SIS TECH

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

SIS Management Part 4: Bypass Management

Eloise Roche, Senior SCAI Consultant, CFSE

A bypass by any other name is just as dangerous. Whether referred to as an inhibit, suppression, or forcing, the bypass of a safety system device or automated function nearly always means that this safeguard will no longer be able to provide the full degree of risk reduction and reliability it was specified to perform. Continued safe operation of that facility will usually depend on timely implementation of compensating measures to provide the risk reduction that was lost through the act of bypassing.

The predictable consequences of bypassing a safety instrumented system device or function lead to the following dual requirements for bypass management:

- *Features to prevent and alert unauthorized use (and other operator error)*
- *Highly effective management of change and access security controls.*

That is, written procedures documenting how and when a SIS bypass may be used, by whom, and for how long, are required, <u>but are not sufficient</u> to meet the requirements of the IEC-61511-1 standard. Regardless of how high quality the procedure is, nor how well trained the operator, a potential for human error will remain. For this reason, features that enable effective access restriction and otherwise protect against operator error using the bypass are required <u>in addition to</u> the management controls. In the correct use of bypasses during continued operation, alternative means of providing risk reduction (compensating measures) are used to manage the process safety risk gap created by the approved bypass activity.

Events that may trigger use of a bypass:

Typical hazard and risk analysis (H&RA) practices assume that safety controls, alarms, and interlocks (SCAI) will be in service nearly all the time, so the best situation is to not have bypass capability at all. Indeed, SIS are required to be designed in such a way that the need for using a bypass to continue operation while a SIS device or function is defeated is minimized. The justification for SIS bypasses should be periodically reviewed by facility management to ensure the removal of bypass features that no longer have sufficient reasons to exist. However, sometimes these piping and design features are needed in order to facilitate timely on-line preventative maintenance, proof testing, and repair of diagnosed failures. As a result of being part of a planned and scheduled activity, this kind of bypass use will usually occur during an inherently safer time (such as during a planned turnaround) or in an operating mode where compensating measures are available.

Unfortunately, not all bypass activity will be planned in advance. Suspected failure of a SIS device may create a demand for an on-line inspection and repair during continued operation. This potential SIS failure may be detected through poor performance of associated equipment. In this case, the actual cause of the deviant equipment behavior may not be immediately evident. Such an unplanned operating situation creates human factors that are far less favorable to successful execution of a complex task such as evaluating the safety of continuing operations. Fear of reprisal from leadership or peers for taking a too conservative approach, incorrect assumptions regarding the reliability of the information being presented on the automation system, and the simple desire to "do a good job" can combine during a crisis event to lead an otherwise experienced operator to bypass a safeguard at precisely the wrong time. Having detailed written bypass procedures that include clear instruction regarding the conditions a bypass may be safely used can address a portion of this risk.

Failures in bypass management procedure use:

"It ain't ignorance causes so much trouble; it's folks knowing so much that ain't so."

Josh Billings

Failures in procedure use mostly fall into the category of systematic error. That is, these are errors driven by human behavior, which cannot be predicted in the same manner as the random failure of devices. As a result, control of systematic error usually requires either prescribed design features or targeted management that involve independent people. An example of such a prescribed practice is the mandated involvement of an independent reviewer for any SIS change.

In the case of bypass management, an operator may attempt to perform a bypass at a time when it is quite unsafe to do so. This error in judgment may be made for many reasons. Some may be chronic reasons that should be caught and corrected during competency assessments. For example, a periodic assessment should identify whether the individual has sufficient training and experience to understand the severe consequence of using a bypass of a given safeguard at an inappropriate time.

However, some errors in judgment occur as the result of the operator having an inaccurate mental map of the process equipment at that particular point in time. In this kind of human error, the operator is certain that the situation is safe even when in fact it is not. The equipment may be in the wrong operating state, the compensating measures may not be available, or the operator may be attempting a bypass on the wrong piece of equipment entirely. In his or her mind, the operator is absolutely sure of being in the right place, attempting the right action at the right time. A simple example of this kind of error that many of us may be familiar with is the driver who upon approaching an intersection looks up and "sees" a green light when the light is actually red. Similarly, a driver may look over his or her shoulder in preparation for making a lane change and not realize that there is a car immediately adjacent in that lane. In psychological terms, these errors are the result of one or more types of cognitive bias. In effect, the person sees what they expect to see, and not the reality. Most people have likely experienced this kind of error personally at some point in their lives. Cognitive biases are a natural result of the kinds of shortcuts that the human brain routinely makes when managing the daily tasks of information processing and decision making.

