Managing Risk Through LAYERS OF CONTROL

By Bruce K. Lyon and Georgi Popov

FROM ANCIENT TIMES, the concept of using multiple lines of defense or layers of protection was practiced to survive. During the Byzantine Empire, cities and castles were fortified by trenches, moats, multiple stone walls built 30 ft wide and 30 ft high or higher, tall towers equipped with archers and drawbridge-gated entrances, all to provide layers of protection against outside forces. The walls of Constantinople were the most famous of the medieval world, not only due to the scale of the layers of defense, but also due to their construction and design. These lines of defense were constantly challenged and tested by would-be invaders and required continual improvement of defense weaknesses, learning from failures and breaches. However, even the best layers of defense are vulnerable. Ultimately, the walls of Constantinople were breached by an emerging risk of the time: gunpowder and cannon fire. When the Ottoman sultan acquired cannons, the walls of Constantinople were rendered obsolete. On May 29, 1453, the Gate of St. Romanus was destroyed by artillery, the garrison of the Circus Gate was seized, and the Fifth Military Gate was stormed by the Turks. The city was finally captured (Livius.org, 2020). Today, organizations face similar battles from an operational risk standpoint.

KEY TAKEAWAYS

- **The concept of protecting people and assets with layers of controls, both preventive and mitigative, is an important aspect of reducing and managing operational risk.**
- **Rarely is one control adequate in reducing and maintaining risk to a level that is considered acceptable. Layers of control selected in accordance with the hierarchy of risk treatment and their actions should be constructed, implemented, verified and monitored to achieve a level that is as low as reasonably practicable (ALARP).**
- **Techniques such as barrier analysis, layers of protection analysis, bow-tie analysis and modified methods such as layers of control assessment can be used to assess existing controls and determine whether risk is at an acceptable level or whether further risk reduction strategies are necessary to achieve and maintain ALARP.**

THEERAPONG28/ISTOCK/GETTY IMAGES PLUS

The concept of employing multiple lines of defense is used today in military strategies, cybersecurity of information technology, and in high-reliability type organizations such as the nuclear power industry and chemical processing. Seldom does a single risk control measure suffice in providing the sustainable risk reduction required or desired. Since the 1960s, the nuclear and petrochemical industries have made use of the concept of layering protection to prevent and reduce operational risk in their facilities.

Traditional safety practices have often taken a more singular view of controlling known hazards. The reliance upon a single machine guard or employee safety training comes to mind. However, what if the control fails or is inadequate or circumvented? Are redundancies, backup controls or additional layers of control in place to prevent the failure from occurring, and mitigative measures to reduce its severity of harm?

Risk Treatment Strategies

In the OSH profession, several terms are commonly used, sometimes interchangeably, in association with reducing risk: prevention, protection, mitigation and control. As each is a risk reduction strategy, each term has a specific meaning and place in a risk treatment plan. Following are descriptions and examples of these risk treatment terms.

Prevention. According to a standard dictionary, to prevent is to keep from happening or existing; to hold or keep back; to hinder or stop. In business, prevention is an action taken to reduce or eliminate the probability of specific undesirable events from happening and is described as generally less costly than mitigating the effects of negative events after they occur (WebFinance, 2020). ANSI/ASSP Z590.3, Prevention Through Design (PTD), Section 9, Hierarchy of Controls, states that the first four control levels of the hierarchy are more effective because they are preventive actions that eliminate or reduce risk by design, elimination, substitution and engineering measures. An example of a preventive measure

FIGURE 1
BOW-TIE ANALYSIS DIAGRAM

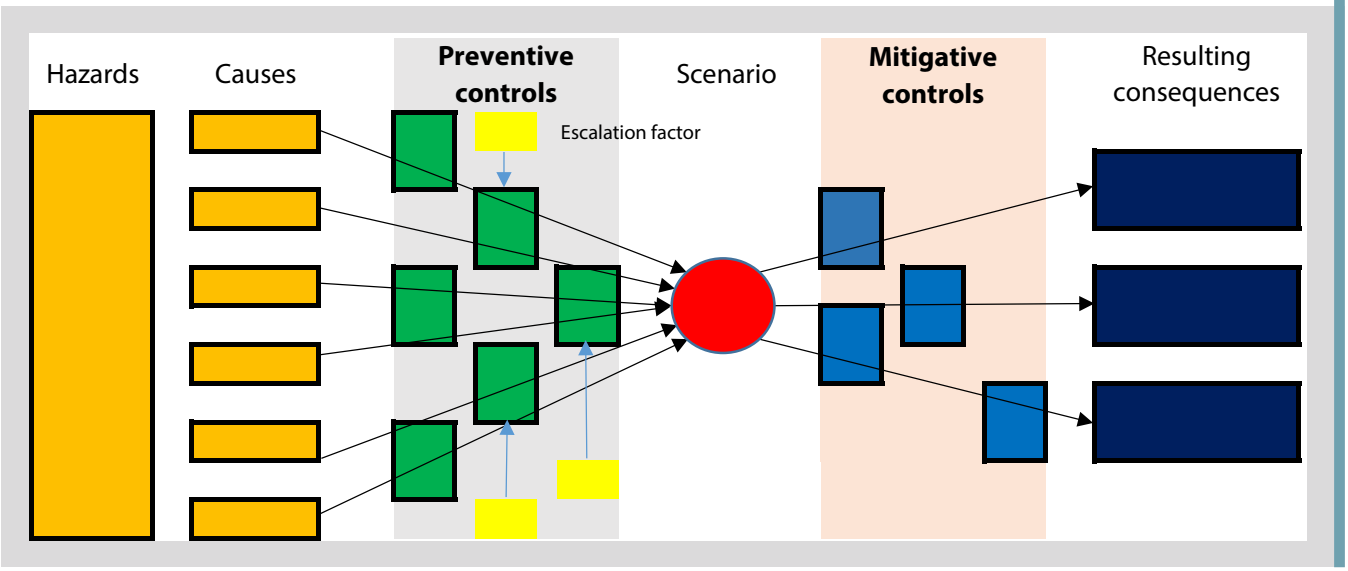
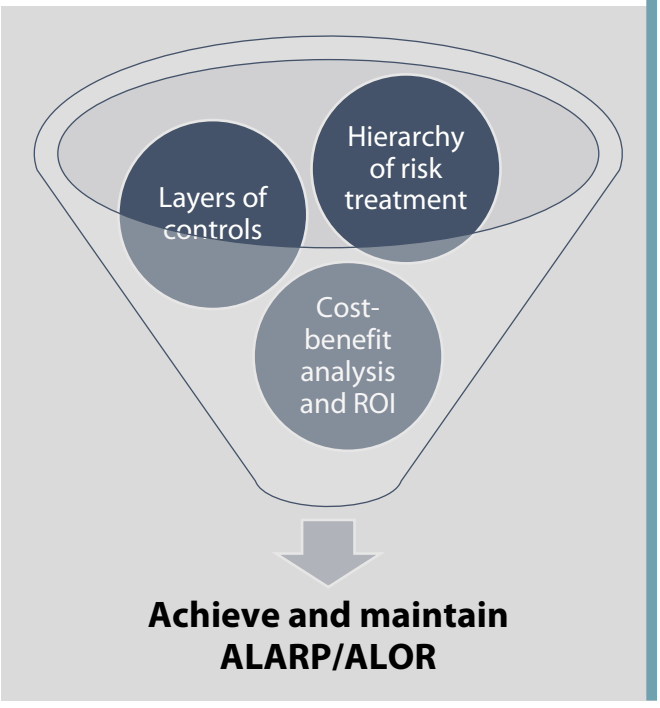


FIGURE 2
CONSTRUCTING RISK TREATMENT PLANS TO ACHIEVE ACCEPTABLE RISK



is a pressure-relief valve on an enclosed tank designed to prevent over-pressurization and explosion.

