Course Learning Outcomes for Unit V

Upon completion of this unit, students should be able to:

5. Examine the role of hazard analysis in system safety efforts.
   5.1 Discuss qualitative and quantitative safety analysis in system safety efforts.

7. Evaluate risk management tools related to system safety management.
   7.1 Discuss the different qualitative and quantitative risk management tools used for system safety management.

Course/Unit Learning Outcomes	Learning Activity
5.1	Assessment, Lesson, Required Reading
7.1	Assessment, Lesson, Required Reading

Reading Assignment

Chapter 8: FMECA, Human Factors, and Software Safety

Chapter 9: Other Techniques

Unit Lesson

Since the first unit, we have discussed how system safety is managed through system safety engineering and how system safety engineering is accomplished through safety analysis. We have mentioned, with several different examples, how safety analysis is most effectively accomplished through the use of conceptual models containing both qualitative and quantitative elements. This is all to achieve the over-arching purpose of system safety engineering, and that is the ability to statistically predict hazards and subsequent risks within work systems well before subjecting humans and the environment to the work system. As a result, you have learned that implementing system safety engineering helps to stop accidents from happening by designing out the hazard from the work system.

In this unit, you are going to investigate the most cutting-edge qualitative and quantitative risk management tools available to system safety engineers and learn to leverage the predictive power of these tools to effectively manage system safety within a work system. Given that you are most interested in predicting accidents before they occur, we need to start with quantitative tools that provide us with the mathematical capacity to statistically calculate probability within a work system. Bahr (2015) briefly introduces us to failure modes and effects analysis (FMEA); failure modes, effects, and criticality analysis (FMECA); human factors safety analysis, and various computer software safety analysis techniques. Let's take a more in-depth look at how these quantitative tools work.

Quantitative Tools

Starting with FMEA, remember that a failure is not required within a work system for a hazard to be present in the system. This is where you have your initial opportunity to identify hazards, analyze the hazard for the probability of occurrence, then make a data-based decision to design out the hazard from the system to remove the specific associated risks from the work system. As you learned in your Unit IV work, quantitative fault tree analysis (FTA) is an effective way to understand the overall top-event probability of occurrence, given our ability to use Boolean mathematics to sum probability among different components of a work system to include even equipment within the work system (Bahr, 2015). On page 219 of the textbook, you will

find a working example of calculated failure probability of a pressure tank system. Where FTA largely differs from FMEA is with the differences in each tool's consideration of reliability and safety. FTA can help us estimate the probabilistic failure of a system as a whole as a measure of reliability, but FMEA evaluates reliability and identifies single-point failures within the system (Stephans, 2004). As a result, FMEA was actually designed to serve as a quality engineering tool and was used as a reliability measurement tool rather than as an applied system safety tool (Bahr, 2015). The result of not understanding this concept when using the FMEA may lead the safety engineer to inadvertently identify failures instead of identifying causes. Consequently, it is imperative that you not confuse the term *reliability* with *safety* and the term *cause* with *symptom* or *effect*, which is often mistakenly identified as a failure within a system (Leveson, 2011).

For example, if an automobile has a faulty brake system, you can calculate a high probability of the automobile consistently, or reliably, not stopping properly when one depresses the brake pedal. As such, the automobile, the entire system, could be considered to be unsafe yet reliable. You would first have to identify the effects, which are the symptoms of the failure such as an inoperable master cylinder or ineffective brake pads, then investigate the causes related to the single-point failures such as the master cylinder not being completely full of brake fluid and without bubbles or worn brake pads. FMEA helps the system safety engineer predict single-point failure within a work system, classify each failure potential with qualitative hazard probabilities (such as Level A, Level B, and so on), then ultimately assess the potential for reliability breaches (failure) with quantitative values (such as Level A = Frequent or $x > 10^{-1}$, and Level B = Probable or $10^{-1} > x > 10^{-2}$), as we learned in our Unit III material (Bahr, 2015). This is due to the use of preliminary hazard list (PHL) or preliminary hazard analysis (PHA) a step within the FMEA process. You may want to review the discussion about these two tools from the Unit IV material.

This is why FMECA, not to be confused with FMEA, was designed with the system safety engineer being able to focus on the probability of failure considerably more than with FMEA. This is accomplished with FMECA by identifying the necessary independent variables, failure effect probability, failure mode ratio, part failure rate, and operating time, then effectively calculating the relationship among the variables. The result is a failure mode criticality number that can then be loaded into a criticality matrix, evaluated among other components within the work system, and subsequently ranked as to the most critical potential failure to the entire work system that would bring it down (Bahr, 2015).

Statistical forecasting, or predicting, in system safety engineering gets more interesting once humans are introduced into the work system. The human factors theory of accident causation considers human-influenced events leading to a chain of events ultimately caused by human error within the work system. The human error is considered the dependent variable, with the potential contributing independent variables including inappropriate human response, inappropriate human activities, and inappropriate human task overloading (Goetsch, 2015). The idea is that the human interaction within a mechanized work system, often as an actual component of the work system such as in service-related work systems or semi-robotic manufacturing systems, has the measureable propensity to compromise the reliability of the work system. Bahr (2015) discusses the resulting field of study termed human factors engineering and equates that field of study with the more contemporary term ergonomics. As a result of the merging three fields of human factors engineering, ergonomics, and human reliability engineering, the system safety tool human factors safety analysis was derived (Bahr, 2015; Hammer & Price, 2001; Stephans, 2004). Using human factors safety analysis, the out-of-tolerance interaction between the human and a mechanized system can actually be quantitatively predicted to derive a human error probability (HEP). Bahr explains how this HEP value is calculated by simply dividing the observed number of errors made with a determined sample size of the human operator population of a work system by the number of potential opportunities for errors to occur, the required physical interactions between the human and the affected machine. The resulting human reliability probability is then simply 1 – HEP or 100% - %HEP.

