Process Automation Reliability vs. Safety:

Noted and well-respected safety guru and author of "Engineering a Safer World," Nancy Leveson, once stated in a presentation — "The Path to More Cost-Effective System Safety" — reliability does not equal safety. This is based on the observation many accidents occur without any component, equipment hardware or software failure, leading to the conclusion systems of highly reliable components or equipment alone are not necessarily safe. So how does this statement relate to process industries? We certainly want a reliable and safe plant, but reliability and safety are many times treated differently as though they're dissimilar concepts or philosophies. How do these concepts interact in a process plant? Is it possible to have "safe" systems that aren't considered reliable?

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 an item will perform a required function under given conditions for a given time interval. Reliability is commonly associated with process equipment — e.g., pumps, compressors, vessels, pipes, etc. The process availability metric often resides in the maintenance department, whose goal is to reduce the cost of maintenance and improve process uptime, increasing the company's bottom line.

Safety is defined as freedom from unacceptable risk. Safety in a process plant is generally divided into worker safety — i.e., reducing lost-time and recordable injuries — and process safety — i.e., reducing the risk of a loss of containment (LoC) event. People safety is improved by having reliable equipment reduce the man-machinery interaction. PSM attempts to control recognized hazards to achieve an acceptable level of risk to people. Process safety is improved by a combination of inherently safer process designs and functional safety provided by safeguards.

Reliance has been chiefly dependent upon safety-instrumented systems to reduce the risk of an LoC event. The importance of other instrumented safeguards has come to the forefront recently, along with the realization reducing the frequency of initiating causes — i.e., reliability — provides a practical reduction in risk. Fewer demands on the safety systems equal fewer potential incidents. The Center for Chemical Process Safety, www.aiche.org/ccps, published a book on the subject in 2014: "Guidelines for Independent Protection Layers and Initiating Events." In addition, the ISA 84 committee has recognized all instrumented safeguards play an important part in process safety and has included them in the ANSI/ISA-84.91.01-2012 standard, "Identification and Mechanical Integrity of Safety Controls, Alarms and Interlocks in the Process Industry."

For safety reliability, the primary consideration is minimizing the potential failure on demand of the safety system, with process availability as a secondary objective. One of OSHA 1910.119 PSM regulation's 14 elements is mechanical integrity to ensure critical process

equipment is designed and installed correctly and operates properly. This sounds like reliability. However, you will probably not find a reliability engineer on the PSM staff or a PSM engineer on the maintenance staff, although there should be substantial interaction between them. Nevertheless, safety systems will be considered neither “reliable” nor “safe” if they often trip up and cause process outages. This problem is often a function of poor system design rather than any inherent limitation of safety equipment with regard to reliability.

Although other causes of incidents may predominate, it seems fairly obvious safety systems should be reliable or at least tolerant of faults or failures. Preferably direct coordination will develop between reliability and PSM organizations to assure instrumented safeguards are reliable and maintained appropriately. Improving reliability is considered an inherently safer design principle. Essentially, the more reliable a facility is, the safer it is.

For more information, visit www.sis-tech.com or call (713) 909-2122.

By: WILLIAM “BILL” L. MOSTIA JR., P.E. and Fellow SIS-TECH Solutions