Protection. Protective measures are designed to reduce the severity of consequences by shielding, covering or isolating an asset from harm. To protect is to cover or shield from exposure, injury, damage or destruction; to guard; to maintain the status or integrity of, especially through financial or legal guarantees. Protection measures are generally put in place before an occurrence to protect assets during an incident and to limit damage or impact. Examples of protection include automatic fire suppression systems in buildings, cathodic protection for an underground storage tank and PPE. Insurance (or risk transfer) could also be considered a form of protection measure for the insured parties or properties.

Mitigation. Like protection, mitigation is used to reduce the severity or seriousness of something, thus making a condition or consequence less severe. To mitigate is to make less severe or painful. Federal Emergency Management Agency (FEMA, 2017) defines mitigation as "the effort to reduce loss of life and property by lessening the impact of disasters." Mitigative measures generally are reactive efforts, procedures or actions taken immediately following an incident such as an emergency action plan.

Control. Control is a more encompassing term that is used to reduce the incidence or severity of, especially to innocuous levels. ISO Guide 73 defines control as "a measure that modifies risk and may include processes, policies, devices, practices or other actions" (ANSI/ASSP, 2011).

A comprehensive approach to reducing and maintaining risk at an acceptable level often requires layers of controls: a combination of preventive, protective, mitigative and control measures (Lyon & Popov, 2016; 2019). The various measures for prevention and mitigation of major incidents may be thought of as lines of defense or layers of protection. These layers serve to prevent an initiating event from developing into an incident (e.g., release of a hazardous substance), and to mitigate the consequences of an incident once it occurs (Franks, 2017).

An example can be given in a bow-tie analysis diagram (Figure 1), which identifies the preventive measures on the left side of the bow tie (barriers positioned between the hazard-causes and the event) and the mitigation measures on the right side of the bow tie (reactive measures between the hazardous event and the consequences). Both preventive and mitigative measures are risk reduction treatment strategies (Lyon & Popov, 2019).

To achieve and maintain an acceptable level of risk, OSH professionals must be proficient and practiced in the selection, implementation and verification of risk treatment plans. Such

plans should be constructed according to the following practices (Figure 2):

- use of the hierarchy of risk treatment and higher-level controls;
- layers of controls and redundancies;
- cost-benefit analysis and return on investment justification;
- testing and verifying effectiveness and reliability.

Hierarchy of Risk Treatment

The objective of occupational risk management is to achieve and maintain an acceptable level of risk (ALOR), a risk level that is as low as reasonably practicable (ALARP). The use of a hierarchical system for selecting risk reduction strategies is a fundamental concept in safety management. Many models are available including those from ANSI/ASSP Z590.3, ANSI/ASSP Z10.0, NIOSH, ANSI B11 and American Institute of Chemical Engineers (AIChE). In most models, the first choices are risk avoidance and risk elimination. Where the risk cannot be avoided or eliminated, substitution and minimization measures to reduce severity should be considered. Risk reduction by lowering likelihood of occurrence through simplification and passive safeguards are the next options. From an enterprise risk management standpoint, additional risk treatment options include:

- separation of risks to minimize the adverse effect of a single loss;
- duplication of critical systems or use of backups;
- diversification of risk to spread exposure over many areas rather than one concentrated area;
- risk financing (insurance, hedging or self-funding);
- risk transfer (hiring third parties, contracts);
- risk retention (determined acceptable to the organization in its present state);
- risk exploitation (speculative risks, opportunities, potential gains).

The concept of inherently safer design control measures can be found in the AIChE steps for managing chemical and process hazards and risks. An interpretation of AIChE's hierarchy is presented in Table 1 (CCPE, 2008).

The hierarchy of risk treatment (HORT) in Figure 3 (Lyon & Popov, 2019) combines the hierarchy from ANSI/ASSP Z590.3 (PTD standard) with concepts from inherently safer design controls used in the chemical process industry. These models all share a common theme that the strategies at the top, the higher-level controls, should always be considered/selected first.

Risk Treatment Plans

Risk treatment is a continuous process that involves the formulation and selection of a treatment plan, its implementation and evaluation of the residual risk level to determine whether it is acceptable or whether further treatment is required. A risk treatment plan can involve a single control; however, it more likely requires multiple risk reduction measures to accomplish the desired risk reduction. Risk reduction concepts such as inherently safe design, layers of protection, recognized and generally accepted good engineering practices, and safer technology and alternatives, along with the hierarchy of controls should be incorporated into the risk treatment plan (Lyon & Popov, 2018).

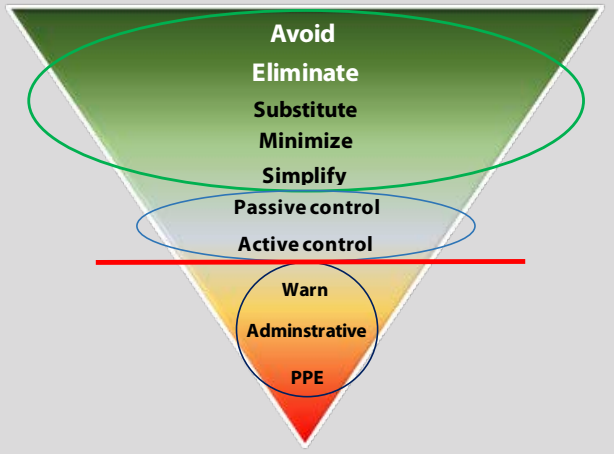
As outlined in ISO 31000, risk treatment options available include the decision to avoid the risk by choosing to not engage in the activity or exposure; eliminating the risk by removing the risk source; reducing the likelihood or reducing the severity; sharing the risk among other parties such as contracts and risk financing; and retaining the risk such as self-funding or other risk-based decisions (ANSI/ASSP/ISO, 2018; Lyon & Popov, 2018).

