.3-2011 (R2016)], by ANSI/ASSP, 2016, Park Ridge, IL: ASSP.

TABLE 1
SYSTEM SAFETY TENETS & PTD ALIGNMENT

System safety tenets	Risk management and PTD concepts
1) Systematically identify, evaluate and control hazards to prevent (or mitigate) incidents.	Hazard analysis and risk assessment Risk treatment
2) Apply a precedence of controls to hazards starting with their elimination, designing to preclude hazards and finally administrative controls. Administrative controls include signs, warnings, procedures and training. (The lowest precedence are those controls that rely on people.)	Risk treatment Hierarchy of controls Layers of protection
3) Perform proactively rather than reactively to events. This starts with a program plan.	Risk management process Prevention through design
4) Design and build safety into a system rather than modifying the system later in the acquisition process when any changes are increasingly more expensive.	Prevention through design
5) Develop and provide safety-related design guidance and give it to the designers as the program is initiated.	Prevention through design Design safety specifications
6) Use appropriate evaluation/analysis techniques from the tabulated variety available.	Hazard analysis and risk assessment
7) Rely on factual information, engineering and science to form the basis of conclusions and recommendations.	Establish context Risk-based decision-making
8) Quantify risk by multiplying the ranking of undesired consequences of an event by the probability of occurrence. There are variations to this "equation."	Risk analysis
9) Design, when allowed, to minimize or eliminate single-point failures that have an undesired consequence. Make at least two-fault tolerant, that is, tolerant of multiple faults or system breakdown that would have adverse safety consequence.	Prevention through design Layers of protection/defenses
10) Identify, evaluate and control hazards throughout the system's life and during the various operational phases for normal and abnormal environments.	Prevention through design and redesign Design safety reviews Management of change System's life cycle
11) After application of controls to mitigate hazard(s), management must recognize and accept the residual risk.	Acceptable risk level ALARP
12) Recognize the quality assurance interface: a) Decrease risk by using materials that are properly specified and possess adequate quality assurance; and b) implement to continually improve the system.	Design safety specifications
13) Tabulate and disseminate lessons learned and incorporate those lessons for future safety enhancement.	Risk communication and consultation
14) Apply system safety to systems to include processes, products, facilities and services.	Prevention through design
15) Recognize that near-hit conditions, if not corrected, most likely develop into incidents.	Hazard/risk identification Risk assessment Risk treatment

ing and welding, which produce air contaminants; however, these health hazards were not considered during the design phase.

•Lack of adequate emergency/tornado shelter space for planned occupancy in the new facility. In addition, conveyor systems and equipment created obstacles for emergency evacuation routes in some areas of the facility.

•No containment for indoor tank storage of chemicals to prevent spillage from entering floor drains.

•Multiple blind corners and bottlenecks for forklift and pedestrian traffic.

•Elevated work platforms requiring fixed ladders and stairs, guardrails, and lifting and lowering of equipment and materials. One platform containing electrical service panels was 24-ft high with only ladder access.

•Poorly designed workstations such as nonadjustable work surfaces and seating, excessively wide conveyors, extensive manual material handling, poor placement of storage, high noise areas and poor lighting.

This experience is likely not uncommon for OSH professionals. Many organizations require OSH practitioners to only focus on the operational phase. The authors estimate that 10% of OSH professionals' time is spent in the preoperational and design phase. This assumption was tested by performing a review of job descriptions for OSH positions posted on the ASSP Career Center. The review revealed that a majority (88%) of the listed job responsibilities described duties such as program management, regulatory compliance, workplace audits and inspections, incident investigations, employee training, loss analyses and other duties associated with operations. Less than 12% of the job postings reviewed mentioned preoperational du-

TABLE 2
ENERGY TYPES & HAZARDS

Energy	Hazards
Mechanical	Acute force to tissues, chronic stress to tissues
Physical	Noise, vibration, gravity, inertia, configuration
Chemical	Toxicity, caustic, acute, chronic
Electrical	Electrocution, explosion, fire, arc flash
Biological	Bacteria, bloodborne pathogens, microorganisms, animals, insects
Thermal	Extreme temperatures
Radiological	Ionizing, nonionizing

Note. Adapted from *Risk Assessment: A Practical Guide to Assessing Operational Risks*, by G. Popov, B.K. Lyon and B. Hollcroft, 2016, Hoboken, NJ: John Wiley & Sons.

