# 1

# The Lens of System Safety

Your occupational electrical safety program may need a reset. This book can help you discover hidden risks that can be reasonably and feasibly reduced using techniques that have demonstrated results in preventing serious injuries, fatalities, and other catastrophic consequences.

Since the passage of the Occupational Safety and Health Act (OSHA) in 1970, the discussion of occupational safety in the United States has focused mainly on compliance with safe work practices in OSHA regulations and industry consensus standards. The regulations and standards have and will continue to help prevent serious injuries and fatalities. However, regulations and standards provide minimum requirements. Compliance with minimum requirements may create an illusion for management and workers that risk is reduced to as low as reasonably practicable (ALARP). A gap may exist between risk reduction achieved from compliance with minimum requirements versus risk reduction achieved by other means, or the difference between the accepted risk and the acceptable risk. ALARP expectations will vary from organization to organization and from one individual to another. What is considered acceptable risk will change over time, impacted by various forces, including social consciousness, competitive environments, and leadership goals.

OSHA regulations and industry standards relevant to electrical safety provide requirements and guidance to control exposure during work activity. However, electrical safety does not start during the installation, operation, and maintenance of electrical systems in the workplace. Decisions made during the design, specification, and procurement of equipment, components, and tools can have a positive or negative contribution to exposure to hazardous electrical energy. These decisions occur long before the workplace exists and have an impact on the exposure for the life of the facility or equipment.

*Hidden Risk in Occupational Electrical Safety: Through the Lens of System Safety*,
First Edition. H. Landis “Lanny” Floyd.

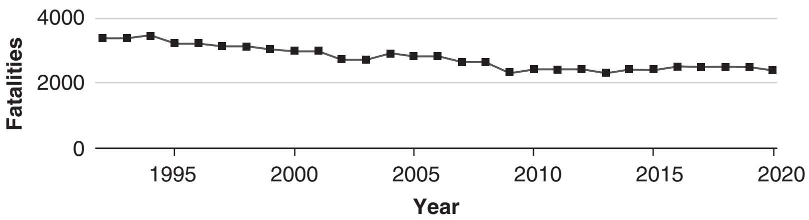


**Figure 1.1** The trend in occupational fatalities from all causes in the United States, 1990–2020.

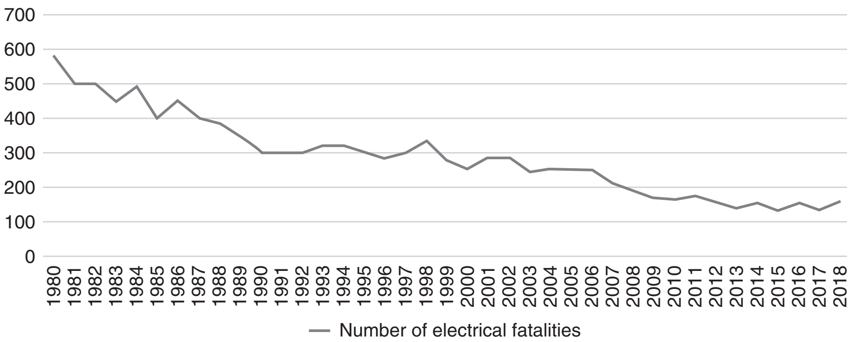


**Figure 1.2** The trend in occupational fatalities from exposure to electrical hazards in the United States, 1980–2018.

Thought leaders in safety management, including Peterson, Krause, and Manuele, have expressed concern about the trend in occupational fatalities in the United States. During this period, the downward trend in the number of fatal injuries from all causes and the subset of fatalities from exposure to hazardous electrical energy has flattened (Figures 1.1 and 1.2).

In a compliance-based culture, organizations adhere to standards and regulations, which can lead to a "check-the-box" approach to comply with the minimum requirements provided by standards and regulations. A risk-based approach helps identify risks that remain even after achieving compliance. The residual risks can then be assessed to determine if additional controls are warranted.

Organizations can be blinded by the data and fail to see the need to go beyond minimal compliance. Lost-time injuries from exposure to hazardous electrical energy are relatively rare in the context of all lost-time occupational injuries. During the third decade of the 21st century, less than 0.2% of all occupational lost-time injuries in the United States are attributed to injuries from exposure to hazardous electrical energy. The very low frequency of electrical injuries in an individual's or organization's experience can create an illusion of the effectiveness of compliance-based risk control in two ways:

1) It can create a false perception for management that hazards have been identified and risk controls are adequate.
2) It can be challenging for workers to stay vigilant and maintain a perception of risk in the face of a low probability of occurrence.