TABLE 1
HIERARCHY OF CHEMICAL PROCESS CONTROLS

1st order	Inherent safety measures	Avoid or eliminate hazard
2nd order	Inherent safety measures	Reduce severity potential of hazard
		Reduce likelihood of exposure
Layers of protection	Passive safeguards	Reduce likelihood or severity of hazard with controls that do not require activation
	Active safeguards	Reduce likelihood or severity of hazard with controls that detect and respond or activate to external input
	Procedural safeguards	Reduce likelihood of exposure through operating procedures and administrative measures that rely on the human element to respond or perform

Note. Adapted from *Inherently Safer Chemical Processes: A Life Cycle Approach* (2nd ed.), by Center for Chemical Process Safety, 2008, Hoboken, NJ: Wiley.

FIGURE 3
HIERARCHY OF RISK TREATMENT



Once treatments or controls have been implemented, it is critical to assess their effectiveness and reliability. Testing and verification of control reliability and effectiveness ensuring that controls are working as expected should be performed and documented. As part of the testing of controls, it should be determined whether any unintended consequences or new hazards are created.

The Concept of Layers of Control

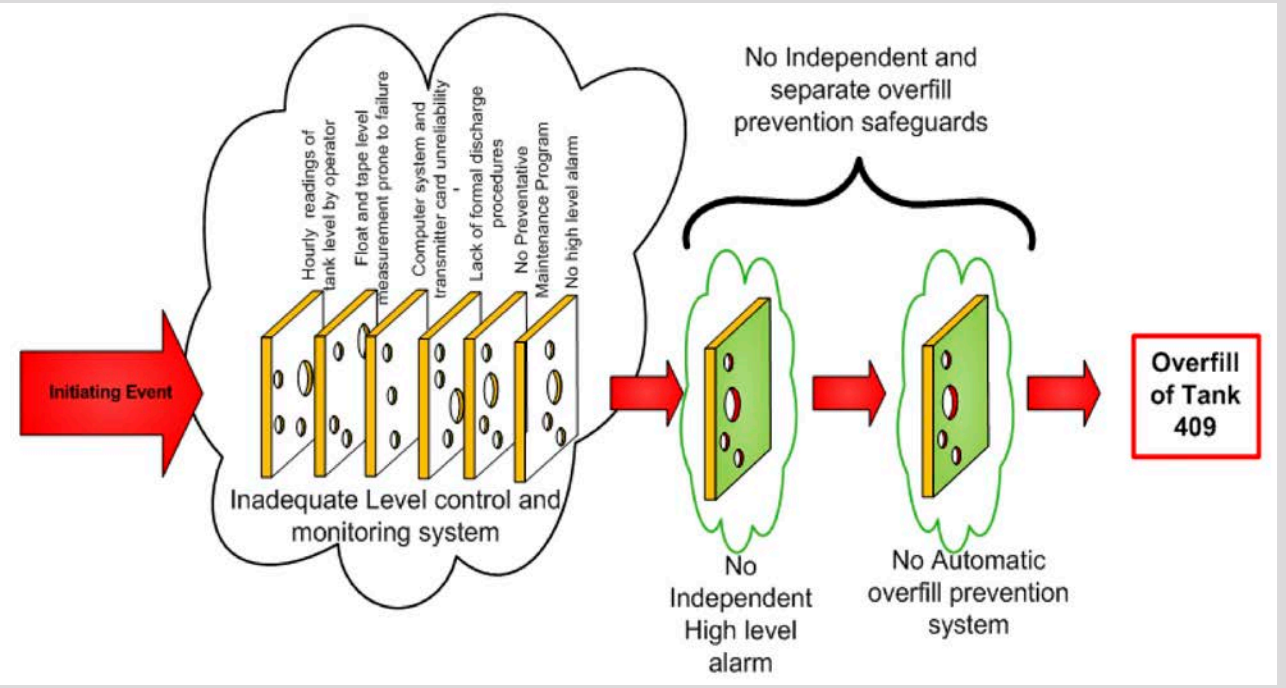
The terms *layers of protection*, *lines of defense* and *depth in defenses* are adopted from military strategy using multiple layers of defense to withstand an attack and maintain defenses through the use of layers that resist rapid penetration, slow the attack, fortify around critical elements and yield rather than exhaust themselves.

American Petroleum Institute (API) standards provide the following definitions of the layers of protection concept:

> A concept of providing multiple independent and overlapping layers of protection in depth. For security purposes, this may include various layers of protection such as countersurveillance, counterintelligence,

FIGURE 4

SWISS CHEESE DIAGRAM FROM CSB REPORT ON CAPECO INCIDENT



Note. Reprinted from "Final Investigation Report: Caribbean Petroleum Tank Terminal Explosion and Multiple Tank Fires (Report No. 2010.02.I.PR)," by CSB, 2015.

> physical security and cybersecurity. A second consideration is the balance of the security measures such that equivalent risk exists regardless of the threat's pathway or method. (API, 2016)
>
> A concept whereby several independent devices, systems or actions are provided to reduce the likelihood and severity of an undesirable event. (API, 2013)

In industries such as chemical processing, layers of protection are constructed with independent protection layers (IPLs). An IPL is defined as a device, system or action capable of preventing an event or exposure from occurring that is independent of other controls and is verifiable or auditable for effectiveness (Rausand, 2011). As described by the aforementioned API standards, IPLs are considered physical barriers or devices, typically engineering controls, that prevent the initiating cause of an event from proceeding to an unwanted consequence. Administrative controls such as inspections, training, standard operating procedures and PPE are not considered barriers and, therefore, are not included in a typical layers-of-protection analysis (LOPA).

The Swiss cheese model made famous by Reason (2016) illustrates the concept of using layers of protection. Reason states that all workplace incidents have at least three common features: 1) hazards; 2) failed defenses; and 3) losses. Of these three features, failed defenses offer the greatest potential for risk reduction improvement. This is an important observation. Controls can exist at many levels and take various forms. However, each control serves one or more of the following functions: to create understanding and awareness of the hazards; to give guidance on how to operate safely; to provide alarms and warnings when danger is imminent; to place barriers between the hazards and the potential losses; to restore the system to a safe state after an event; to contain and eliminate the hazards should they escape the barriers and controls; and to provide the means of escape and rescue should the defenses fail catastrophically (Reason, 2016).

Reason's defenses-in-depth concept can be effective in making complex technological systems such as nuclear power plants largely protected from single-point failures. But, as he points out, no defense is perfect. Controls can contain weaknesses, flaws and gaps such as holes in Swiss cheese slices. Under certain conditions, these holes or weaknesses can line up, allowing an incident to occur, as illustrated by the Swiss cheese model (Reason, 2016).

