SIS-TECH
12621 FEATHERWOOD, STE 120
HOUSTON, TX 77034
713-909-2100

Process Automation Reliability vs. Safety:

Is It Possible to Have Safe Systems That Aren't Considered Reliable?

By William L. Mostia, PE. Published in *Control,* April 2014

Noted and well-respected safety guru and author of Engineering a Safer World, Nancy Leveson, once stated in a presentation on "The Path to More Cost-Effective System Safety" that reliability does not equal safety: Reliability ≠ Safety. This is based on the observation that many accidents occur without any component or equipment hardware or software failure, leading to the conclusion that systems of highly reliable components or equipment alone are not necessarily safe. She also said that complexity compounds this issue.

So how does this statement relate to the process industries? Reliability and safety are many times treated differently, as if they're dissimilar concepts or philosophies. It seems certain that we want a reliable and safe plant, but how do these concepts interact in a process plant?

How Do You Define Reliability?

Reliability as a plant function depends somewhat on one's perspective and goals. Reliability from the perspective of the maintenance department may not be the same as reliability in the process safety management (PSM) or engineering departments.

Reliability can be defined as the probability that an item will perform a required function under given conditions for a given time interval. Reliability is commonly associated with process equipment (pumps, compressors, vessels, pipes, etc.). It resides in the maintenance department, whose goal is to reduce cost of maintenance and improve process uptime to increase the company's bottom line.

Computerized maintenance management systems (CMMS) are used to record, manage and communicate day-to-day operations and implement various reliability-based maintenance models. One common maintenance management system is reliability-centered maintenance (RCM). Some of the other maintenance management strategies that incorporate reliability are asset integrity management (AIM), reliability-based inspection (RBI) and reliability, availability and maintainability (RAM). The British standard PAS 55, soon to be ISO 55000, provides a benchmark for these types of systems.

While safety is a consideration, risk-based maintenance management system goals typically identify critical equipment, and allocate maintenance resources to improve their reliability, while allowing other, less critical systems to operate until failure, in effect doing the safe minimum maintenance to preserve the functions and integrity of physical assets. This way, reliability may be used as a cost-minimization process, allocating resources based on risk.

The connection of these systems with PSM may be somewhat tenuous, as they typically reside

in different departmental silos, but there seems to be a growing awareness that process safety should be more intimately connected to asset reliability management and vice versa.

Reliability from the PSM perspective consists of meeting required reliability of the safety instrumented systems (SISs), such as using safety integrity levels (SILs) and more recently emphasizing the reliability of non-SIS independent protection layers (IPLs). Some people also view safety as a cost-minimization process based on risk. So if they do the minimum necessary to achieve what was determined in their layer of protection analysis (LOPA) or equivalent risk evaluation methodology, and the minimum they can do to meet the safety standards, then they have achieved "safety."

The problem is that safety is not a minimization process. Would you do a minimum repair job on the brakes of your family car? Doing the minimum to achieve an acceptable level of "safety" implies perfect knowledge of the risks and systems involved. It is hubris to claim or even imagine that we can do this. This philosophy can also lead to a lack of system robustness and resilience, resulting in a fragile system prone to safety incidents.

Capital projects, however, often are driven by cost and schedules and less by lifecycle considerations, such as reliability. Reliability from a project engineering perspective involves implementing SIS to meet SIS-reliability targets, providing adequate equipment by sparing and purchasing equipment per a company-approved vendor list. While maintenance department reliability engineers may participate in projects, it is less common to have a reliability function as part of the project engineering team. This is more commonly left to the individual design engineers.

Reliability has different measures to indicate properties of interest, such as availability, unavailability, probability, failure rates, etc. Reliability in a plant is typically tied to availability, for example, percent uptime for equipment and unavailability for safety systems. Availability can be defined as the probability that the equipment is operational at any moment in time. Unavailability is the converse—the probability that a system will not successfully carry out its function when required.

Reliability and the I&C Engineer

Instrument and control systems reliability has lagged behind their mechanical brethren, perhaps due to complexity and the daunting number of instruments in typical facilities. With the introduction of digital communications, which allow instruments to transmit health and remote access to instruments, asset management systems (AMS) have become more practical and popular. In 2012, the Instrument Reliability Network (on LinkedIn at Instrument Reliability Network–Public Forum) was formed at the Mary Kay O'Conner Safety Center at Texas A&M University to address instrument reliability issues and collection of instrument failure rate data.

This is a consortium of companies coming together with a vision to benchmark current performance of instrumentation and controls in process industry applications, define a common failure taxonomy to support consistent collection of quality data from maintenance and proof-test activities, and share lessons learned in improving instrumentation.

Control system availability is related to equipment and functional reliability. While higher-level control equipment can contribute to downtime, control system availability is a function of the cumulative availability of the individual loops in the system, which depends in part on the

reliability of the loop equipment hardware. It's also a function of the unavailability of the loop functionality, such as the time in manual, in bypass, bad tuning and systematic errors that lead to loss or degradation of loop functionality, etc. If you're running control valves with their bypasses open, have out-of-tune loops, are not keeping up with your instrument maintenance due to poor management, lack resources due to budget cuts, you might also be suffering from a lack of availability. Human beings are often expected to fill gaps in control systems lacking availability, but they can have varying degrees of success.

Free from Danger, Risk or Injury

Safety can be defined as the condition of being free from danger, risk or injury. Process safety management can be defined as the control of recognized hazards to achieve an acceptable level of risk to people.

One of OSHA 1910.119 PSM regulation's 14 elements is mechanical integrity—to ensure that critical process equipment is designed and installed correctly and operates properly. This sounds like reliability is probably in there somewhere, but you will probably not find a reliability engineer on the PSM staff nor a PSM engineer on the maintenance staff, and maybe not even cross-pollenization of duties. Hopefully, there will be some direct coordination between these functionalities to assure that safety-critical equipment is reliable and is maintained appropriately.

How else are safety and reliability related? Is it possible to have safe systems that aren't considered reliable? Due to redundancy designs to achieve high safety reliability (e.g., 1oo2), the reliability equation has minimization of the potential unavailability of the safety system as a primary consideration, with process availability secondary. Safety systems will not be considered "reliable" if they trip often and cause process outages, but this is many times a function of poor design rather than any inherent limitation of safety in regards to reliability.

Safety in a process plant is generally divided into worker safety (e.g., reduction in lost-time accidents and recordables) and process safety (e.g., reducing the risk of a loss-of-containment (LoC) event). People safety is improved by reliable equipment by reducing the man-machinery interaction. With the introduction of LOPA in the late 1990s, emphasis has been placed on independent protection layers (IPLs), which can include instrumented and non-instrumented systems. Emphasis has been largely on safety instrumented systems to reduce the risk of an LoC event.

The importance of other non-SIS IPLs has come to the forefront recently, along with the realization that reducing the frequency of initiating causes (i.e., reliability) provides a practical reduction in risk (i.e., fewer demands on the safety systems equals fewer potential incidents). The Center for Chemical Process Safety (www.aiche.org/ccps) has published a book on the subject, "Guidelines for Independent Protection Layers and Initiating Events". In addition, the S84 committee has recognized that instrumented protective systems other than SIS play an important part in process safety and has moved to address them in the ANSI/ISA-84.91.01-2012 standard, "Identification and Mechanical Integrity of Safety Controls, Alarms and Interlocks in the Process Industry."

It seems fairly obvious that safety systems should be reliable, or at least tolerate faults or failures. From the design perspective, improving reliability can be considered an inherent safe design principle. Essentially, the more reliable a facility is, the safer it is.