Understanding System Safety

Hazards are ever-present in the steel plant environment, and a heightened awareness and emphasis on safety is a necessary priority for our industry. This monthly column, coordinated by members of the AIST Safety & Health Technology Committee, focuses on procedures and practices to promote a safe working environment for everyone.

Author

Malcom Dunbar
President, MDSC LLC, Detroit, Mich., USA

Comments are welcome. If you have questions about this topic or other safety issues, please contact safetyfirst@aist.org. Please include your full name, company name, mailing address and email in all correspondence.

The steel industry is full of complex systems and risk. With systems and technology comes exposure to incidents because systems can fail or not work as designed, which could lead to property damage, personal injury and even death. The systems in ironmaking, steelmaking, hot rolling, cold rolling, transportation, maintenance and others each have unique designs and components and thus create a multitude of different potentials for things to go wrong.

On any given day, workers interact with these systems with the goal of completing their assigned tasks in the most safe and efficient manner. Every activity involving a human has a hazard associated with the task. Some the most common hazards are working with heavy mobile equipment, excessive heat, working with molten metals, energy (electrical, mechanical and chemical), confined space and working at heights, to name a few. Evaluating the potential of these systems to fail in a manner as to cause a personal injury or property damage is critically important. The tools of risk assessment when properly and systematically applied can be most effective in identifying the hazards so they can be eliminated or controlled before an incident occurs.

Looking at the historical safety performance of the industry reveals statistics showing a continuous improvement such that days away from work restricted time (DART) and total recordable rate (TRIR) decrease. Unfortunately, despite all the progress made within the industry, the potential for catastrophic system failures still exists, which may lead to serious property damage and/or injuries. This is the reason why taking a step back and looking at the system from a safety perspective is important. Assessing an entire process, the system and subsystem, is known as system safety.

The ideal objective of system safety is to develop a system with the hazards eliminated or controlled to an acceptable risk level. Many organizations have adapted a statement or slogan of absolute safety — or a goal of zero — however, absolute safety is not possible, especially when dealing with complex systems. The more complex the system, and the more human interactions required, the more difficult it is to gain a system free from all hazards and risk. A more realistic goal is having a system with acceptable risk which is defined as the probability of a hazard-related incident or exposure occurring as low as reasonably practicable (ALARP).

An example of this concept is the United States' current traffic system. Driving a vehicle from one point to another has risks associated with it. Despite all the efforts of the traffic highway system designers, the automotive industry, the skill and experience of drivers and the professionals who police the traffic system, there are still hazards and risks which lead to over 40,000 fatal traffic incidents every year.

The conclusion could be made that driving personal vehicles is too risky based upon the large number of fatal incidents. Every year, 3.2 trillion miles are driven and it becomes reasonable to assume the risk of personally getting involved in a fatal traffic incident is statistically very low. Driving risk is something that one doesn't give a second thought and accepts this risk daily. This is an example of a system with risk being ALARP.

Figure 1

System safety process (SSP) flow chart.

Defining System Safety

The concept of systems safety has been around since the start of time. One of the first formal system safety risk assessments came to the forefront in London with Edward Lloyd in 1687. It was Lloyd of London, with help from others, who started assigning risk profiles to the shipping industry while relying upon the reports from ships' captains for the identification and potentiality of hazards in the shipping lanes. System safety risk assessment was formalized with the splitting of the atom during World War II, which was subsequently made into a weapon of mass destruction. Having this type of a weapon in the arsenal meant accidental system failure was not an option. The military needed a more robust system safety risk assessment to seek out hazards and eliminate or control them before a catastrophic weapon system failure occurred. This led to a formal system safety which was established by the U.S. Department of Defense and codified into a document entitled MIL-STD-882. Even after years of innovation, this critical work remains the basis for system safety assessment even today.