Case Study No. 1: Petroleum Tank Terminal Explosion & Fires

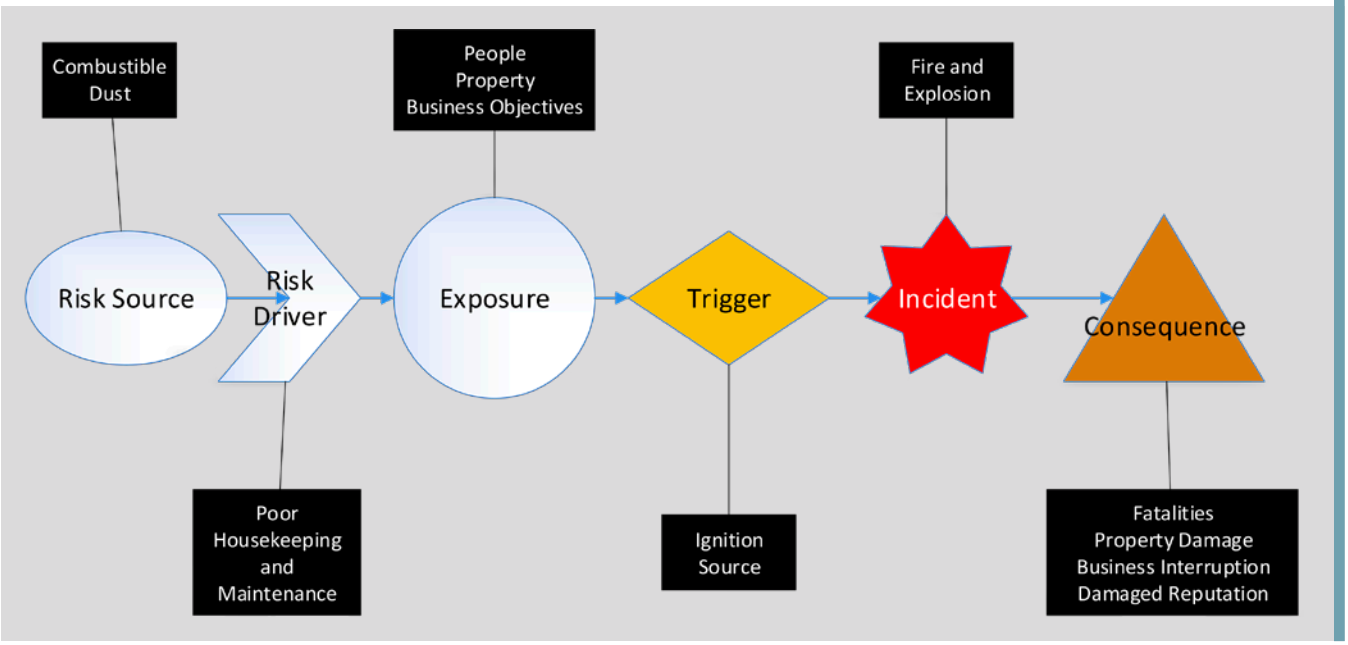
An example of the Swiss cheese model demonstrating layers of protection can be found in the CSB (2015) final investigation report on the Caribbean Petroleum Corp. (CAPECO) tank terminal explosion and tank fires. The following statement and Swiss cheese diagram in Figure 4 are from the report:

> The CSB determined that numerous technical and systemic failures contributed to the explosion and multiple tank fires at the CAPECO tank terminal. The CSB found that multiple layers of protection failed within the level control and monitoring system at the same time. In addition, a lack of independent safeguards contributed to the overfill. James Reason's Swiss cheese model best demonstrates these systemic failures that led to the accident. Reason postulates that an accident results from the breakdown of the "interaction between latent failures and a variety of local triggering events (active failures)" and although rare, the "adverse conjunction of several causal factors" from various layers. The deficiencies or holes at each layer of protection are constantly increasing or decreasing based on management decisions and operational deviations. (CSB, 2015)

Case Study No. 2: Metal Dust Explosion & Fire

The following scenario is excerpted from the metal dust explosion and fire at the AL Solutions facility in New Cumber-

FIGURE 5
RISK PATHWAY OF A DUST EXPLOSION



land, WV, as reported by CSB (2014). The incident resulted in three employee fatalities and one contractor injury. The explosion and ensuing fire damaged the production building and ultimately caused shutdown of the plant. Figure 5 illustrates the risk pathway of the event.

The CSB report states:

> Like all fires, a dust fire occurs when fuel (the combustible dust) is exposed to energy (an ignition source) in the presence of oxygen (typically from air). Removing any one of these elements of the classic fire triangle (depicted in [Figure 6]) eliminates the possibility of a fire.
>
> A dust explosion requires the simultaneous presence of two additional elements: dust dispersion and confinement (as shown in the dust explosion pentagon in [Figure 6]). Suspended dust burns rapidly, and confinement enables pressure buildup. Removal of either the suspension or the confinement element can prevent an explosion, although a dust fire can still occur. (CSB 2014)

Using this scenario and the risk matrix shown in Figure 7 (p. 30), a modified what-if risk assessment shown in Figure 8 (p. 30) indicates that there were no sufficient risk prevention measures available at the time of the incident. As a result, additional preventive measures were added including the redesigned blender and inert gas blanket, creating layers of prevention.

As presented in the example, likelihood and severity could be reduced for all three hazards by 63% and 75%. The remaining 25% may be retained if the organization assumes that the risk is within acceptable limits.

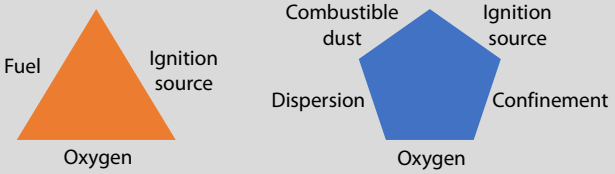
Methods for Analyzing Layers of Control

The analysis of risk control effectiveness is a critical aspect of risk assessment. ISO 31010-2019 states that "risk is affected by the overall effectiveness of any controls that are in place" and notes a risk can have more than one control, and that controls can affect more than one risk. Important aspects to consider when analyzing controls include:

- the mechanism by which the controls are intended to modify risk;
- whether the controls are in place, are capable of operating as intended, and are achieving the expected results;
- whether shortcomings exist in the design of controls or the way they are applied;
- whether gaps in controls exist;
- whether controls function independently, or if they need to function collectively to be effective;
- whether factors, conditions, vulnerabilities or circumstances exist that can reduce or eliminate control effectiveness including common cause failures;
- whether controls themselves introduce additional risks (ISO 31010-2019).

A number of methods are available for analyzing controls and their effectiveness. Some of these are described in ISO 31010-2019 and include bow-tie analysis, hazard analysis and critical control points (HACCP), event-tree analysis and LOPA. Barrier analysis, bow-tie analysis, conventional LOPA, a new

FIGURE 6
CLASSIC FIRE TRIANGLE & DUST EXPLOSION PENTAGON



Note. Adapted from "AL Solutions Inc., New Cumberland, WV: Metal dust explosion and fire (Case study No. 2011-3-I-WV)," by CSB, 2014.