FIGURE 4

PERCENT OF TIME SPENT IN THE FOUR RISK MANAGEMENT STAGES

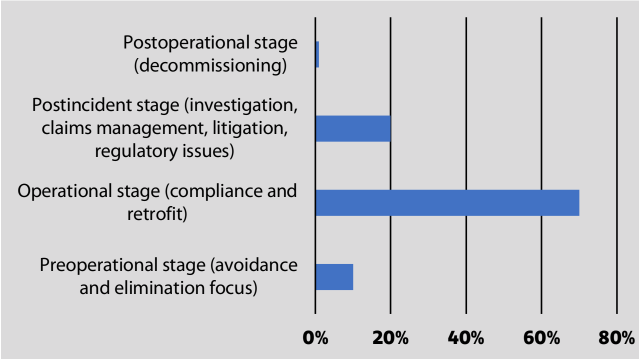
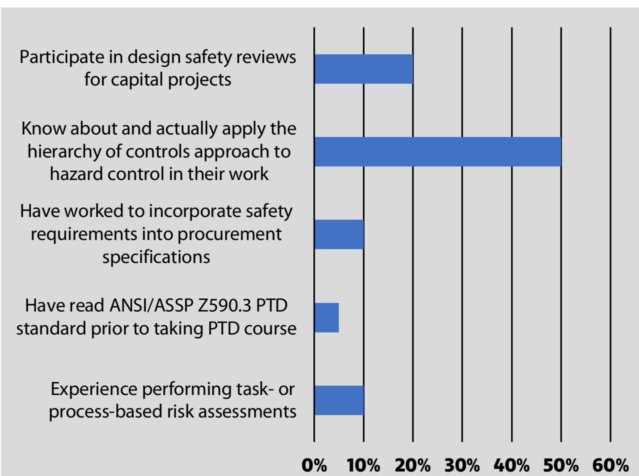


FIGURE 5

PERCENTAGE YES RESPONSES FROM COURSE PARTICIPANTS



SEVEN STEPS TO PTD

OSH practitioners can employ the following seven steps for improving PTD within their organizations.

1) Establish safety specifications and safety minimums for design, procurement and management of change.

2) Establish a protocol for performing risk assessment during the conceptual design and redesign phases. The protocol should require design safety to be addressed at the earliest possible point during the conceptual scoping and specification phase.

3) Establish a strong safety culture that requires acceptable risk levels be attained and maintained.

4) Explicitly communicate goals for achieving safe designs for all departments. Goals must be SMART (specific, measurable, attainable, relevant and time-based) with accountability. Expectations and accountabilities for safety in design must be clearly defined and communicated.

5) Enable, encourage and require effective communication regarding the design process among departments (horizontally) and within departments (vertically).

6) Provide/verify basic competency in hazard recognition, risk assessment, risk control options and PTD concepts for engineers, architects and designers. Decision-makers (senior management) should also have some basic knowledge of these concepts as well.

7) OSH professionals must become the subject-matter experts and lead the effort to bring PTD practices into organizations.

ties such as reviews of new systems/equipment, preplanning for construction or expansions, and process changes analyses. No mention of PTD, designing in safety or design safety reviews was found in any of the job descriptions.

This premise is supported by data collected by one of the authors. Figure 4 reflects data compiled from student training survey and feedback collected over a 5-year period from 2-day PTD training course attendees (Walline, 2014). Participants included more than 200 OSH professionals from a wide range of industries, varying sizes of organizations, nationally. The survey data was used to determine OSH professionals' time allocated to the four major stages of occupational risk management as outlined in Section 1.3 of ANSI/ASSP Z590.3.

Additionally, one of the authors collected responses from course participants while conducting PTD training for ASSP members over a 3-year period (Figure 5). Questions measured participants' knowledge of and experience with PTD concepts and functions.

The future OSH professional's job description must look much different than it does today. Progressive employers will want individuals who possess key competencies in PTD, risk assessment, higher level risk treatments and SIF prevention, to name a few.

Barriers to OSH professionals in the design and redesign phases are many. It is important to identify and understand these barriers so that OSH professionals can overcome such challenges (Popov, Lyon & Hollcroft, 2016).

Traditional Barriers

Organizational cultures and structures are highly compartmentalized (silo management) with a chain of command. Information does not typically flow from one department to another (horizontally) or above or below a particular manager (vertically). These interdepartmental barriers prevent collaboration.

The following scenario illustrates how individual department goals can conflict and impede interdepartmental communication and cooperation if no formal mechanisms or specific requirements to do so are in place.

•Engineering department: Designers and engineers develop designs according to design criteria including project objectives, cost, quality and performance within their department as expected by the organization. The engineering department's primary goal is to produce a design that works. There is no requirement to seek peer review by other departments concerning the design.

•Procurement department: Components and materials specified by the engineering department are provided to the procurement department. Typically, there are few specifications for safety, health, environmental or ergonomics requirements other than code compliance or regulatory requirements. The procurement department's goal is to acquire the necessary materials by the specified time, at the lowest cost possible (often within a specified budget). There are no requirements for peer review of materials selected by other departments.

•Supplier/contractor: The completed design is handed over to a third-party supplier/contractor responsible for building and installing the unit. There are few contractual requirements regarding safety and limited oversight by the facilities engineering/maintenance or production departments during the installation. The supplier/contractor's goal is to install and complete the unit according to design specifications within the required time frame and budget.

•Production department: Once installation is complete, the production department takes over operations. Operations may include pre-start-up inspections and procedures, programming, adjusting, lubricating, clearing jams, resetting machines and normal production operations. The production department's primary goal is to achieve and maintain maximum production (as measured by number of units produced), meeting quality standards at the lowest cost possible. There are no requirements for the production department to involve the OSH department until incidents or safety problems arise.

•Maintenance department: The operation requires regular scheduled preventive maintenance and occasional breakdown repair service performed by the maintenance department. The maintenance department's goals are to maintain equipment, perform repairs and return systems to normal as quickly as possible to reduce downtime and prevent business interruption. Outside of OSHA's lockout/tagout requirements, the organization does not require involvement from the OSH department until incidents occur.