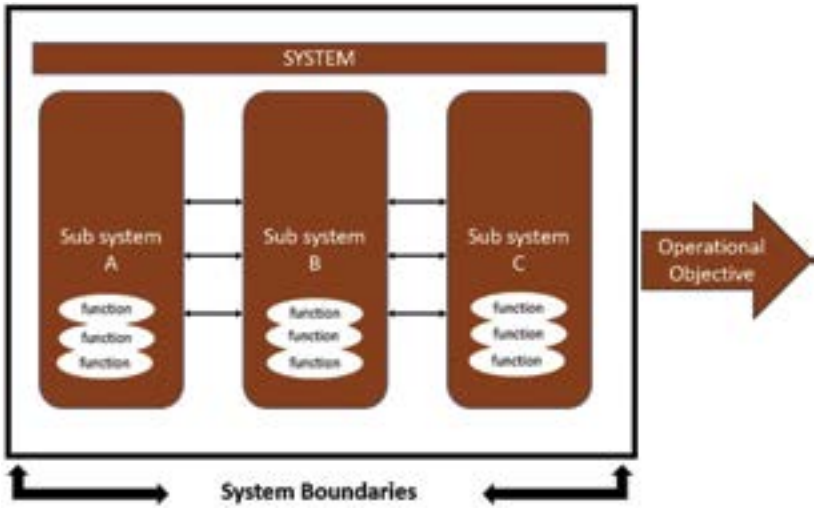
System safety as defined in MIL-STD-882 is: "The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time and cost, throughout all phase of the system life cycle." It involves planning, organizing and controlling the efforts directed toward looking at the system to determine potentially what can go wrong and to eliminate that potential or putting in a control to mitigate the effects should it fail.

The system safety process (SSP) works in the following order (also shown in Fig. 1):

1. Develop a plan of action: who, what, when, where and how.
2. Identify and review the potential hazards present in the system.
3. Assess these potential hazards and determine how serious these hazards could be if they transitioned to a failure.
4. Identify and install safety measures to eliminate or mitigate identified hazards.
5. Re-assess the system to evaluate the elimination and mitigation effects to identify residual risk remaining in the system.
6. Determine what problems may still exist and is the residual risk level acceptable.
7. Present the findings to the organization highlighting the residual risk remaining.
8. Collect data on hazards, mitigation strategy to share with others as a continuous learning loop and close out the analysis.

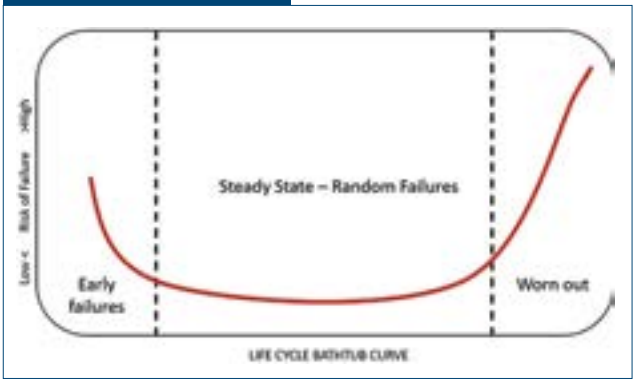
For system safety to be effective, one must first understand the system and how it operates. In its

Figure 2



The MIL-STD-882 system chart.

Figure 3



Life cycle of a system, illustrated in a bathtub curve.

most basic form, a system is a combination of subsystems interconnected to accomplish an objective. The MIL-STD-882 definition of a system is (also shown in Fig. 2): "A system is a composite, at any level of complexity, or personnel, procedures, material, tools, equipment, facilities and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support of mission requirements."

System Life Cycles

The best time to perform a system safety analysis is during the concept and design phases of building the system. The obvious reason for this is change can be made more efficiently and cost effectively. The further along in the life cycle, the harder and more costly it is to make a change. Although the concept and design phases are the ideal time, many system safety assessments are completed after a system is fully installed and operational.

In fact, most system safety assessments are completed during the operational phase in response to property damage or personal injury incidents. System life cycles are defined as having five distinct phases:

- Phase 1 — Concept phase where the overall goal and objective of the system are determined.
- Phase 2 — Design phase where design, development and testing of component subsystems occurs before they are installed into a system. This is often broken down into various subphases such as:
  - Preliminary design phase.
  - Detail design phase.
  - Test phase.
- Phase 3 — Production phase when the actual system is being put into place.
- Phase 4 — Operational phase when the system is in actual use fulfilling its objective.
- Phase 5 — Disposal phase is an often-overlooked time when the system is being dismantled.

A visual way to show life cycles is often used by Six Sigma/total quality control managers when engineering system reliability models. The most common visual is the bathtub curve, which highlights the potential failure rate along the life cycle of the system. As shown in Fig. 3, most system failures occur either early in the life of the system, or after the system is worn out and nearing disposal. For reliability managers, failures are lost time, high cost and inefficiency. For safety professionals, failures mean property damage and injury incidents.

A system safety assessment can be performed at any time during the life cycle. As stated, it is always more efficient and cost effective when in the earliest phase or concept and design. The phase of the assessment will determine what assessment types and techniques are the most effective.