FIGURE 7
RISK MATRIX

Incident outcomes				Likelihood of occurrence				
				1	2	3	4	5
Severity rating	Health effects (people)	Property damage	Environmental impact	Very unlikely	Unlikely	Possible	Likely	Very likely
5	Death or permanent total disability	Catastrophic damage	Significant impact	5	10	15	20	25
4	Permanent partial disability; hospitalizations of three or more people	Severe damage	Significant but reversible impact	4	8	12	16	20
3	Injury or occupational illness resulting in one or more days away from work	Significant damage	Moderate reversible impact	3	6	9	12	15
2	Injury or occupational illness not resulting in lost workdays	Moderate damage	Minimal impact	2	4	6	8	10
1	First aid only; no injuries or illnesses	Light damage	No impact	1	2	3	4	5
Very high risk = 15 or greater; high risk = 9 to 14; moderate risk = 5 to 8; low risk = 1 to 4								

FIGURE 8
WHAT-IF ANALYSIS

#	What if?	Answer	Human error and systems issues	L	S	Risk level	Risk level acceptable (Y/N)	Additional controls	L 2	S 2	Risk level 2	% RR
1	Metal blender is not functioning properly?	Ignition source	Task complexity or design	4	4	16	No	Redesign the blender. Inert gas (no oxygen). New procedures.	2	3	6	63%
2	Sufficient concentration of combustible dust is present?	Explosion possible	Task complexity or design	4	4	16	No	Redesign the blender. Inert gas (no oxygen). Improve ventilation to reduce combustible dust concentration. New housekeeping procedures.	1	4	4	75%
3	Explosion generates toxic gases?	Operators and EM personnel exposure	Task complexity or design. Experience	4	3	12	No	Redesign the whole operation to eliminate operator exposure.	1	3	3	75%

FIGURE 9
CONTROLS LEGEND

method called layers of mitigation analysis (LOMA), risk summation analysis, and a new method called layers of controls analysis (LOCA) are briefly presented here.

Barrier Analysis

Often used in incident investigation, a barrier analysis can be used to identify and analyze all existing controls related to the hazard(s) of a system or events and conditions of an incident.

In the analysis, the hazards, potential targets and consequences, and the pathways through which hazards can affect targets are defined. Within these risk pathways, controls, barriers and procedures that are designed to block the pathway and prevent the hazard from affecting the target are identified. The identified controls are reviewed individually in sequence of the pathway event, and in combination for effectiveness. Controls are then evaluated as to their role and performance in the incident and identified by color-coded octagons (Figure 9).

Color-coding can be used to indicate control conditions such as 1) green octagon: existing control functioned as intended; 2) yellow octagon: existing control that was not used or ignored; 3) orange octagon: existing control that was less than adequate (LTA); 4) red octagon: existing control that failed to work as intended; and 5) purple octagon: additional

FIGURE 10

LAYERS OF PROTECTION ANALYSIS

Event	Cause	Independent protection layers (IPLs)		Current state (CS) - Existing LOP			Proposed additional IPLs					Future state (FS) - After additional IPLs		
		1	2	Severity	Likelihood	Risk level	3	4	5	6	7	Severity	Likelihood	Risk level
Thermal expansion - gasoline - vapor generation	Sun - vent failure	Tank vents		4	3	12	Shade protection for tanks	Explosion-proof equipment	Internal pressure alarm	Spill containment	Auto fire extinguishing system	4	1	4
Corrosion- gasoline tanks, trim and piping	Moisture/ oxidation	Visual inspection		4	2	8	Corrosion inhibiting materials	Cathodic protection	Nitrogen blanket	Auto fire extinguishing system	Spill containment	3	1	3
Human factors/errors- gasoline tanks - overfilling	Distraction/ deviation	Visual - floating device		5	3	15	Overfill tank design	Automatic shutoff	Overfill alarm	Auto fire extinguishing system	Spill containment	4	1	4

control needed. Each evaluated control is labeled within its color-coded octagon and placed within the map connected to the affected event(s) and condition(s) as shown in Figure 9 (Lyon, Popov & Roberts, 2018).

Bow-Tie Analysis

As described in ISO 31010-2019, a bow-tie analysis is a graphical depiction of pathways from the causes of an event to its consequences. The conventional bow-tie model shows the controls that modify the likelihood of the event and those that modify the consequences if the event occurs. It can be considered as a simplified representation of a fault tree (left side of bow tie) and an event tree (right of bow tie). Bow-tie analysis is useful in visualizing the existing preventive and mitigative controls in place for an identified hazardous scenario (as shown in Figure 1, p. 26).

LOPA

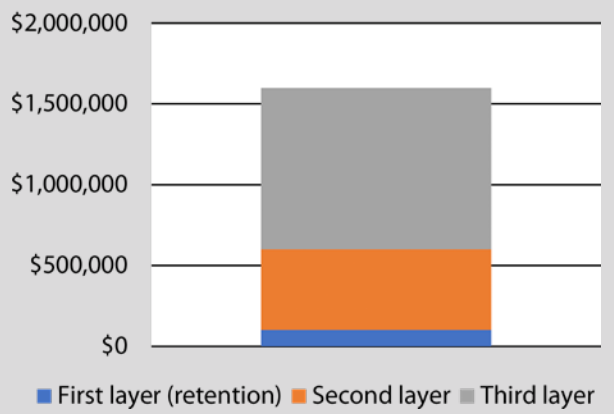
Traditionally, LOPA has been used as a barrier analysis in the chemical processing industry to analyze barriers or controls for their effectiveness in controlling an associated hazard. LOPA can be used qualitatively, semiquantitatively or quantitatively to analyze each IPL and safety integrity levels for risk reduction provided. IPLs are defined as physical barriers and controls such as design changes, engineering controls, warnings and alarms that prevent the initiating cause of a hazardous event from proceeding to an unwanted consequence. Lower-level controls such as inspections, training, standard operating procedures, and PPE are not considered barriers and are not included in LOPA. This is an important distinction.

IPLs are identified for each hazard-consequence pair. Each IPL is evaluated for its effectiveness, independence and probability of failure on demand to determine whether the overall protection provides an acceptable level of risk. Each IPL should be auditable or observable, allowing evidence and measure of its control status to verify effectiveness and reliability (Mulhausen, 2017; Rausand, 2011). Figure 10 provides an example of a conventional LOPA showing current and future states with independent protection layers.

Modified LOPA methods can be used that extend the analysis to administrative controls, financial controls and other risk reduction measures. However, if these additional layers/methods are reactive or mitigative in nature (after the undesirable event), they would not be considered layers of prevention. Hence, the new method, LOMA.

FIGURE 11

LAYERED FINANCIAL MITIGATION



Layered $ mitigation	$ amount
First layer (retention)	$100,000
Second layer	$500,000
Third layer	$1,000,000

LOMA

The term *mitigation* is generally defined as the action of reducing the severity or seriousness of something, thus making a condition or consequence less severe. Rather than a preventive measure, mitigation is a reactionary measure used to reduce severity of consequences. An emergency action plan is a mitigation plan that is designed to limit damage and harm in response to an emergency-type event (Lyon & Popov, 2019).