•Maintenance/decommission contractor: At some point, the system or equipment completes its life span or usefulness. It is removed from service by maintenance or an outside contractor, making way for a new unit or technology to take its place. The OSH department has little involvement in decommissioning equipment except to respond to incidents that may occur during the process.

•OSH department: Throughout the life cycle of the system, exposure to hazards can cause harm to people, assets or the environment. The OSH department is responsible for identifying and controlling existing hazards, as well as responding to incidents that occur. For those systems and products that have not adequately addressed safety in the design, a greater number of control measures is required to achieve the organization's acceptable level of risk. Often, the primary goals of the OSH department are to meet compliance and reduce losses.

Training Barriers

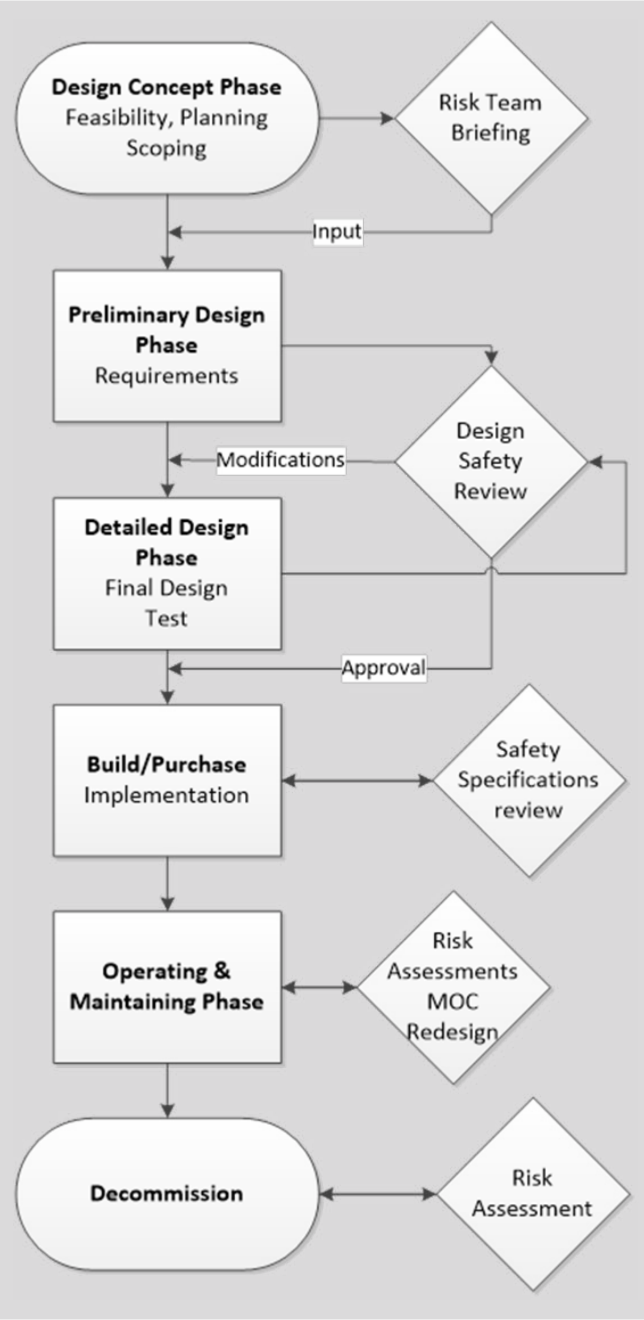
Formal education and training provided to engineers, architects and business professionals typically has not included basics in OSH principles and concepts. Many designers have little or no experience in hazard recognition, risk assessment or the concept of the hierarchy of controls. NIOSH's (2013) PTD program recognizes this deficiency and has prepared educational modules to help universities to integrate PTD principles into engineering curricula. OSH professionals need to improve their understanding of the design process, business objectives, cost drivers and internal protocols for engineering and design to be more effective in their organizations.

Turf Barriers

Architects and engineers are responsible for designing buildings, systems and products according to established design criteria, within set time and budget constraints, with the primary goal of designing things to work (Main, 2012). Engineers are not prone to deviate from their formal education and training or established protocols. As a result, they are reluctant to seek input from nonengineering departments. This presents an opportunity for OSH professionals to prove their value to designers and management by facilitating preoperational risk assessments that enable designs that are safer and more cost effective. The use of financial measures such as cost/benefit analysis and return on investment, as well as nonfinancial benefits, will aid in communicating the value of design safety reviews.

FIGURE 6

DESIGN SAFETY REVIEW PROCESS EXAMPLE



Time Barriers

Time is limited during the critical path from conceptual design to production. Tight schedules and deadlines coupled with lack of forethought or time allotted for safety reviews during design are common. OSH professionals should engage as early as possible, providing safety requirements to the design team. In some cases, risk assessments may require more time than allowed during a design review session. It may be necessary to perform the risk assessment separately, providing risk-based information to the design team during the conceptual stage.