Andersen and Denkle noted that there is a wide range of severity associated with occupational lost-time injuries. Their research showed that 1 in 250 lost-time injuries from all causes was fatal. However, Cawley and Brenner reported that 1 in 13 lost-time injuries from exposure to hazardous electrical energy is fatal. The low frequency of electrical injuries can lead to the electrical hazards being accepted, the risk of injury being underestimated, and the effectiveness of mitigation controls being overrated (Table 1.1).

A risk-based approach to managing occupational safety reaches beyond compliance with the minimum requirements of regulations and standards. In a risk-based approach, compliance with standards and regulations is a means, but not the end, of hazard identification and applying risk control measures. Even after achieving compliance, residual risk may be further reduced using hazard identification and risk control evaluation tools. The most comprehensive safety and risk management methodology is system safety; however, its use has historically been limited to the never-before-seen catastrophic safety risks that

**Table 1.1** Comparison of select non-fatal occupational injuries in the United States 2010.

| Type of Non-Fatal Injury | Number of Injuries |
|---|---|
| Total | 1, 191, 100 |
| Sprains, strains, tears | 474, 000 |
| Musculoskeletal disorders | 346, 300 |
| Falls on the same level | 182, 400 |
| Struck by object | 138, 530 |
| Falls to lower level | 73, 520 |
| Assault/violent act by person | 40, 310 |
| Highway accidents | 36, 460 |
| Assault/violent act by animal | 7, 160 |
| Fires and explosions | 3, 000 |
| **Electrical shock and burn** | **1,890 (0.16%)** |

Adapted from U.S. BLS Economic News Release, 2010.

emerged in the 20th century, such as nuclear weapons and commercial aviation. What if electrical safety professionals were more familiar with concepts derived from system safety? System safety has its roots in the 1940s, with the rapidly expanding military and commercial aviation industries and nuclear weapons technology. Designers, manufacturers, and pilots were pushing the envelope in technology. As airplanes became more sophisticated, the cost of mishaps escalated. The aviation industry recognized that analyzing mishaps after the fact was becoming unacceptable in terms of human safety and financial loss. In his paper, "Using System Safety Techniques to Perform Hazard Analysis," Kolak noted, "The costs associated with damaging expensive fighter jets and the development of nuclear energy (where a single system failure was unacceptable) contributed to the concept that hazards must be anticipated and controlled before even a single loss occurs." These emerging technologies, operating at the edge of engineering capability, using unproven technology, required conservatism to protect against unknown mishap risks and allowed for novel solutions.

System safety evolved to address exotic technologies with never-before-seen catastrophic consequences. It was not intended to be applied in managing the risks associated with the more common hazards in the workplace. Table 1.2 lists more than 20 risk assessment tools and techniques used in system safety. The costs and resources needed to apply system safety to all hazards and risks would be unreasonable and impractical. However, concepts learned from system safety were instrumental in developing regulations and standards for highly hazardous

**Table 1.2** Hazard identification and risk analysis tools used in system safety.

| | |
|---|---|
| Preliminary hazard analysis | Sneak circuit analysis |
| What if analysis | Layers of control analysis |
| Subsystem hazard analysis | Petri net analysis |
| System hazard analysis | Markov analysis |
| Operating and support hazard analysis | Barrier analysis |
| Health hazard analysis | Bent pin analysis |
| Layers of protection analysis | Hazard and operability analysis |
| Fault tree analysis | Cross-consequence analysis |
| Event tree analysis | Common cause failure analysis |
| Failure mode and effect hazard analysis | Management oversight risk tree analysis |
| Fault hazard analysis | Software safety assessment |
| Functional hazard analysis | Bow tie analysis |

chemical processes in the early 1990s, including OSHA 1910.119 Process Safety Management and the Environmental Protection Agency's Risk Management Program. The demonstrated results of system safety influenced the development of ISO 45001 in 2018 and also the 2019 revision to ANSI/ASSP Z10. The critical concept learned from decades of experience with system safety is that it can provide the "lens" to illuminate and identify risks that remain after compliance with regulations and standards is achieved.

