

Selection of an SIS for Maximum Process Availability

By Buddy Creef

Vice President, Safety Systems

RTP Corporation

Since the first safety systems were introduced, users have had to balance safety vs. availability. Since industry experts recognized that the safe state had to be a de-energized state whenever possible, any fault in the safety loop would generally result in a trip to the safe state. Often times, these trips were the result of spurious operation of the relays that made up the first safety systems or of the initiators or actuators monitored and controlled by those relays. Thus was born the concept of nuisance trips. From then until now, there would always be a trade-off between safety and availability.

In many instances, relays were replaced by PLC's, which experienced fewer nuisance trips and, therefore higher availability. Simplex PLC's were replaced by redundant PLC's, which were eventually replaced by Triple Modular Redundant Systems, essentially triplicated PLC's. In every case, process industries opted for improved operational availability, essentially a decrease in nuisance trips, assuming that safety was not compromised.

Early in the 21st century, a flurry of new SIS systems was introduced. Interestingly, there was no consensus on the configuration as far as redundancy or availability is concerned. Thus it is left to then end user to determine the importance of availability in each application and how the desired availability will be achieved.

If we assume that the primary purpose of an SIS is to take the monitored process to a safe state whenever a potentially unsafe situation is observed, we might make its second objective to never interfere with the operation of the process at any other time, thus achieving maximum availability. In order to achieve this second objective, the user needs to minimize or eliminate all conditions that would result in the SIS taking the process to a safe state when the process is running safely.

While this sounds simple, different safety systems on the market today will provide vastly different capabilities in meeting this objective. The educated user will find that there are vast differences between even relatively "new" safety systems in this regard, and that the selection of a state of art SIS designed to provide maximum process availability will return dividends that justify its selection.

Let's turn our attention to the factors that figure into meeting those two objectives.

The two primary Objectives of an SIS:

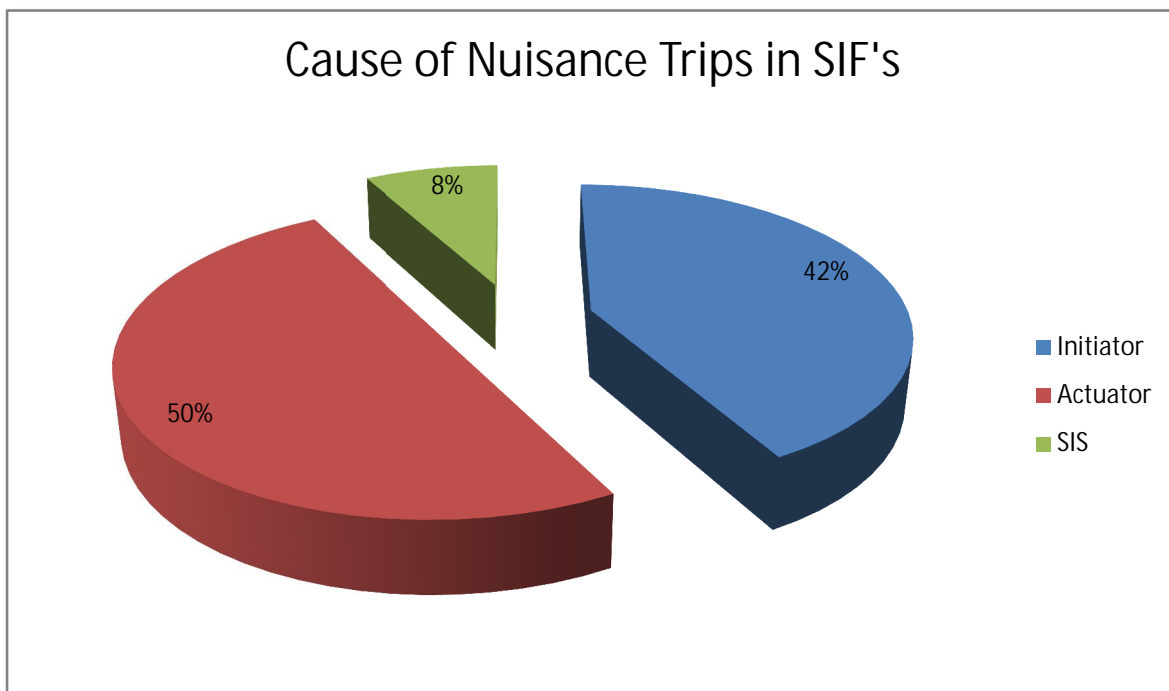
1. Take the monitored process to a safe state when a potentially unsafe situation is observed.
2. Never interrupt the process at any other time.