FIGURE 7
DESIGN SAFETY REVIEW PROCESS

OSH practitioners largely have not engaged in the design process. Many reasons can be cited including job descriptions, daily work demands, lack of notification or invitation to participate in design reviews, position and status with an organization, and general lack of knowledge in the design and engineering process. This presents a great opportunity for OSH professionals to become change agents, advising in the safety requirements of new designs, and avoiding and eliminating hazards and risks. The "Seven Steps to PTD" sidebar (p. 28) outlines steps for improving PTD within organizations.

Design Safety Reviews

Codes and compliance reviews are common in fire protection-related designs, often conducted by third-party consultants and insurance representatives. However, designing to regulatory compliance does not ensure that all hazards are adequately controlled or that error traps are avoided (Lyon, 2016).

Design safety reviews are used to anticipate, identify and assess hazards during the design and redesign process of new facilities, expansions in existing buildings, new or modified processes and systems, equipment and machines, and products. The purpose of a design safety review is to avoid anticipated hazards in the design of a new system or redesign of an existing system.

Main (2012) recommends that design safety reviews be performed in the conceptual stage to provide designers specific safety guidance in the design. In simple designs, anticipated hazards can be identified by the team and addressed by designers. Where potential risk is high, design safety reviews may be needed at each stage (i.e., conceptual, preliminary, final design, testing) as a sign-off or approval process from the OSH, ergonomics and compliance stakeholders (Main).

Design safety reviews and assessments will vary in their degree of complexity depending on the context and the system being reviewed. Methods include:

- design safety checklists and guide words;
- preliminary hazard analyses;
- failure mode and effects analysis;
- what-if analyses and what-if/checklist analyses.

Design safety reviews are most effective when performed early in the design process while objectives are being discussed and should be considered in any major planned change. Design reviews typically include a compliance/codes review aspect. ANSI/ASSP Z590.3 states that the design safety review process is an effective means for achieving inherently safer designs and includes an informative addendum (Addendum E) on design safety reviews. Figure 6 (p. 29) presents an example showing the trigger points for risk assessments in the life cycle of a system.

The process should be systematically applied to all designs, changes in existing designs, and procurement and construction of new systems, and used to anticipate, identify, avoid, eliminate or control hazards. A commitment from management is required to fully integrate PTD concepts into the organization.

An established process for design safety reviews within the organization's operational risk management system should be implemented. The following model depicted in Figure 7 provides general steps for a design safety review process:

1) Design safety policy: A written management policy that provides direction on when, where and how hazard analyses and risk assessments are performed, including the design phase, should be established and communicated. Roles, responsibilities and accountabilities for design safety should be outlined to include engineers, designers, production, maintenance, quality, legal, OSH, human resources, procurement and other involved parties.

2) Design safety team: A qualified leader and cross-functional team to perform the design safety review should be selected. Design safety review team members should have expertise in applicable areas such as safety and health, ergonomics and human factors engineering, environmental safety, fire prevention and protection, and products liability prevention as appropriate for the project. In some cases, it may be necessary to include outside consultants or specialists to assist in the review. Effective communication should be maintained.

3) Method(s) selection: For each design, specific methods should be selected for conducting the design safety review based on the complexity of the project and the established context.

4) Design safety review: In the conceptual stages, a design safety review that includes hazard analysis and risk assessment should be initiated to identify hazards. ANSI/ASSP Z590.3 advises that design safety reviews should be performed as design objectives are being discussed. Depending on the project, the safety review can be performed separately, with the findings and risk reduction recommendations incorporated into the design process. Design safety reviews may include analysis of similar designs; plan drawings; specifications and limitations; hazard checklists; applicable standards; discussions with manufacturers of components and materials; safety data sheets; loss experience related to similar designs; and existing controls and technology on similar designs. The design safety review should address operational hazards as well as hazards resulting from nonroutine activities such as maintenance, emergency upsets and repairs, testing, adjusting, lubricating, and other related activities.

5) Deviations approval: Established safety standards and specifications should be followed. If a deviation from stated standards or specifications is requested, appropriate management personnel including OSH, legal or other parties must review the request and determine whether it is approved or denied.

6) Design completion sign-off: Upon completion, the project leader should sign off on the project to verify that the design safety review has been completed, signifying a consensus among the safety team and engineering group. Communication is needed between the design safety review team and engineering/design group throughout the process.

7) Action plan: The findings and recommendations from the completed design safety review may include modifications or markups of drawings; changes in specifications; a prioritized list of specific hazards and means for avoidance or control; a list of design modifications necessary prior to approval; action

FIGURE 8
PTD SELF-ASSESSMENT

No.	Description	Max points	Your organization
1	My design team members and I have read and understand the basic concepts and critical steps outlined in ANSI/ASSP Z590.3-2011(R2016) standard on prevention through design (PTD).	10	7
2	My design teams and I have access to and knowledge of the capital projects taking place within my organization.	10	5
3	My organization has established PTD business rules that trigger design safety reviews of projects.	10	7
4	My organizational leaders know the percentage of serious mishaps that have occurred in my organization related to design gaps.	10	3
5	My organization has created a design safety checklist based on lessons learned from past mishaps and incidents that have taken place within my organization or facility.	10	5
6	My organizational leaders understand that to reduce severity of harm (magnitude of energy/exposure) the organization must avoid risk, eliminate the hazard or seek to mitigate risk through substitution.	10	3
7	My organization insists that design safety reviews and risk assessments for capital projects are documented to an acceptable level of risk.	10	7
8	My organization captures and shares long-term burden costs with leaders and design teams related to poor design decision-making.	10	5
9	My design teams and I participate in documented pre-start-up safety reviews and commissioning activities with proper stakeholders to verify that all required established safe design criteria have been meet before releasing new or modified facilities, processes or equipment into operational mode.	10	3
10	My organization insists that proven solutions and cost-effective safe design criteria from completed capital projects are captured, shared and incorporated into future similar projects to reduce risk, cost and eliminate barriers to safe work.	10	3
	Point total	**100**	**48**

item list with assigned responsibilities; and follow-up questions, concerns or requests for additional information necessary to satisfy or complete the review and approve the design.