For this reason, no amount of training can totally defeat human error driven by cognitive bias. Even the use of procedures that require documentation of current instrumentation readings may not be sufficient to overcome a strong cognitive bias, as the operator will likely interpret any information that is inconsistent with their current mental map as being the result of faulty instrumentation. While certain unfavorable human factors can make this type of error more likely to occur, no amount of favorable human factors can completely eliminate its affect on the behavior of an individual. An independent evaluation of the situation by a different person is required in order to detect and intervene in this kind of human error. Bypass access restriction features create an opportunity to catch and correct any error in judgment regarding the proposed bypass of a safeguard. However, the bypass access restriction implementation must be robust enough to enforce the engagement of a sufficiently independent second person.

Failures in bypass access restriction:

Unfortunately, access restriction features are not immune to systematic error either. Two of the more obvious systematic failure modes in bypass access restriction systems are:

- Insufficient control of the keys or passwords used in the access restriction system
- Insufficient training of the bypass approver

Is the lock on the front door of a home likely to be an adequate deterrent to theft if the key is left in the lock all the time? Would desirable cyber security results be expected if the password to a computer is written on a slip of paper and taped to the computer screen where anyone could see? The answer to these questions is obvious, but the need for restrictive management of SIS change keys and passwords can seem less clear initially. The operators, after all, are not thieves or saboteurs, but people honestly trying their best to advance the objectives of the plant in accordance with their training. Nevertheless, the purpose of access restriction is to enforce the involvement of an independent person who may see a problem with the proposed bypass that the initial operator may simply not see. If the means of gaining access is immediately available to the operator desiring to make a bypass, it will be a quite predictable practice for experienced operators to use those access keys on their own in order to meet the needs of the plant. In short, keys and passwords must be secure in order to remain effective.

Likewise, too much routine involvement between the bypass seeker and the bypass approver might result in a systematic error commonly referred to as group-think. The necessary task of the bypass approver is to take the role of an independent "devil's advocate". Is the bypass really *needed* right now? How do we know that the use of the bypass right now is safe? What evidence is there that the compensating measures are ready to take over for managing the risk? When the bypass requestor and approver are members of the same operating shift, it will be natural for the approver to develop a tendency to grant approval to the requestor based on a history of shared events and knowledge of the requestor's degree of experience without going through the extra work involved in performing a frank and independent review of current data. Unfortunately, if the approver simply hands over the keys to the requestor without performing the intended independent evaluation of the requested bypass, the access restriction system is broken. In addition, the societal dynamics between the requestor and the approver must be such that the approver will be likely to stop a bypass activity through refusing access in a situation that they evaluate as being currently unsafe. For this reason, the role of bypass approver is often reserved for senior management positions in the facility. It is essential, however, that the personnel granted this authority have the detailed knowledge of the facility installation and the associated hazards to be able to identify potential errors that might occur in the information being received from plant instrumentation, to accurately judge the safety of a bypass action at a particular moment in time, and to evaluate the likely effectiveness of proposed compensating measure for the specific situation at hand. Thus, competency assessments must be performed on those who are granted the authorization to approve a SIS bypass, and not just on the front line personnel who execute a SIS bypass.

Managing risk with an approved bypass:

Even if the use of a bypass is approved by an appropriately trained and independent person and access to use the bypass is provided to the operator, continued operation of the associated equipment during the bypass will not be sufficiently safe unless the risk reduction lost as a result of the safeguard bypass is replaced in some effective manner. This temporary implementation of a different method for managing risk while a SIS is degraded is called a compensating measure. Perhaps it involves dedicated personnel who will monitor sensing devices that are still active during the bypass and take manual action if needed. Perhaps there is an applicable independent interlock that exists as part of the normal process control strategy that will protect against the hazard but was simply not needed to fulfill the risk reduction requirements per the facility's risk criteria. In any case, in order to remain effective the compensating measures that will be used to manage the risk gap during a bypass operation must:

- Be effective against the hazard (i.e., fast enough, have an effective response action)
- Be explicitly included in the written SIS bypass procedures and as a result protected from unapproved changes
- Be included in an appropriate mechanical integrity or instrument reliability program

Summary:

The written bypass procedure provides necessary information to the operator, such as the correct way of using the bypass and expected restrictions for use. Operators must be trained on these procedures and the correct use of SIS bypasses should be included in the content of the periodic competency assessment required for operators performing safety lifecycle activities. However, the systematic conditions that usually surround the unscheduled use of a SIS bypass feature increase the probability that the operator may make an error in judgment regarding whether the use of the bypass is sufficiently safe. It is the effective implementation of access restriction that ensures there is the opportunity for independent confirmation of the appropriateness of the proposed bypass activity and for verification that compensating measures have been put in place prior to the impairment of the normal source of protection. For sustained effectiveness of the bypass management and countermeasure program, functional safety audits should ensure:

- Justification for bypass capability is reviewed on a periodic basis by management
- Keys and passwords are kept secure in order to remain effective
- Devices used for compensating measures are maintained and managed

Please visit this edition's Unsafe Automation Incident case study, to see an example of how failure in safety interlock bypass management led to a multiple fatality outcome.