Nuisance Trips

The first thing that should be considered when availability is discussed is nuisance trips. Nuisance trips are normally associated with MTTFS or Mean Time to Fail Spurious (or Safe). MTTFS is really a measure of how often the SIS will take the process to a safe state without being instructed to by the instruments in the SIF. These numbers are usually readily available from the SIS manufacturer or from available documentation. But even though they are easily obtained, many users do not take these numbers into account when selecting an SIS.

Most users generally consider nuisance trips to be functions of the initiator and/or the actuator in a SIF. In fact, about 92% of nuisance trips are caused by initiators and/or actuators and 8% of nuisance trips are caused by the SIS. If the SIS causes 8% of those trips and that 8% can be reduced significantly, the impact to the bottom line of an enterprise can be sizeable. The typical MTTFS of a safety system could be 200 years, but some current state of the art systems exhibit MTTFS numbers an order of magnitude better than that. Processes protected by these state of the art systems would experience a 90% reduction in nuisance trips attributable to the SIS or a 7% reduction in overall nuisance trips.

One plant in Southern Ohio reported 300 nuisance trips per year. If 8% of those are associated with the SIS and if the SIS-caused nuisance trips are reduced by 90%, these 300 nuisance trips would be reduced to 279. How much extra profit would this plant make if it experienced 21 fewer nuisance trips in a year? While this is an extreme example, it does demonstrate a basic truth that many end users have lived with this issue so long they do not believe it can be remedied.



Nuisance trips are generally a function of the MTTFS (Mean Time to Fail Spurious or Safe) of the SIS and the other components installed in the SIF (Safety Implemented Function). Quite often users do not consider MTTFS when selecting a SIS even though it is a predictor of nuisance trips and, thereby, has major impact on the productivity and profitability of the operating unit. This is partially due to the fact that all MTTFS numbers seem adequately large. But it should be remembered that a system exhibiting an MTTFS of 2000 years will cause 90% fewer nuisance trips than one with an MTTFS of 200 years. Such differences will make their way to the bottom line and should be considered when SIS systems are selected.

Redundancy/Fault Tolerance/On-Line Repair

There seems to be a great deal of disagreement on the issue of redundancy in SIS systems. Most users would require it for SIL-3 applications, but most users don't have SIL-3 applications. If the standards can be met without redundancy, why spend the extra money for it, particularly if fault tolerance can be achieved without redundancy?

Let's return to the second objective of an SIS.

Never interrupt the process at any other time.

Does the lack of redundancy interfere with this objective? It would seem to. If there is no redundancy and there is a fault in the SIS, the process will be taken to a safe state causing lost production which, in turn, causes decreased profitability.

But, some SIS systems claim fault tolerance without redundancy. This would seem to imply that a fault in the SIS would NOT result in a shutdown of the process. Perhaps we should examine the term fault tolerance to see how it would apply to safety systems. The traditional definition of fault tolerance is the ability to complete a critical task in the presence of a fault. It was originally a computer term that referred to batch tasks in an IT environment. How does that apply to safety systems in the process industries?

What does ISA84 have to say about faults in an SIS? Checking with ISA84, Section 11.3.1, we learn,

The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem which can tolerate a single hardware fault shall result in either

- a) A specified action to achieve or maintain a safe state (see note) or:
- b) Continued safe operation of the process whilst the faulty part is repaired. If the repair of the faulty part is not completed within the mean time to restoration (MTTR) assumed in the calculation of the probability of random hardware failure, then a specified action shall take place to achieve or maintain a safe state (see note)."

So, if a fault tolerant device such as an SIS detects a dangerous fault, it can continue to operate for the designed repair time (MTTR). Therefore, if the fault tolerant SIS is repairable on line within the MTTR, the process will not be interrupted. If not, a process interruption must be scheduled

within the designed MTTR. So, fault tolerance without the ability to correct the fault on line only allows the user to schedule a shutdown. And, the shutdown must be scheduled within the MTTR, usually four to eight hours. So, fault tolerance without the ability to repair the fault online may require that the process be interrupted.