A PTD Success Story

The role of OSH professionals now and in the future is to affect positive change that reduces risk and resulting losses. An example of how this might look is presented in the following success story based on the authors' personal experiences. The names of the organization and the individuals involved have been substituted but the story is real.

Alpha Manufacturing, a privately held medium-sized company, operates six manufacturing facilities within the U.S. The company had experienced significant growth during a recent 4-year period. Two facilities were designed, built and put into operation within this business growth period to meet customer demand. In late 2014, Alpha Manufacturing recognized the need to add a second full-time OSH professional (safety specialist, and safety and health trainer) to support growth, meet business objectives and achieve an acceptable level of risk. The primary job of the new safety position was to help manage the rising frequency and costs of occupational incidents in the company's operations and support the organization's objectives.

As a result, Jane was hired in early 2015 as the new OSH business leader. During her first week, she discovered startling statistics surrounding design-related causal factors and their association with workplace incidents. A large number of serious and even fatality-level risks seemed to have contributing factors linked to design issues in the facilities and processes.

Jane prepared a report for senior management on her findings. The report showed that several serious incidents were directly or indirectly connected to design-related factors. Specific examples, pictures and diagrams were included to help visualize some of the concerns. In addition, she identified the annual costs to the organization for existing engineering, administrative and PPE controls required to manage the risks. Management was intrigued and asked her to make a short presentation to the management team. Jane prepared handouts with graphics, photos, cost-benefit analyses and a brief summary of the report. A compelling case was made that the company was spending more than $1 million to implement, maintain and monitor these control programs. Anticipating management's questions, she followed up with a recommended action plan starting with a company self-assessment in design safety. Management agreed, and as a result she prepared a PTD self-assessment checklist (Figure 8) to establish a baseline and determine areas that could be improved.

Step 1: Plan & Prepare

Jane obtained a copy of ANSI/ASSP Z590.3. She immersed herself particularly in the sections of the standard around:

FIGURE 9
DESIGN SAFETY REVIEW CHECKLIST

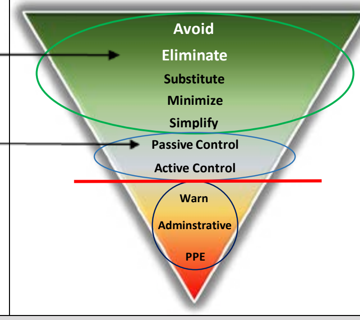
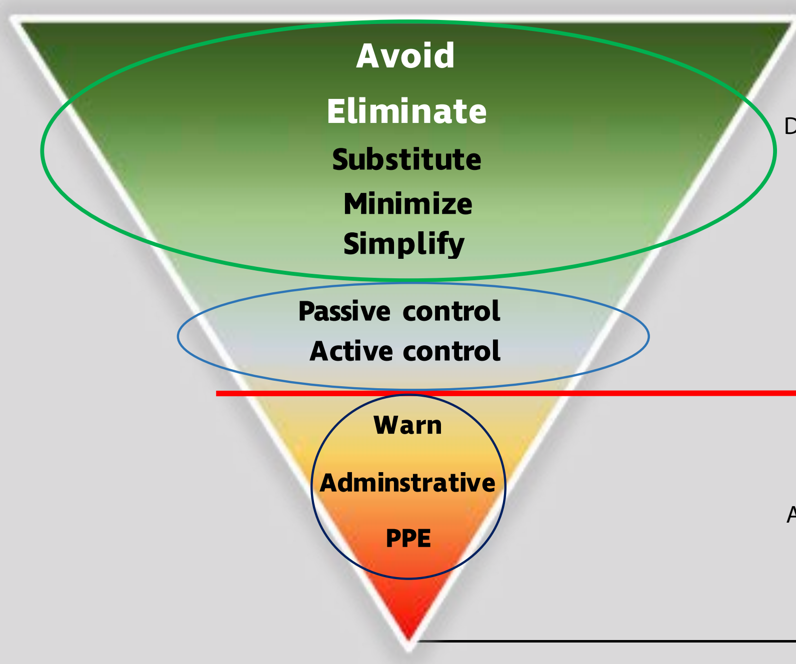
Hazard category Pathway to harm	Case no. Incident description	Year	Work condition Normal or abnormal	Severity potential	Design specification	Hierarchy of risk treatment
Powered machinery and equipment (hot roll machine) In-running nip point Caught in/between	(377042) Employee hand caught between hot power rolls (150 °F) and fixed guides while adjusting feed. Multiple fingers amputated, second-degree burns to right hand.	2012	Abnormal (facing sheet was not adhering to product)	Life altering	1) Redesign machine with guides to keep product in line with rolls to avoid employee interface with material. 2) Install fixed guarding to prevent worker access to machine hazard zone with equipment powered up.	