Software safety analysis is another common application of quantitative tools with computer-assisted statistical forecasting of safety-critical systems reliability and probabilistic hazard analysis. These become considerably useful when attempting to assess system safety within highly specialized industries such as mass transportation systems. Bahr (2015) provides you with an overview of these optional tools, but it is important to realize that while the system safety engineer loads the software programs with qualitative data in many instances, the program often quantitatively assesses probabilistic risks. What becomes important is for the system safety engineer to remember that there is an inherent risk of human factors impact between the safety engineer using the program and the program itself. As such, it is arguably reasonable to expect an HEP value to be associated with even these programs, given that a human, the safety engineer is using a machine, the computer, and software to accomplish a safety analysis of a work system. This is one of the tremendous

ironies of safety engineering. Ultimately, the locus of control remains with the safety engineer, and the safety engineer's personal and professional experiences necessarily inform the safety analysis results. This is why qualitative tools become so important, used in tandem with quantitative tools, during safety analysis.

Qualitative Tools

Several qualitative tools are provided in the textbook for you to consider, providing only a cursory review of a select number of tools. These include management oversight and risk tree (MORT) analysis, energy trace barrier analysis (ETBA), sneak circuit analysis, cause-consequence analysis, root cause analysis, bow tie analysis, chemical emission and dispersion modeling, and the concept of test safety. What becomes very important to realize is that while most of these tools are actually interactive conceptual models featuring qualitative information, they can easily be used in a quantitative technique, especially chemical emission and dispersion modeling. Test safety is described as a conceptual process rather than an actual safety analysis technique or tool and deems it most appropriately used in non-production environments and work systems (Bahr, 2015). The suggestion is that the process of test safety be considered for use in research and development settings.

With this quick overview of the various tools available to us as system safety engineers, one can quickly realize the need to understand a work system well enough to recognize when to attempt to conduct specialized safety analysis on a work system and when to call in specialists to do so. As with most graduate-level learning, the true intended knowledge outcome is one's ultimate ability to recognize personal skill sets and when to employ the skill sets of others. This becomes paramount in system safety management. What you will do through the rest of this course is learn to study a given work system, understand the work system well enough to know what safety analysis tool needs to be deployed, identify where and how to collect the data necessary to deploy the safety analysis tool, evaluate risks, and then effectively manage those risks with engineering and administrative controls. This is applied system safety management, through system safety engineering.

References

Bahr, N. J. (2015). *System safety engineering and risk assessment: A practical approach* (2nd ed.). Boca Raton, FL: CRC Press.

Goetsch, D. (2015). *Occupational safety and health for technologists, engineers, and managers* (8th ed.). Upper Saddle River, NJ: Pearson.

Hammer, W., & Price, D. (2001). *Occupational safety management and engineering* (5th ed.). Upper Saddle River, NJ: Prentice Hall.

Leveson, N. G. (2011). *Engineering a safer world: Systems thinking applied to safety*. Cambridge, MA: Massachusetts Institute of Technology.

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

Suggested Reading

In order to access the following resource, click the link below.

In this unit, you investigated different qualitative and quantitative tools available to safety engineers. We also discussed the importance of learning to recognize when to select and deploy which available tool depending on the work system and specific scenario. This article is related to mineral mine development and operation, but it may be beneficial for you to consider which tools were selected for specific tasks related to the entire mine development and operations by work system phases. Specifically, you may appreciate Tables 1 and 2 within this article.

Moraru, R. & Popescu-Stelea, M. (2016). Risk assessment traits in various mine operation stages. *Revista Minelor/Mining Revue, 22*(4), 31-36. Retrieved from https://libraryresources.columbiasouthern.edu/login?auth=CAS&url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=120550212&site=ehost-live&scope=site

Learning Activities (Nongraded)

Nongraded Learning Activities are provided to aid students in their course of study. You do not have to submit them. If you have questions, contact your instructor for further guidance and information.

Calculating the Human Reliability Probability Value for a Work System

Carefully reread the Unit V Lesson material related to calculating the human reliability probability as well as the textbook discussions on pages 236 and 241. Now set up a work system in your kitchen using plastic cups and your tap water. Set out ten empty plastic cups along a clear space on the counter or on a table. Now, hold an additional empty cup in your hand—this makes 11 cups, total. Your work system will be filling the ten empty plastic cups as fast as possible, with no spillage on the counter or table surface.

Step 1: Using the additional empty cup, do the following tasks as fast as you can.

a. Turn on the cold tap water from the kitchen sink. Do not use hot water, as you could burn yourself.
b. Fill the additional empty cup with cold tap water.
c. Turn off the cold tap water.
d. Fill an empty cup, one of the ten, from the additional cup and tap water.
e. Repeat steps a through d, filling all ten empty cups with cold tap water and turning off the kitchen tap between fillings.

Step 2: Using a pen and paper, do the following.

a. Record the number of errors like spillage while filling a cup.
b. Record the number of opportunities for errors, assumedly ten, one for each empty cup.
c. Calculate the human error probability.

Step 3: Calculate the human reliability probability for this work system.

Step 4: Theorize both engineering and administrative controls to decrease the impact of the human reliability probability on the affected work system.