Similar to LOPA, the mitigation or reactive measures that are designed to limit or reduce the impact of resulting consequences could also be layered. Such layers of mitigation might include engineering, administrative, and financial and contractual measures. Examples of engineering-type mitigation measures include automatic fire suppression systems; secondary containment; automatic fire doors; and vent gas scrubbers (in case toxic gases release due to an explosion). Administrative-type mitigative measures designed to reduce the impact of the damage might include community early alarm systems and community warnings; an emergency action and evacuation plan; coordination plan with local fire and emergency responders; an Emer-

FIGURE 12

HAZARD-BY-HAZARD LOPA WORKSHEET

Event	Cause	Result	Layers of prevention				Current risk		
			1	2	3	4	Severity	Likelihood	Risk level
Combustible dust generation	Metal blender not functioning properly	Worker exposure; combustible dust accumulation	Administrative (water spray, not effective)				4	2	**8**
Ignition	Ignition source (sparks from blender)	Minor fire	Visual inspection				3	2	**6**
Operators and emergency personnel exposure	Toxic gases and hydrogen generation	Hospitalizations					4	2	**8**

FIGURE 13

LOPA WITH COMBINED RISKS CONSEQUENCES & RISK SUMMATION

Event	Cause	Result	Current layers of prevention				Current risk			Top event	Combined risk			
			1	2	3	4	Severity	Likelihood	Risk level		Severity	Likelihood	Risk summation	Combined residual risk
Combustible dust generation	Metal blender not functioning properly	Worker exposure; combustible dust accumulation	Administrative (water spray, not effective)				4	2	**8**	**Explosion and toxic gas release:** Explosive concentration of combustible dust and ignition source	5	3	**15**	**14**
Ignition	Ignition source (sparks from blender)	Minor fire	Visual inspection				3	2	**6**					
Operators and emergency personnel	Toxic gases and hydrogen generation	Hospitalizations					4	2	**8**					

FIGURE 14

LAYERS OF CONTROL ANALYSIS EXAMPLE

Event	Cause	Result	Current layers of prevention				Current risk			Top event	Combined risk				Current layers of mitigation			Consequence	Risk reduction			
			1	2	3	4	Severity	Likelihood	Risk level		Severity	Likelihood	Risk summation	Combined residual risk	Engineering layers	Adminstrative layers	Financial layers		Engineering risk mitigation factor	Adminstrative risk mitigation factor	Financial risk mitigation factor	Residual risk
Combustible dust generation	Metal blender is not functioning properly	Worker exposure; combustible dust	Admin (water spray, not effective)				4	2	**8**	**Explosion and toxic gas release:** Explosive concentration of combustible dust and ignition source	5	3	**15**	**14**	Water deluge system	EPCRA	1st layer 100K retention	Serious injuries, illnesses and fatalities	0.7	0.9	0.95	**8.08**
Ignition	Ignition source (sparks from blender)	Minor fire	Visual inspection				3	2	**6**							Business continuity plan	2nd layer 500K to primary carrier	Property damage		0.9	0.95	**11.54**
Operators and emergency personnel	Toxic gases and hydrogen generation	Hospitalizations					4	2	**8**						Natural ventilation	Evacuation plans	3rd layer 1 M to excess carrier	Environmental issues	0.7	0.9	0.95	**8.08**

FIGURE 15

STRIPED BOW-TIE MODEL WITH LAYERS OF CONTROL ANALYSIS

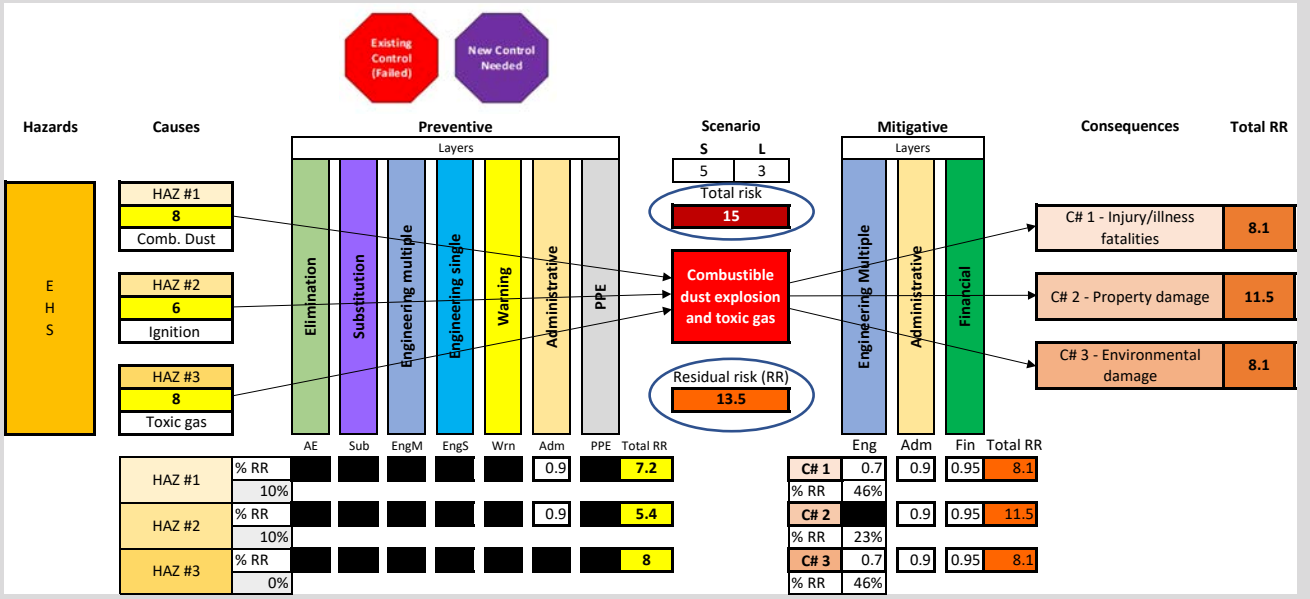


FIGURE 16

EXPANDED LOCA WITH ADDITIONAL CONTROLS

Event	Cause	Result	Future layers of prevention					Future combined risk			Future layer of mitigation			Consequence	Risk reduction			
			2	3	4	5	6	Severity	Likelihood	Risk summation	Engineering layers	Administrative layers	Financial layers		Engineering risk mitigation factor	Administrative risk mitigation factor	Financial risk mitigation factor	Residual risk
Combustible dust generation	Metal blender is not functioning properly	Worker exposure; combustible dust accumulation	Reduce quantities	Enclose the blender	Local exhaust ventilation	Dust concentration monitoring	Housekeeping	5	1	5	CO2 fire protection	EPCRA	1st layer 100K retention	Serious injuries, illnesses, fatalities	0.7	0.9	0.95	2.99
Ignition	Ignition source (sparks from blender)	Minor fire	Enclose the blender	Local exhaust ventilation	Explosion-proof equipment	H2 monitoring and FLIR heat detection	Housekeeping					Business continuity plan	2nd layer 500K to primary carrier	Property damage		0.9	0.95	4.28
Operators and emergency personnel exposure	Toxic gases and hydrogen generation	Hospitalizations	Warning alarm (local)	Local exhaust ventilation	Toxic gases monitoring							Evacuation plans	3rd layer 1M to excess carrier	Environmental issues		0.9	0.95	4.28

gency Planning and Community Right-to-Know Act plan for community evacuations or shelter-in-place; and a business continuity plan. Risk financing measures might include purchasing insurance for a large of portion of risks, transferring selected risks to third parties by contractual agreements (risk transfer), and retaining the remaining risks through self-funding. An example of financial layers of mitigation is illustrated in the stratified concept described here:

> The organization decides to retain the risk up to $100,000 U.S. Any covered losses to the organization above $100,000 would be transferred through insurance contracts to the insurance carriers (first layer at $500,000 to primary carrier; second layer at additional $1 million to excess carrier), as shown in Figure 11 (p. 31).

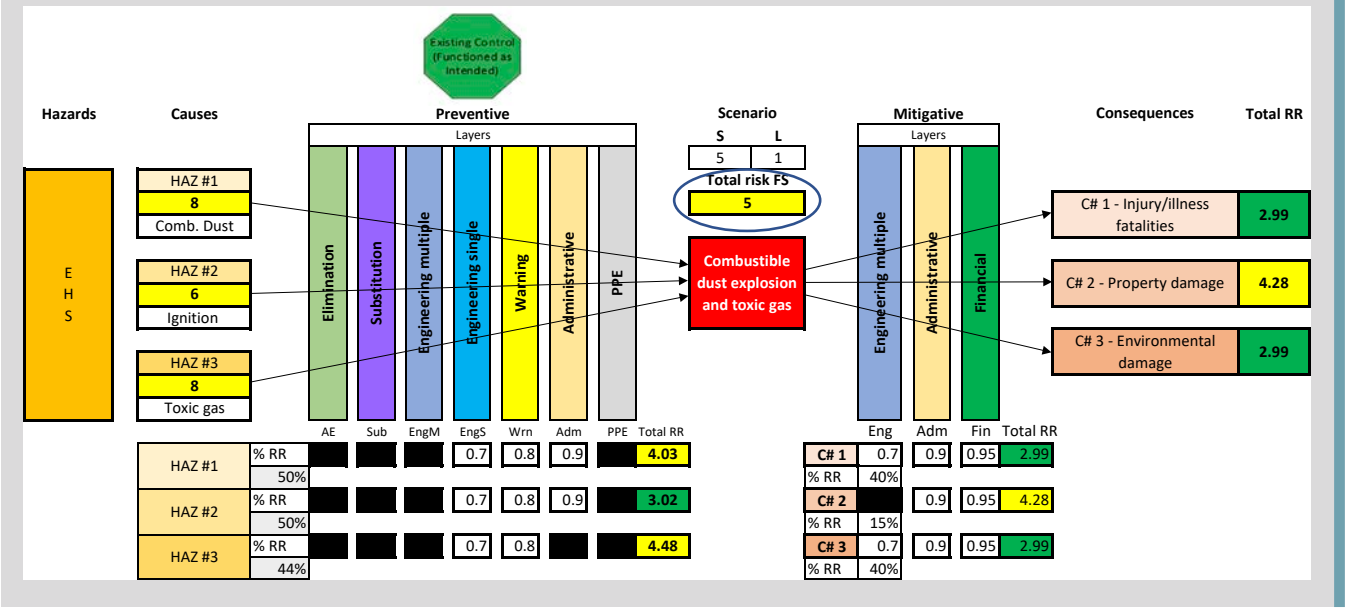
Risk Summation Analysis

Another important concept in risk assessment is whole-system risk. Conventional risk assessment methods can be described, for the most part, as linear. For example, risk assessment methods such as failure mode and effects analysis, or preliminary hazard analysis typically analyze hazards individually or hazard by hazard rather than as a whole. A hazard-by-hazard analysis would consider only partial risks within the system or operation. If partial risks are acceptable, the system or operation is then judged to be safe. Such conclusions may be misleading.

The potential effect of combined or whole-system risks is often greater than any single risk in a system. Risk assessment teams that identify and catalog individual hazards as line items may miss the potential for certain risks occurring at the same time and producing synergistic effects. For example, in the

FIGURE 17

FUTURE STATE STRIPED BOW-TIE LOCA MODEL



meat processing industry, cold temperatures combined with hand-arm vibration from pneumatic hand tools increase risk of soft-tissue damage that if analyzed individually may not be considered (Lyon & Hollcroft 2012).

If the combustible metal dust explosion previously discussed were viewed from a hazard-by-hazard perspective, the real risk level would be missed. Consider the CSB (2014) statement that "removal of either the suspension or the confinement element can prevent an explosion, although a dust fire can still occur." If risks are analyzed individually without considering additive (summation) effects, the whole-system risk can be underestimated.

The LOPA of the combustible dust case (Figure 12, p. 32) finds each individual hazard or event to be moderate risk, while missing the combined-risk effects of all three events creating a catastrophic risk level. For the metal dust generation, it was determined that it could lead to worker exposure and potential combustible dust accumulation, but by itself it was not sufficient to cause an explosion. Therefore, the severity level was considered high but not catastrophic with a low likelihood. For ignition sources, a review of past incidents in the facility revealed two minor fires leading to the determination that the severity was moderate and the likelihood low. Releases of toxic gas due to minor fires were determined to possibly lead to hospitalizations, which were considered high severity but low likelihood. Each individual event was viewed as moderate, not catastrophic.

Such an analysis does not consider the potential additive effect or sum of all risks. If the additive effects of combustible dust generation, ignition source from poor blender maintenance, confinement, potential dispersion and the presence of oxygen are considered, the risk summation (total risk) would produce a more realistic risk level in the higher risk category as shown in Figure 13 (p. 32).

Additionally, residual risk of the combined risks could be added based on the current controls. The company's dust control methods of washing down the metal powder, an administrative control, was considered acceptable by the property risk insurer. In fact, the control methods were highly ineffective and may have added hazards like hydrogen generation. Assuming that administrative controls would reduce the risk by 10%, the operation's combined residual risk would still be considered high at 13.5.

LOCA

Recognizing a need for a method that considers the layers of preventive measures along with layers of mitigative measures and their risk levels, the authors developed the LOCA method. LOCA is described as a combination of LOPA, which analyzes preventive independent protection layers, and LOMA, which analyzes reactionary measures including engineering, financial and administrative controls.