FIGURE 10
HIERARCHY OF RISK TREATMENT MODEL



	Effectiveness and reliability	Compliance burden
Design and redesign	Complete	None
	Very high	Low
Engineer	High	Limited
Adminster	Moderate	Moderate
	Limited	High
	Very low	Very high

TABLE 3
HAZARD CATEGORY: POWERED MACHINERY & EQUIPMENT EXAMPLE

No.	Performance objective	Hazard (energy source)	Above-the-line control
1	No exposure to hazardous energy	Electrical, air, mechanical	Energy isolation at point of need (engineering)
2	Fixed barrier guards	Mechanical	Engineering
3	No exposure to electrical energy	480 V AC	Diagnostic ports, energy isolation devices, protective covers (engineering)
4	No hearing protection	< 80 dBA, 8-hour TWA	Avoidance
5	No machine tip over	Gravity	Engineering, machines anchored
6	No portable ladders	Elevated work, gravity	Work performed at ground level, fixed stairways and platforms with protective railings (avoidance and engineering)

FIGURE 11

TASK-BASED RISK ASSESSMENT WORKSHEET EXAMPLE

Task-Based Risk Assessment Worksheet: New Line 22—Powered Conveyor System

Design performance objective: No uncontrolled exposure to conveyor hazards
Design (residual risk) target: No SIF mishaps
See ANSI/ASSP Z590.3, Addendum F, Table 2

No.	Conveyor task exposure	Hazard	Severity	Probability	Risk	Design specification	Proven solutions	Residual risk
1	Adjust air pressure at receiver station	Fall to level below: 12 ft	5	5	**25**	Air receiver tank and controls at floor level	**Elimination:** Acoustical treated sound enclosure at floor level, no elevated work	**1**
2	Manually upload parts on conveyor at feed station	Restricted work space: crushing by forklift	5	5	**25**	Automated product feed system	**Elimination:** Forklift product feed station, removal of exposure	**1**
3	Clear jam at chopper station	Mechanical energy: cutting, chopping	5	5	**25**	Jam clearing device	**Elimination**: Automated jam clearing system at chopper station, removal of exposure	**1**

- design safety reviews (Section 6);
- hazard analysis and risk assessment process (Section 7);
- hazard analysis and risk assessment techniques (Section 8);
- hierarchy of controls (Section 9);
- the corresponding addendums.

She summarized an action plan based on the PTD standard and presented it to management. The plan was to form a design safety team, create design safety criteria and specifications based on available data, develop a design safety checklist, implement a design safety review protocol, and track progress. With management approval, she initiated the plan.

Step 2: Form Team

With this newfound knowledge and understanding, Jane identified the capital project leaders, design partners and suppliers for the corresponding projects that her organization was planning to engage with over the next few years. Jane trained her teams on the key concepts and critical steps outlined in the PTD standard and her newly crafted PTD self-assessment checklist elements. This became her PTD implementation strategy. Jane's effort was aligned with the following sections of the PTD standard:

- Section 4, roles and responsibilities;
- Section 5, relationship with suppliers.

Step 3: Establish Parameters

To clearly establish with all stakeholders the PTD business rules, Jane created a list of trigger events to ensure that all risk-based design safety review requirements would be fulfilled for all projects going forward. The triggers for risk assessment were:

- new facilities, equipment and machinery;
- regulatory driven;
- customer expectations, new products;
- redesigns and modifications;
- company injury claims and loss history;
- Kaizen and lean manufacturing events relating to design/redesign;
- relocated equipment and processes;
- highly complex processes;
- demolition, decommissioning.

Step 4: Analyze Data

During the first 3 months, Jane compiled and reviewed data from Alpha's injury/illness and workers' compensation claim report database, near-hit reports and associated incident investigation reports. Her review focused on gaps in current operation designs and processes. She reviewed in detail some 200 injury/illness cases and serious near-hit reports from a 4-year period and identified the following critical information:

- 37% of OSHA recordable injury cases identified a primary causal factor related to gaps in design of equipment, machinery and process.
- 21% of the total recordable injuries had potential to be a SIF event.
- Of the cases that had SIF potential, 42% were linked to gaps in design of equipment, machinery or process.

When Jane shared these facts with company leadership and project delivery teams, the information was shocking to them but it reinforced the importance of designing for safety and health. Management encouraged her to proceed.

Step 5: Develop Design Checklist

From her incident analysis and findings, Jane established a set of safety performance objectives for all capital projects. The safety performance objectives are the outcomes to be seen at the completion of the design and install. These safety performance objectives are hazard and exposure avoidance based. The design safety performance specifications were:

•no portable ladders (step and extension types);
•no open chemical systems;
•no manual handling or lifting of products greater than 15 lb in production cycle;
•no chemicals/materials to be used as noted on organization's material of concern list;
•no elevated work without protective guardrails;
•no sharp edges;
•no energized work;
•no exposure to energized parts, including diagnostics;
•energy isolation devices for lock-tag-try at ground or floor level and at point of need;
•no respirator-required tasks;
•no exposure to noise levels above 80 dBA for an 8-hour time-weighted average;
•no pedestrians in warehouse while forklift traffic present.