System safety engineering evolved as a way to minimize the consequences and likelihood of mishaps by eliminating causes attributed to equipment design, equipment reliability, and human error. In 1969, the U.S. Department of Defense published MIL-STD 882, *Standard Practice for System Safety*. Initially published for managing risks associated with the first-generation nuclear ICBM deployment, this standard has provided the basis for managing the safety of complex systems such as military aviation, nuclear weapons, nuclear-powered ships and submarines, as well as less complex systems such as facility operations. The standard has influenced the application of safety system engineering to non-military systems, including commercial nuclear power generation, commercial aviation, space travel, and highly hazardous petrochemical operations. The following definitions from MIL-STD 882E, *Standard Practice for System Safety*, provide an introduction to some of the fundamental concepts of systems safety engineering:

> Mishap: An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
>
> System: An integrated composite of people, products, and processes that provide the capability to satisfy a stated need or objective.
>
> System safety: The application of engineering and management principles, criteria, and techniques to achieve an acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and costs, throughout all phases of the system life cycle.

System safety engineering concepts include hazard identification and analysis, application of a hierarchy of hazard control measures, and integration of management, engineering, procurement, and operations functions in managing safety objectives. These concepts are the foundation of occupational safety and health management systems standards that emerged since the 1990s, including OHSAS 18001 *Occupational Safety and Health Management Systems – Requirements*, ANSI Z10 *Occupational Health and Safety Management Systems*, CSA Z1000 *Occupational Safety and Health Management*, and ISO 45001 *Occupational Safety and Health Management Systems.*

## Demonstrated Performance

Research by Mendleoff and Staatsky shows that the countries in the European Union (EU) have a significantly lower occupational fatality rate than the United States, with the U.S. fatality rate being ~4× that of the United Kingdom. Although there are cultural, social, educational, and political differences that may contribute to the lower fatality rates, thought leaders in safety point to the broad application of risk assessment processes as a significant difference between the United Kingdom and the United States. Fred Manuele noted that risk-based culture is the cornerstone of the EU approach to occupational safety management. The American Society of Safety Professionals, OSHA, and other safety institutions have promoted a risk-based approach as critical to further improvement in injury and fatality reduction.

For over 75 years, system safety has delivered extraordinary results in reducing risks of 20th-century technological advancements that have the potential for catastrophic mishaps, including nuclear energy, advanced weapons systems, aviation, and manned space exploration.

Exploring electrical safety through the lens of system safety involves understanding hazard identification, risk assessment, and risk reduction to supplement the results in injury prevention afforded by a compliance-based approach. To create a lens of system safety and enable this exploration, individuals and organizations must recognize that simple compliance with the minimum requirements of regulations and industry standards always has residual risk that may not be ALARP. Electrical safety leaders should commit to continual learning on system safety and risk-based safety management.

After achieving compliance with safe work practices, applying risk management techniques includes exploring answers to questions, such as "How can the risk controls fail? What are the consequences if one or more controls fail? Are the potential results acceptable?" These questions are fundamental to system safety. In the context of possible exposure to hazardous electrical energy, asking and answering these questions can help see beyond compliance with minimum requirements to how hidden hazards can be identified and how residual risk can be further reduced. Electrical safety leaders can explore these questions throughout the life cycle of a facility or system, including initial design, equipment specification and procurement, task planning, job safety analysis, and incident investigations.

## Demonstrating Results in Moving Beyond Compliance

In 1989, DuPont, a global Fortune 500 company made a highly visible commitment to reduce the likelihood and severity of injuries to employees and contractors from

**Table 1.3** Elements of the strategy described in the paper "Creating a Continuous Improvement Environment for Electrical Safety."

- Understand the business consequences of electrical incidents
- Engage all employees
- Stimulate near-miss reporting
- Apply quality improvement model – Plan Do Check Act
- Build networks
- Challenge accepted practices
- Improve collaboration among management, electrical experts, and safety professionals
- Use standards as tools
- Promote prevention by design
- Address life cycle: design, construct, operate, maintain, dismantle

electrical hazards. Goals for sustainable improvement were established, financial support provided, and dedicated people empowered to reduce the likelihood of electrical incidents, injuries, and fatalities, with the intent to accomplish a step change in electrical safety performance, as was done in the mid-1950s. At that time, the company had taken action to eliminate the practice of working on energized circuits, which was commonplace in the early days of industrial electrification. In the early 1990s, leaders in the electrical safety improvement initiative outlined a strategy for establishing a culture for long-term continuous improvement in electrical safety. The elements of that strategy, shown in Table 1.3, describe organizational culture intent on long-term impact on preventing electrical incidents and injuries. The culture and continuous improvement strategy described in these papers and nurtured for more than 20 years resulted in significant improvement in reducing the severity and frequency of electrical injuries in the company. Most dramatic is the impact on the frequency of fatalities from electrical energy. In the 1980s and early 1990s prior to 1993, fatalities from electrical energy were occurring on average every 33 months. The chart in the figure represents a global workforce of employees and contractors that ranged from 80,000 to 120,000 during this period. From 1993 through 2016, there were zero fatalities from electrical hazards in company facilities.

