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 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. So how does this statement relate to the process industries? It seems certain that we want a reliable and safe plant but reliability and safety are many times treated differently, as if 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 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.). The process availability metric often resides in the maintenance department, whose goal is to reduce 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 (e.g., reduction in lost-time and recordable injuries) and process safety (e.g., reducing the risk of a loss-of-containment (LoC) event). People safety is improved by reliable equipment through reducing the man-machinery interaction. Process safety management 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 design and functional safety provided by safeguards.

Reliance has been chiefly on safety instrumented systems to reduce the risk of an LoC event. The importance of other ~~non-SIS~~instrumented safeguards 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. That is, fewer demands on the safety systems equal~~s~~ fewer potential incidents. The Center for Chemical Process Safety (www.aiche.org/ccps) ~~has~~ published a book on the subject in 2014, "Guidelines for Independent Protection Layers and Initiating Events". In addition, the ISA ~~S~~84 committee has recognized that all instrumented ~~protective systems~~safeguards ~~other than SIS~~ 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 minimization of 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 that critical process equipment is designed and installed correctly and operates properly. This sounds like reliability, but you will probably not find a reliability engineer on the PSM staff nor a PSM engineer on the maintenance staff although there should

be substantial interaction between them. Nevertheless, safety systems will not be considered either "reliable" or “safe” if they trip often and cause process outages. This problem is many times a function of poor system design rather than any inherent limitation of safety equipment in regards to reliability.

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

~~At SIS-TECH Solutions we invite you to contact us to chat about both your process automation reliability and safety needs. Our team of on-staff experts have combined decades of experience. At SIS-TECH we are Proven-in-Use®™.~~

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