The information collected by Jane was incorporated into a company-specific design safety review checklist that offered design solutions to prevent future mishaps. The design safety review checklist included hazard category, incident description, year, whether it was a normal or abnormal condition, severity potential and design specifications linked to the hierarchy of risk treatment (Figure 9, p. 32). The checklist was then used in every design safety review for capital projects.

Step 6: Use of Higher Level Controls

Jane established strong linkage between PTD and control effectiveness. All the cases she studied with a causal factor related to design could have been prevented with what she called an "above the line control" solution. To reduce energy levels and severity of harm potential, particularly with SIF risks, avoidance/elimination, substitution, minimization, simplification and engineering controls were to be the primary controls used. This was a new stake in the ground that Jane established for her organization and engineering/design partners for assessing and controlling design risk going forward. Jane was establishing for the organization, an acceptable level of risk (ALOR) for all designs and projects by designing above the line. Any exception to this rule would require documented verification from her that above the line control was not feasible. Alternative feasible controls that would reduce risk as low as reasonably practicable (ALARP) would be required in any case.

Jane developed a training module that she shared throughout the organization and with external design partners to educate them on her findings and approach to risk reduction in the design phase of projects. The title of her presentation was "PTD: Design Above the Line." The cornerstone of her message was the hierarchy of risk treatment model (Figure 10, p. 32) with risk reduction strategy options, effectiveness levels and ongoing cost burdens.

Jane established and communicated two PTD business rules for design safety with the design team:

1) All hazards identified must be adequately addressed using above the line controls to reduce risk to an acceptable level.

2) Any exception to this business rule must undergo OSH professional review and approval.

Step 7: Establish & Implement Process

Jane established the expectation that company safety resources would participate in the design safety review of all capital projects, new designs, redesigns, procurement of new equipment, materials and chemicals, and in the management of change (MOC) process. Such reviews would be documented. The same expectation would be set for employee participation in design safety reviews. As part of the design safety review process, a documented risk assessment would be conducted with all appropriate parties. Design safety reviews would include hazard category checklists and documented task or process-based risk assessments (Table 3, p. 32; Figure 11, p. 33). These tools were created over time by Jane and the other company safety resources.

Step 8: Document & Communicate Results

To communicate to management the many benefits derived from PTD and design safety risk management, Jane captured the ongoing burden costs from managing risk below the line. She wanted leaders to understand that selecting low-level controls (e.g., procedures, signs, training, PPE) to manage high-level risks comes with a long-term cost that would add up to millions of dollars over the life expectancy of major capital projects. The company advised staff that these two new manufacturing facilities each have an expected life span of 50 years. Jane's approach was to avoid and reduce burden costs associated with managing design-embedded problems by incorporating safety into the design process. As a result, she presented management with an ongoing burden

TABLE 4
ONGOING BURDEN COSTS

People-related costs	Equipment-related costs	Methods-related costs
Training	Purchase	Scheduling and planning
Buddy systems	Rental	Written program
PPE	Repair and maintain	Safe work procedures
Supervision	Clean	Audits/inspection
Injuries	Retrofit	Permits
Claims	Storage	Observations
Citations and penalties	Transport device	Investigations

FIGURE 12
PTD TRACKING SHEET EXAMPLE

PTD milestone	OSH professional (approval)	Affected workers (approval)
Final design review approval	X	X
Vendor trial(s) approval (as required)	X	X
Pre-start-up safety reviews and commissioning approval	X	X
ALOR documented	X	X
Final open punch list items to achieve ALOR completed	X	X

costs table identifying some of the operating costs an organization must fund and manage annually for most compliance-based programs (Table 4).

Step 9: Monitor & Refine

As part of the safe design verification process, Jane helped establish a PTD business rule declaring that adequate safety resources and affected workers would be involved in final design approvals, vendor trials, pre-start-up safety reviews and commissioning activities for the purpose of achieving an ALOR. In addition, the completion of these activities and resources would be verified and documented in a PTD tracking sheet (Figure 12).

Step 10: Communicate

Jane established a SharePoint site for her organization where risk reduction solutions (proven solutions) and cost-effective design criteria would be posted and shared. Workers often identified proven above the line controls that would achieve ALOR and remove burden costs from the operation or design. A big part of the proven solutions centered around fail-safe design, and error tolerant designs and processes. These proven solutions were then referenced for future projects to expedite PTD process to achieve ALOR.

OSH professionals who participate in the design safety process and PTD efforts should take credit for the benefits derived from a successful completed project. An organization's value creation and protection as well as achievement of business objectives at an acceptable risk level, improved quality and production, employee and stakeholder satisfaction, and cost savings are all ultimately derived from successful safety through design efforts.

Conclusion

The pace of risk reduction and prevention improvement is directly linked to the speed of change led by OSH professionals in PTD. Risk assessment and safety in design must be at the forefront of the OSH professional domain. Specifically, OSH professionals must 1) become subject matter experts and leaders in PTD; 2) define safety specifications for designers to incorporate into their designs; 3) help define acceptable risk levels; 4) be active in the design process, design safety reviews, MOC and procurement; and 5) implement higher-level risk reduction strategies to avoid, eliminate and reduce risks throughout the life cycle of systems.

