EMERSON
Process Management

PlantWeb University

SIS 301 - Operation & Maintenance

15 minutes

In this course:

Overview

You don't really "operate" an SIS the way you operate a basic process control system (BPCS). That is, operators don't change setpoints or alarm values, tune loops, and so forth in an SIS.

That's because the BPCS is dynamic and constantly being operated to maximize production and quality. An SIS, on the other hand, is normally static, waiting patiently in the background until the process demands the quick execution of a pre-defined action to keep people and the environment safe.

Car enthusiasts might think of a BPCS as performing like an engine management system, making constant adjustments to improve ongoing performance. The SIS is more like an airbag, waiting invisibly until something goes wrong but always ready to act when required.

But the operations and maintenance phase is the heart of the SIS lifecycle, and your Operations and Maintenance teams will play an essential role — from reacting properly if the SIS is activated, to conducting periodic proof tests, to monitoring and maintaining the equipment.

That's why there needs to be more than a "here's your SIS" handoff from Engineering to Operations and Maintenance. Instead, a formal review of SIS design assumptions and considerations, as well as training on operating and maintenance procedures, is needed to help Operations and Maintenance personnel understand what they need to do to ensure that the SIS will work properly when it's needed.

To help you plan for these sessions, this course highlights some of the requirements IEC 61511 places on Operations and Maintenance teams to maintain the designed-in functional safety of the SIS throughout its installed life.

Hint

Pay special attention to:

- What topics should be covered in SIS operations and maintenance planning
- Why Operations personnel need to understand what the SIS does (and why it does it)
- The Maintenance team's primary responsibility with regard to the SIS
- How preventive maintenance can affect SIS reliability.

Planning

IEC 61511 requires that there be operations and maintenance planning for the SIS. This planning has two objectives:

- **proper maintenance** to ensure that each safety instrumented function continues to have its defined safety integrity level throughout its life, and
- **proper operations** to ensure that the SIS as a whole gives the required level of risk reduction.

The planning should cover such topics as…

- Routine operational activities, such as partial-stoke valve testing and full proof testing of all SIS components.
- Abnormal operational activities, such as what to do when an SIS transmitter fails or Maintenance technicians must work on an SIS block valve while production continues.
- What to do when automated testing detects an SIS device problem.
- SIS reset and restart procedures to use after a demand or a spurious trip — and the requirements for investigating, analyzing, and reporting such a trip.
- The requirements for identifying, analyzing, and documenting discrepancies between expected SIS behavior and actual behavior following a system demand trip.
- How to ensure the SIS is fully restored to verified operational state upon completion of routine or emergency maintenance.
- Testing schedules, not just for SIS sensors, logic solvers, and final control elements, but also for SIS subsystems. For example, how often should the SIS power and grounding subsystem, the HART multiplexer used to collect and report device health information, or the alert/messaging system be re-validated?

In other words, you need to identify, analyze, and document every conceivable scenario and train Operations and Maintenance personnel on what to do (and *not* do) in that situation — all ***before*** the scenario actually happens.

Remember, too, that operations and maintenance responsibilities aren't always confined to traditional roles and departments. For example, if the SIS uses automated alerts to notify key personnel, the systems for communicating those alerts may be the responsibility of an Information Technology (IT) group. In such instances, the plans should include how that group will deal with software upgrades, changes in user assignments, and other events that might influence the SIS solution.

Procedures

Once you've planned the operations and maintenance work, you must write procedures that define how to work the plan. These should include

- Routine actions such as proof testing and preventive maintenance that need to be carried out to maintain the as-designed functional safety of the SIS
- Actions required to prevent an unsafe state during maintenance, such as how bypasses will be implemented
- How information about the system will be gathered — including demand rates and system failure rates, as well as the results of audits and tests of the system
- What Maintenance personnel will do when there is a fault or failure in the SIS
- What test equipment will be used and how it will be calibrated and maintained.

Even the best planning cannot foresee every possible event or change, so the procedures may eventually require revision. This revision will usually follow functional safety audits or tests on the safety system, and be done in light of data collected by the Maintenance department.

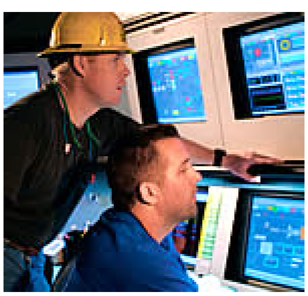
Finally, Operations and Maintenance personnel must be thoroughly **trained** in every aspect of the plans and the procedures, and their competency must be documented and kept current.

Operations' Responsibilities

Although the SIS isn't "operated" in the traditional sense, the Operations team still has plenty to do to ensure the installed SIS continues to provide its designed-in functional safety.

These responsibilities require an understanding of the identified risks and what actions the SIS should take if a specific demand occurs. This can be especially valuable when, for example, maintenance must be conducted on part of the SIS. Operations personnel must know how to run the plant safely while the maintenance is in progress and the SIS is potentially degraded.

It's also vital that they understand the importance of any diagnostic alarms that the SIS might raise — whether the alarm means that a transmitter will fail soon or that the SIS is no longer functioning as a layer of protection.



Operators must understand the function the SIS serves, what to do when it initiates a shutdown, and how to react to diagnostic alarms from SIS components.