The exposure to hazardous electrical energy increased due to the increasing application of electrical technologies for energy, control, and communications. The significant change was the shift in the electrical safety culture driven by the continuous improvement environment that looked beyond simple compliance with regulations and standards.

## A Task Example

In this example, the power system for an industrial manufacturing facility included five 12-kV feeders and 13 substations configured to enable 100%

redundancy to allow maintenance access without disrupting production. The isolation of one substation involved 36 lockout points, including eight 12-kV circuit breakers, eight 12-kV potential transformers, six 480-V circuit breakers, six 480-V switches, five 480-V tie breakers, two 125-V DC control circuits, and one 120-V AC station power circuit. Nine sets of temporary safety grounds were applied for personnel protection. After establishing an Electrically Safe Work Condition (ESWC) for this substation, the supervising engineer recognized that the shutter in the rear of a 12-kV circuit breaker cell presented a residual risk. The cell shutter was an engineering control providing a barrier covering the 12-kV stationary connection contacts when the 12-kV circuit breaker was removed from the cell. A worker could easily lift the shutter in an empty cell, creating a dangerous exposure to bare, unguarded 12-kV circuit parts. After achieving the original ESWC, the supervising engineer asked the following questions:

1) Where is the hazard?
2) What have I done to control exposure to the hazard?
3) How can the controls fail?
4) Will additional controls further reduce the risk of exposure?

These questions demonstrate the power of creating a lens of system safety to illuminate the hidden danger. A previously unrecognized significant risk of exposure to lethal hazardous energy was avoided by asking the above simple questions in collaboration with the maintenance crew. This residual risk was controlled by adding the shutter lever as an additional lockout point to the ESWC plan.

An organization's electrical safety program is typically an integration of regulations and standards that establish minimum requirements for the safe design, installation, operation, and maintenance of electrical systems. By creating a "lens of system safety," electrical safety leaders can be vigilant in identifying and further reducing residual risk.

The above example shows how the lens of system safety was used during the execution of a work task with potential exposure to hazardous energy. The lens can be used throughout the life cycle of a project. Hazard identification, assessment of risk, and selection of risk controls during the design phases of the life cycle are generally more effective and less costly than during the post-design phases, as design changes are permanent and less dependent on human performance during the operational phases of the life cycle. Other application opportunities include incident investigations, equipment specification and procurement, safety audits, and pre-job planning.

The rigorous methodologies of system safety have proven effective in managing the risks of technological mishaps with catastrophic consequences. Significant further reduction in occupational electrical injuries and fatalities will require a culture shift in safety management. Compliance-based programs must shift from compliance only to incorporate risk management and other concepts derived from system safety. Electrical safety leaders must commit to continual learning of the most effective approaches to safety management.

Adding risk management components to compliance involves an in-depth understanding of hazard identification, risk assessment, and risk reduction to supplement the results in injury prevention afforded by a compliance-based approach. A pure application of system safety to common risks, such as electrical injuries, is not practical or reasonable due to the resources and competencies needed. However, lessons from system safety can be used to identify and control risks that may remain after compliance with regulations and standards is achieved.

Significant improvement in preventing injuries and fatalities from exposure to electrical energy is possible and achievable. Electrical safety leaders can use the lens of system safety to highlight ways to address the residual risk left unmitigated by a compliance-only approach to electrical safety. Using a lens of system safety can change the paradigm of compliance and the opportunities to integrate the lessons of system safety into existing electrical safety regulations, standards, and programs to prevent electrical injuries and fatalities further.

## Crosstalk: Questions for Thought and Discussion

**1** How do you and your organization view regulations, codes, and standards? Are they minimum or optional requirements in your electrical safety program?

**2** Have you ever heard someone say, “If OSHA doesn’t require it, why should we do it?” What does this say about the electrical safety culture in your organization?

**3** How does your organization describe acceptable risk?

**4** How do you know you have achieved acceptable risk?

**5** How do you know if what is considered acceptable risk could be reduced with reasonable effort?

## Further Reading

Anderson, M. and Denkl, M. The Heinrich triangle—Too simplistic a model for HSE management in the 21st century? *Proc. Int. Conf. Health Safety Environ*. (December 2010), Rio de Janeiro, Brazil, Society of Petroleum Engineers.

ANSI/ASSE Z590.3. Prevention through design guidelines for addressing occupational hazards and risks in design and redesign processes, Des Plaines, IL, USA, American Society of Safety Professionals.