As a key stakeholder of a design team, the OSH professional has the responsibility, creativity and power to cause injury-free lives around the world. This must be our legacy. The benefits are many and the OSH profession must be viewed as creating value. OSH professionals must be the agents for change. If not us, then who? **PSJ**

ACTION STEPS

As a key stakeholder of a design team, the OSH professional must be an agent for change.

1) Learn. Read, understand and embrace the Z590.3 standard and share its value and benefits with key stakeholders.

2) Practice. Gain knowledge and experience in risk assessment, safe design criteria and the design process in your organization.

3) Engage. Break out of the comfort zone and engage in the workplace design process. Don't wait for an invitation.

4) Communicate. Share successes, learnings and value of safety design initiatives across the organization.

5) Influence. Become a trusted agent for change in your organization among designers and decision-makers.

References

ANSI/ASSP. (2011). Risk assessment techniques (National adoption of ISO/IEC 31010:2009) (ANSI/ASSP Z690.3-2011). Park Ridge, IL: ASSP.

ANSI/ASSP. (2016). Prevention through design: Guidelines for addressing occupational hazards and risks in design and redesign processes [ANSI/ASSP Z590.3-2011 (R2016)]. Park Ridge, IL: ASSP.

ANSI/ASSP/ISO. (2018). Risk management: Guidelines (ANSI/ASSP/ISO 31000-2018). Park Ridge, IL: ASSP.

Behm, M. (2005). Linking construction fatalities to the design for construction safety concept. *Safety Science, 43*(8), 589-611. doi:10.1016/j.ssci.2005.04.002

Howard, J. (2008). Prevention through design: Introduction. *Journal of Safety Research, 39*(2), 113.

Lyon, B.K. & Popov, G. (2018). *Risk management tools for safety professionals*. Park Ridge, IL: ASSP.

Main, B.W. (2012). *Risk assessment: Challenges and opportunities*. Ann Arbor, MI: Design Safety Engineering.

Manuele, F.A. (2014). *Advanced safety management: Focusing on Z10 and serious injury prevention* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Morgenthaler, T. & Harper, C.M. (2015, Oct. 20). Getting rid of "never events" in hospitals. *Harvard Business Review*. Retrieved from https://hbr.org/2015/10/getting-rid-of-never-events-in-hospitals

NIOSH. (2013). Prevention through design. Retrieved from www.cdc.gov/niosh/programs/ptdesign/pubs.html

Popov, G., Lyon, B.K. & Hollcroft, B. (2016). *Risk assessment: A practical guide to assessing operational risks*. Hoboken, NJ: John Wiley & Sons.

Safe Work Australia. (2014). Work-related fatalities associated with unsafe design of machinery, plant and powered tools, 2006-2011. Retrieved from www.safeworkaustralia.gov.au/system/files/documents/1702/work-related-fatalities-unsafe-design.pdf

Shorrock, S. (2016, Feb. 27). Never/zero thinking. Humanistic Systems. Retrieved from https://humanisticsystems.com/2016/02/27/never zero-thinking

Stephans, R.A. (2004). *System safety for the 21st century: The updated and revised edition of system safety 2000*. Hoboken, NJ: John Wiley & Sons.

Walline, D.L. (2014, Nov.). Prevention through design: Proven solutions from the field. *Professional Safety, 59*(11), 43-49.

Bruce K. Lyon, P.E., CSP, ARM, CHMM, is vice president with Hays Cos. He is a board member of BCSP, advisory board chair to University of Central Missouri's (UCM) Safety Sciences program, and vice chair of the ISO 31000 U.S. TAG. Lyon is coauthor of *Risk Management Tools for Safety Professionals* and *Risk Assessment: A Practical Guide to Assessing Operational Risk*. He holds an M.S. in Occupational Safety Management and a B.S. in Industrial Safety from UCM. Lyon is a professional member of ASSP's Heart of America Chapter, and a member of the Society's Ergonomics and Risk Management/Insurance practice specialties.

David L. Walline, CSP, is president of Walline Consulting Ltd., which he formed after spending 42 years in global safety leadership roles with Owens Corning and General Dynamics Corp. He is former chair of the ASSP's Risk Assessment Committee and Risk Assessment Institute. He served on the review committee for ANSI/ASSP Z590.3-2011, the prevention through design standard. Walline is a professional member of the Society's Gold Coast Chapter.

Georgi Popov, Ph.D., CSP, ASP, SMS, ARM, QEP, CMC, is a professor in the School of Geoscience, Physics and Safety Sciences at UCM. He is coauthor of *Risk Assessment: A Practical Guide for Assessing Operational Risk* and *Risk Management Tools for Safety Professionals*. Popov holds a Ph.D. from the National Scientific Board, an M.S. in Nuclear Physics from Defense University in Bulgaria, and a post-graduate certification in environmental air quality. He graduated from the U.S. Army Command and General Staff College in Fort Leavenworth, KS. Popov is a professional member of ASSP's Heart of America Chapter and a member of the Society's Risk Management/Insurance Practice Specialty.