Taking the layers of protection analysis for the combustible dust explosion case study in Figure 10 (p. 31), the resulting LOCA is presented in Figure 14 (p. 32).

For consequences such as fatalities, serious injuries and illnesses, extensive property and environmental damage, mitigation measures have limited effect on reducing residual risk as indicated by the CSB report on the metal dust explosion.

The water deluge system on the ceiling of the production building is considered a mitigation layer. However, it is not advisable to use water to fight a titanium or zirconium fire due to hydrogen generation. CSB (2014) found that "AL Solutions did not have a ventilation system to control hydrogen concentrations. Natural ventilation was inconsistent in the production building; employees reported closing rollup doors for temperature control during the cold months."

Evacuation and business continuity plans would not reduce the risk significantly. Even the layered insurance would probably be insufficient. The families of three people killed in an industrial incident in 2010 have reached a $15.8 million final settlement with two private equity firms that had invested in AL Solutions Inc. (The Review).

To effectively reduce risk, both preventive and mitigative measures must often be used. This concept can be further visualized

in the striped bow-tie model (Lyon & Popov, 2016). This model considers both the preventive measures for existing hazards on the left-hand side of the top event, and the mitigating or reactive measures for reducing the impact of the event on the right-hand side (Figure 15, p. 33). All three hazards are analyzed as a whole for their severity and likelihood to determine their combined or total risk, which is entered above the top event. Then, the mitigating measures such as the administrative controls, water spray and visual inspections are analyzed together to estimate the residual risk, which is displayed below the top event.

Using the barrier analysis previously discussed, any existing controls that failed are identified, along with new additional controls that are needed. The two octagons described in the barrier analysis (see Figure 9) are inserted above the layers of prevention or preventive controls columns to indicate these actions.

As a general rule, it is more beneficial from a risk-reduction standpoint to invest in layers of prevention, than layers of mitigation. Therefore, additional LOPs are added and the risk level recalculated after the implementation of the new preventive control measures. Suggestions for additional controls are presented in Figure 16 (p. 33). Notice that controls such as blender enclosure, local exhaust ventilation and warning alarms will address multiple risks.

Using the striped bow-tie methodology to analyze and estimate the total risk (or risk summation) in a future state indicates that a risk reduction could be achieved that is considered acceptable. This, of course, requires assurances that all controls (new and existing) are effective, reliable and consistently functioning as intended. Upon verification and validation of controls, a green octagon from the barrier analysis can be inserted above the preventive controls columns as shown in Figure 17.

Conclusion

Layers of defense have been used throughout the years and have proven to be effective in reducing the risk from multiple threats. The OSH professional should consider this approach for the workplace when analyzing and designing risk reduction measures, to include preventive measures as well as mitigating measures. Rarely is one control method adequate in preventing or protecting people, property or environment from harm. Using methods such as bow-tie analysis, LOPA, LOMA and LOCA to analyze existing controls and their effectiveness, and estimate risk summation can help OSH professionals identify weaknesses and needs for building additional layers of control. **PSJ**

References

American Petroleum Institute (API). (2013). Security risk assessment methodology for the petroleum and petrochemical industries (API Std 780) (1st ed.). Washington, DC: Author.

API. (2016). Facility security plan methodology for the oil and natural gas industries (API RP 781) (1st ed.). Washington, DC: Author.

ANSI/ASSP. (2011). Vocabulary for risk management (National adoption of ISO Guide 73:2009) (ANSI/ASSP Z690.1-2011). 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.

ANSI/ASSP/ISO/IEC. (2019). Risk management—Risk assessment techniques (ANSI/ASSP/ISO/IEC 31010-2019). Park Ridge, IL: ASSP.

Center for Chemical Process Safety (CCPS). (2008). *Inherently safer chemical processes: A life cycle approach* (2nd ed.). Hoboken, NJ: Wiley.

CSB. (2014). *AL Solutions Inc., New Cumberland, WV: Metal dust explosion and fire* (Case study No. 2011-3-I-WV). Retrieved from www.csb.gov/al-solutions-fatal-dust-explosion

CSB. (2015). *Final investigation report: Caribbean Petroleum tank terminal explosion and multiple tank fires* (Report No. 2010.02.I.PR). Retrieved from www.csb.gov/assets/1/20/capeco_final_report__10.21.2015.pdf

EPA. (2013, Dec. 19). AL Solutions Inc. Settlement. Retrieved from www.epa.gov/enforcement/al-solutions-inc-settlement

Federal Emergency Management Agency (FEMA). (2020). What is mitigation? Retrieved from www.fema.gov/what-mitigation

Franks, A. (2017). Lines of defense/layers of protection analysis in the COMAH context. London, England: Health and Safety Executive. Retrieved from www.hse.gov.uk/research/misc/vectra300-2017-r02.pdf

Livius.org. (2020). Constantinople, Theodosian walls. Retrieved from www.livius.org/articles/place/constantinople-istanbul/constantinople-photos/constantinople-theodosian-walls

Lyon, B.K. & Hollcroft, B. (2012, Dec.). Risk assessments: Top 10 pitfalls and tips for improvement. *Professional Safety, 57*(12), 28-34.

Lyon, B.K. & Popov, G. (2016, March). The art of assessing risk: Selecting, modifying and combining risk assessment methods to assess risk. *Professional Safety, 61*(3), 40-51.

Lyon, B.K. & Popov, G. (2017, Nov.). Communicating and managing risk: The key result of risk assessment. *Professional Safety, 62*(11), 35-44.

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

Lyon, B.K. & Popov, G. (2019, May). Risk treatment strategies: Harmonizing the hierarchy of controls and inherently safer design concepts. *Professional Safety, 64*(5), 34-43.

Lyon, B.K., Popov, G. & Roberts, A. (2018, Oct.). Causal factors analysis: Uncovering and correcting management system deficiencies. *Professional Safety, 63*(10), 49-59.

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

Mulhausen, J. (2017). Improving general industry qualitative risk assessment using LOPA concepts. Safety 2017: ASSP Professional Development Conference, Denver, CO.

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

Rausand, M. (2011). *Risk assessment: Theory, methods, and applications*. Hoboken, NJ: John Wiley & Sons.

Reason, J. (2016). *Organizational accidents revisited*. Boca Raton, FL: CRC Press.

The Review. (2016, Oct. 5). AL Solutions settlement ends civil claims. Retrieved from www.reviewonline.com/news/local-news/2016/10/al-solutions-settlement-ends-civil-claims

WebFinance Inc. (2020). BusinessDictionary: Prevention. Retrieved from www.businessdictionary.com/definition/prevention.html

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. In 2018, he received the CSP Award of Excellence from BCSP. 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.

Georgi Popov, Ph.D., CSP, ASP, QEP, SMS, ARM, 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. He received the chapter's 2015 Safety Professional of the Year (SPY) Award and the 2016 ASSP Region V SPY Award. In 2017, Popov received ASSP's Outstanding Safety Educator Award.