ANSI/ASSP Z10. Occupational health, and safety management systems. Des Plaines, IL, USA, American Society of Safety Professionals.

ANSI/ASSP Z590.3. Guidelines for applying prevention through design in design and redesign processes. Des Plaines, IL, USA, American Society of Safety Professionals.

Barr, N.J. (2015). *System Safety Engineering and Risk Assessment*. Boca Raton, FL: CRC Press.

Benton, J. ASSE & OSHA concentrate collective efforts on risk-based approach. *EHS Safety News* (26 October 2012), retrieved from https://ehssafetynewsamerica.com/2012/10/26/asse-osha-concentrate-collective-efforts-on-risk-based-approach-in-oil-gas-industry/.

Cawley, J.C. and Brenner, B.C. (2013). Occupational electrical injuries in the U.S., 2003–2009. *IEEE Industry Applications Magazine* 19 (3): 16–20.

Dezfuli, H., Benjamin, A., Everett, C. et al. *NASA System Safety Handbook, – Vol 2: System Safety Concepts, Guidelines, and Application Examples*. US National Aeronautics and Space Administration NASA/SP-2014-612, version 1.0 (1 November 2014).

Ericson, C.A. (2005). *Hazard Analysis and Techniques for System Safety*. Hoboken, NJ: Wiley.

Floyd, H.L. (2024). Through the lens of systems safety: the limitations of a compliance-based safety culture and opportunities to reduce electrical injuries. *IEEE Industry Applications Magazine* 30 (3): 12–17.

Floyd, H.L. and Cole, B.C. (2015). Twenty years later: creating a continuous improvement environment for electrical safety. *IEEE Transactions on Industry Applications* 51 (3): 2633–2640.

Floyd, H.L., Cole, B.C., Doughty, R.L. et al. (1994). Creating a continuous improvement environment for electrical safety. *IEEE Transactions on Industry Applications* 30 (3): 543–552.

ISO 45001. Occupational health and safety management systems, international standards organization, Geneva, Switzerland.

Kolak, J.J. Using system safety techniques to perform hazard analysis. *Conference Record of American Society of Safety Engineers Safety 2012 Conference* (3–5 June 2012), Denver, CO.

Krause, T., Bell, K., and Libby, D. Serious injury and fatality prevention – 10 years later (25 May 2020). https://krausebellgroup.com/serious-injury-and-fatality-prevention/.

Lewis, C.L., Haug, H.A. (2006). *The System Safety Handbook*. Self-published, retrieved from the internet at https://www.aerohabitat.eu/uploads/media/14-04-2006_-_Lewis_-_Haug__System_safety_handbook__0.3MB_.pdf.

Liberty Mutual Research Institute for Safety. *Work Related Electrical Injuries: Study Sparks New Insights*, vol. 13, no. 3, Liberty Mutual Research Institute for Safety, Hopkinton, MA: 2010.

Lyon, B. and Popov, G. (2018). *Risk Management Tools for Safety Professionals*. Parkridge, IL: Am. Society of Safety Professionals.

Manuele, F. (2013). Preventing Serious Injuries & Fatalities: Time for a Sociotechnical Model for an Operational Risk Management System. *Journal for Professional Safety* (May 2013).

Manuele, F. (2020). *Advanced Safety Management, Focusing on ANSI Z10, ISO 45001 and Fatality Prevention*, 3e. Hoboken, NJ, USA: Wiley.

Mendeloff, J. and Staatsky, L. (2014). Occupational fatality risks in the U.S. and the U.K. *American Journal of Industrial Medicine* 57: 4–14.

Peterson, D. Why safety is a people problem. *EHS Today* (31 March 1996), retrieved from https://www.ehstoday.com/archive/article/21907885/dan-petersen-why-safety-is-a-people-problem.

Peterson, D. and Williamsen, M. (2007). The culture of safety. *Journal for Professional Safety* March 2007: 17–19 and 57–59.

Stevans, R. (2004). *System Safety for the 21$^{st}$ Century*. Wiley.

U.S. Bureau of Labor Statistics. Injury, illness and fatalities. https://www.bls.gov/iif/latest-numbers.htm.

Walter, L. Facing the unthinkable – fatality prevention in the workplace. *EHS Today* (31 December 2007). https://www.ehstoday.com/safety/article/21904194/facing-the-unthinkable-fatality-prevention-in-the-workplace.

Wyzga, R.E. and Lindroos, W. (1999). Health implications of global electrification. *Annals. New York Academy of Sciences* 888: 1–7.