If the SIS is not redundant, even if it is fault tolerant, it cannot be repaired on line. So, simplex fault tolerant SIS's will cause a process interruption if they experience a fault, violating the second objective of an SIS.

Again, current, state of the art SIS systems can provide redundancy at reasonable prices and, with redundancy, offer the ability to repair any fault without interrupting the process, maintaining the ability to meet the second objective of an SIS.

On-Line Modification

SIL classifications of risks can be affected by updated PHA's, an individual plant's experience, or the experience of similar plants with similar applications. For these and other reasons, it is often necessary to modify an existing SIS.

It should be noted that modification of an SIS must comply with ISA84 and plant procedures. Proper testing and verification must be done to insure the intended operation of the SIS. This is true whether changes are made while the SIS is running or while it is offline. The user should be sure to do proper verification and documentation before making any changes to an existing SIS.

However, when the need for a modification is identified, the modification must be made expeditiously. In a continuous process, this would mean that the change cannot generally be delayed for the next turnaround. Even in a batch operation, depending on the length of the batch processing cycle or the time between batches, an SIS modification may have negative impact on productivity and, thereby, profitability.

Since these modifications must be made, the SIS must either be taken offline or modified online. Taking the SIS offline means either interrupting the process or leaving the process unprotected while the modifications are made, thus violating either the first or second objective that was set for an SIS earlier in this document.

Taking the process offline means reduced production and profitability. It may even mean making off-spec product during shutdown or start-up further affecting the profitability of the process. Leaving the process unprotected means additional operator oversight and hoping that the process doesn't experience a fault while the SIS is being updated. The best answer would be to employ an SIS that allows for unlimited online modifications, an ability that some current state of the art systems have.

Many SIS systems allow some online modification. Many older systems and even some relatively new ones use "change buffers" where the modified portions of programs can be stored. When online changes are made, a partial download is done, downloading the changes to the "change buffer". This works well until the "change buffer" is full. At that point, no more changes can be

made without powering down the SIS and doing a complete download of the program. This obviously means interrupting the process or leaving the process unprotected.

Making I/O configuration changes can be even more problematic. Many SIS systems limit the changes that can be made online. I/O may or may not be able to be reconfigured, added, or deleted. Remote chassis may or may not be able to be configured, added, or deleted. Again, if there is a requirement to make these changes, and they cannot be made online, the process will have to be interrupted or left unprotected, violating at least one of the objectives of an SIS.

However, newer technology third generation SIS systems allow for unlimited online changes. Complete program downloads eliminate problems associated with “change buffers”. Unlimited online I/O configurability eliminates the necessity of taking the process down to add, delete, or modify I/O points, modules, and/or chassis. All of this means less interruption of the process which means more productivity and profitability.

Conclusion

When selecting an SIS, the user should consider the impact that the SIS may have on the process it protects. One objective, certainly secondary to the objective of protecting life, property, and the environment, should be to interrupt the process as little as possible. No user wants to sacrifice or even risk safety for productivity, but if the selection of a state of the art safety system can insure safety and optimize productivity, it must be selected. In order to meet this objective, a number of attributes need to be considered. These include:

- Mean Time To Fail Safe (MTTFS) – an indication of the probability of a nuisance trip.
- Redundancy and the ability to do online repairs without interrupting the process.
- The ability to modify the SIS online without interrupting or otherwise affecting the process.

By considering all these issues, the user can meet the two objectives of a safety system.

Those objectives are to:

1. Take the monitored process to a safe state when a potentially unsafe situation is observed.
2. [Never interrupt the process at any other time](#)

About RTP

Founded in 1968, RTP Corp. is a developer and manufacturer of high-performance critical control and safety systems. RTP Corporation's products serve applications for both basic process control and safety systems. Markets for RTP's products include Refining, Upstream Oil and Gas, Chemical, Nuclear Power, and Glass Industries. RTP offers a wide range of rugged hardware and a complete suite of software for industrial control solutions that include seamlessly redundant and triplicated systems for mission-critical applications.

Buddy Creef is the Vice President of Sales at RTP Corporation. The insights reflected in this paper are the result of 25 years of experience dealing with process industry users in applications designed to protect their personnel, equipment, neighborhood, and environment.

Process Availability vs. SIS Attributes