Figure 4

Type	Description
CD-HAT	Conceptual design phase – is a high level (low level of detail) assessment which identifies top level potential hazards
PD-HAT	Preliminary design phase – a low level of detail assessment designed to obtain an initial assessment of the system design
DD-HAT	Detailed design phase – a more detailed assessment which assess the potential hazards identified in the PD-HAT
SD-HAT	System design phase – looks at the entire system taking the DD-HAT into consideration. Important for system and sub-system interfaces
OD-HAT	Operational design phase – starts the assessment of critical system operations as well as support functions such as maintenance, training, material handling, etc.
HD-HAD	Human design phase – is an assessment of the health and human exposure hazards associated with the operations of the system
RD-HAT	Requirements design phase – is an assessment to verify the safety requirements are in place and effective as it applies to the hardware, software and system test requirements

Seven types of analysis matching up to the life cycles.

Assessment Types

In the process of system safety, there are two interconnected terms which have different meanings: types and techniques. Types take into consideration where the system is in its life cycle. That is an important consideration when assessing risk and the type

of assessment needed. Once the type is chosen, the technique is determined. The technique is matched to the type, and it becomes the actual tool the risk assessment team uses to perform the assessment.

There are seven types of analysis matching up to the life cycles. It is important to know the type of analysis being performed to match the proper technique. Although most all the techniques follow the basic cadence of plan, assess, identify, eliminate or mitigate, review residual risk for acceptability, document and communicate, some of the techniques are more detailed than others and each has some unique characteristics. The seven basic types are shown in Fig. 4.

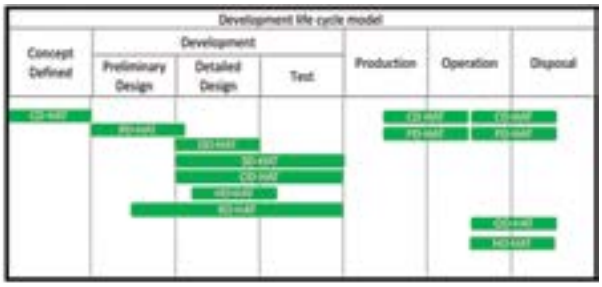
The overall goal of the system safety types is determining the proper technique to use and to ensure there are overlapped assessments so there are no gaps present in the analysis. Pure overlap happens best when assessment of the system starts at the very beginning of the project (concept and design), but also it can be just as effective later in the life cycle. Matching the various types up to the system life cycle would look like what is shown in Fig. 5.

Assessment Techniques

Once the type of assessment is determined, the next step would be to determine the technique to be used. In the risk assessment world, there are well over 100 various risk assessment techniques available. Each one of them share common characteristics but they also have their own distinct characteristics depending on the needs of the assessment team. The task is to pick the technique matching the type required as well as the time and skill level of the assessment team. Here are some of the major characteristics of assessment techniques to consider before choosing which one(s) to use:

- Complexity — Some of the techniques can be quite complex to use.
- Cost — One must be prepared to accept the cost of doing the assessment, which can vary depending upon the technique.
- Data required — This is an important area to watch for, as sometimes there is a large volume of data and other times there is not.
- Difficulty — As with complexity, some of the techniques can be difficult to use.
- Expertise — Some techniques are intuitive, but many require the assessment team to have the training and expertise on using the technique.
- Inductive or deductive — Most of the time when a system is up and running and an incident occurs, it is best to work from the existing system down into the subsystems (deductive); otherwise you are starting from design documents and moving forward (inductive).
- Level of detail — Some techniques provide a high degree of detail while others do not.
- Program timing — How fast the project is moving is a key factor to consider to ensure the team has the time to perform the assessment.
- Qualitative or quantitative — Most assessments are qualitative, but there are several that are both qualitative and quantitative.
- Time required — Some of the techniques take more time than the others, so time available and time of assessment must be matched.
- Tools required — Many of the techniques stand alone in their use while others require additional tools to be effective.

Figure 5



Development life cycle model.

Choosing the proper risk assessment technique can seem like an overwhelming task, but by following the guidelines above and with a little help from risk assessment professionals, it can be narrowed down to a few. A point to remember is that no one assessment tool will reveal all the potential hazards and risk in a system. Rather it is best to use multiple tools which overlap in their coverage to get a complete view of the system including the subsystems and their interactions. Fig. 6 shows an example of matching the type to the technique.