Similarly, operators must understand the SIS testing requirements, and what happens if tests are delayed. For example, the tendency to run processes longer between shutdowns also means longer intervals between proof testing to verify SIS performance, and therefore less assurance that the SIS will function properly when needed. (In-service partial-stroke testing of SIS control valves can help compensate for the longer intervals.)

They also need to understand how a manual shutdown affects the plant and what manual start-up activities will be required to get the plant running safely again.

Operations personnel should be responsible for scheduled backups of SIS software (and BPCS software for that matter) and for archiving the backup media copies. Just how essential this task is becomes apparent as soon as a recovery is needed.

Finally, Operations should coordinate Maintenance access to the plant for all activities that could affect SIS performance or other aspects of plant safety.

Maintenance's Responsibilities

After that introduction to Operations' responsibilities, you might think there would be few SIS-related tasks for the Maintenance team.

You would be mistaken.

While the operators' job is to ensure that the plant runs safely, it is the Maintenance team's role to provide them with an SIS that performs to its targeted integrity. They must monitor and document how the safety devices in the plant behave, compare that to the expected behavior, and make modifications if required to ensure the required safety is maintained.

And it almost goes without saying that Maintenance must thoroughly document all that they do, including calibrations, repairs or routine maintenance, and system or equipment tests. They also keep track of the actions taken after a demand on the system, what equipment failed during testing or a demand, what caused any demand, and what caused any false trip.

Different systems, different maintenance. In most cases the same Maintenance personnel who work on the BPCS will also work on the SIS. These people need to understand that SIS sensors, logic solvers, and final control elements may be different from similar devices used for the BPCS.

For example, although a Rosemount 3051S pressure transmitter may have similar technical capabilities to a Rosemount 3051S SIS pressure transmitter, the 3051S isn't a substitute for the 3051S SIS unless it has the SIS feature board installed.

Even when SIS instruments look similar to standard devices, they may be different "under the hood" — and require different maintenance procedures.

Similarly, instrument recalibration and/or valve rebuild practices used for the BPCS may not be appropriate for the SIS. Besides failing to comply with IEC 61511, using the wrong procedures may prevent the SIS from working properly when it's needed most.

Proof testing. Conducted while the SIS is offline (usually during a scheduled shutdown), proof testing confirms that the SIS is still in as-built condition. During these tests, the Maintenance team verifies the correct action of every part of the safety system and all of the logical functionality. If anything fails to work as expected, they fix it.

The frequency of future proof tests will be determined by the same PFD calculations that were used when the system was designed. Maintenance must therefore update the demand rate for the SIS and failure rate for its components to reflect the actual numbers that have been logged during plant operation.

The frequency (and cost) of these and other maintenance tasks can be significantly reduced by making greater use of **predictive maintenance**.

Predictive Maintenance

Traditional **preventive** maintenance requires that equipment be calibrated, lubricated, rebuilt, or undergo some other service periodically, whether it needs it or not. **Predictive** maintenance, on the other hand, uses real-time information from intelligent devices to predict when each device's performance will reach the point where maintenance makes sense — neither before it's needed, nor after it's too late.

The potential cost savings are obvious. But predictive maintenance can also have a major impact on SIS reliability.

Despite the abundance of advanced instrumentation and control valve diagnostic capabilities available, many facilities still insist on recalibrating instruments and rebuilding control valves during scheduled shutdowns. For a host of reasons — from equipment contamination to human error — it's not uncommon for some of the instruments and valves to be worse after the recalibration and rebuild than before.

With predictive maintenance tools, however, you can identify which instruments and valves will actually need work before the next scheduled shutdown, and leave the others alone.

During ongoing operations, predictive diagnostics can also alert you to potential problems with SIS valves and instruments before they reach the point of failure — while there's still time for corrective action to maintain the system's integrity.

Combining such diagnostics with partial-stroke testing increases confidence that SIS control valves will work when needed, which can also help extend the intervals between shutdowns required for proof testing.

For more about using predictive maintenance to maximize availability and minimize costs, see Maintenance 101, "Understanding Maintenance Strategies," in PlantWeb University's Business School.

The PlantWeb Advantage

Emerson's smart SIS takes full advantage of PlantWeb® architecture's predictive maintenance technology, including built-in diagnostics and partial-stroke testing and the analysis and reporting capabilities of AMS™ Suite: Intelligent Device Manager software.

Together with the proven reliability of Emerson valves, instruments, and systems, these predictive maintenance technologies can significantly reduce maintenance costs while helping ensure SIS availability.

Summary

Section 16 of IEC 61511 includes a fairly extensive list of SIS operation and maintenance requirements, but they all really come down to two things:

- Both Operations and Maintenance must possess a thorough understanding of what's required of them to maintain the SIS's validated state, and

- Every discrepancy between expected and actual SIS behavior must be analyzed, the findings thoroughly documented, and appropriate corrections developed, implemented, and tested.

Other key points you learned in this course include

- Every aspect of SIS operation and maintenance must be planned, defined by appropriate procedures, carried out by trained personnel, and carefully documented.
- Operations must know how to react not only when the SIS conducts an on-demand shutdown, but also when diagnostic alarms indicate a potential problem with part of the system.
- SIS maintenance procedures may be different from those for basic process control systems — even for similar components.
- The frequency of proof tests should be adjusted to reflect actual SIS performance during plant operations.
- A predictive maintenance strategy can help increase SIS availability, while also reducing costs.