Documentation and Communication

The documentation of the system hazards is to be completed in the form dictated by the technique used. Often a simple Microsoft Excel spreadsheet can be used to document the findings and the elimination and mitigation efforts. If doing a qualitative analysis, the outcome could be as simple as Risk = Probability x Consequence. Should the goal be a quantitative analysis requiring a risk probability assumption, there will be a need to determine that probability on a numerical basis. The problem with probability is there are basically two ways look at the subject.

Figure 6

Example of Matching the Assessment Type to the Technique

Type	Coverage	Focus	Technique
CD-HAT	Conceptual Design	System hazards	PHL – Preliminary Hazard List
PD-HAT	Preliminary Design	System hazards	PHA – Preliminary Hazard Analysis
DD-HAT	Detailed Design	Subsystem hazards	SSHA – Sub System Hazard Analysis
SD-HAT	System Design	Integrated hazards	SHA – System Hazard Analysis
OD-HAT	Operational Design	Operational hazards	O&SHA – Operations & Support Analysis
HD-HAT	Human Health	Human health hazards	HHA – Human Health Assessment
RD-HAT	Requirements	Requirements / testing	SRCA – Safety Requirements Criteria Analysis

Example of matching the assessment type to the technique.

First, the math associated with doing a probability calculation is well settled, but the philosophy of the probability is most often variable. A good example is doing a probability estimate of lightning striking a worker who is assigned to do work outside. The one way to approach this would be to study the lightning strikes in the general area in which the worker will be assigned, as well as similar work done by others. Armed with this data, the assessment team would work with stated history and facts from previous strikes to determine the probability of future strikes.

The more philosophical way is to think about the potential of lightning striking anywhere at any time, which is often the case with lightning, as it can be unpredictable. Whether to use known historical or theoretical philosophical data can create quite the discussion within a risk assessment team. Either way, there are some great techniques such as Monte Carlo analysis and others which can help with the probability issue. Regardless of the type of assessment, these are the various types of issues the assessment team would need to work out internally.

A key goal for the team is to first understand the data and then be able to communicate it to the public. Often risk assessments are too detailed and complex for the average person to gain an understanding of the process and/or the outcome. Historically, this is one of the reasons many organizations shy away from doing an assessment in the first place. They assume it is too complex. With time, attention to detail, and working the process step by step, even the most unexperienced team can have tremendous success following the guidelines provided with the various techniques available today.

Regardless of the type of technique used, the outcome must be communicated to the organization in a clear and easily understood way, especially regarding residual risk. As mentioned, ALARP does allow for acceptable risk to remain, as this risk is generally accepted to be as low as possible but it is still risk and many will not understand why it remains. The goal of the team when reporting their findings is to highlight this residual risk and explain why it is as low as practical.

Conclusions

Risk assessment is a systematic process for identifying and describing potential hazards, and the likelihood and magnitude of risk which can be eliminated or controlled before a serious incident would occur. It can be used by a small group of people in doing their everyday job tasks or in the case of a complex industry such as steel manufacturing where it is good to do on a system level. System safety is all about seeing the big picture, recognizing that systems are designed by humans to work with humans, and that both humans and systems are not perfect. Systems can have design flaws which would show up early in the system operations, or later as it gets worn down and near the end of its expected life. Performing a system safety assessment can be done at any time in its life cycle with the more efficient and least cost being during the concept and design phase. A key indicator as to what technique to use for the assessment depends upon where the system is in its life cycle. This is where identifying the type comes in handy. Knowing the life cycles and matching the technique it to the right type will lead to the best outcome. Once the assessment is completed, the last major component is the communication. It is a critical part of every risk assessment as it tells a

story what was found, eliminated, or mitigated and what residual risk resides. System safety is available to the steel industry and should be used both when new operations are being designed and put into service as well as when existing operations age.

References

1. F.E. Bird, G.L. Germain and M.D. Clark, *Practical Loss Control Leadership rd Edition*, Det Norske Veritus USA, 1985.
2. C.A. Ericson, Hazard Analysis Techniques for System Safety, Wiley-Interscience, 2005.
3. MIL-STD-882E, Department of Defense, Review: https://www.dau.edu/cop/armyesoh/DAU%20Sponsored%20Documents/MIL-STD-882E.pdf, August 2022.
4. L.T. Ostrom and C.A. Wilhelmsen, *Risk Assessment Tools, Techniques, and Their Applications*, Wiley, 2012.
5. C. Yoe, *Principles of Risk Analysis – Decision Making Under Uncertainty*, CRC Press, 2012. ✦