EMERSON
Process Management

PlantWeb University

SIS 302 - Modification

15 minutes

In this course:

Overview

Despite all the careful planning that goes into designing and implementing a safety instrumented system, change is inevitable. Processes get modified, equipment replaced, software upgraded.

Any change that affects plant safety must be managed carefully — a point driven home by examples like the 1974 explosion and fire at Flixborough in the UK, where 28 plant workers died because of inadequate attention to the safety impact of a piping change. And as we learned in SIS 202, in 20% of accidents caused by control and safety system failures, the root cause was changes after the system was put into service.

This course provides an overview of things to keep in mind when making changes that may affect how the safety instrumented system ensures safe operations — from the objectives of SIS modification management, to procedures for making the changes, to (of course) documenting what you've done.

Hint

As you go through the topics in this course, pay special attention to…

- IEC 61511's two key requirements for SIS modifications
- What kinds of changes require modification management
- Who needs to be informed of modifications, and why.

Objectives

Modification management (also called change control) provides a structured methodology for changing a document, equipment, or process — and keeping track of the changes. In the case of an SIS, it ensures that the system remains validated by recognizing and addressing the potential impact of system changes. And used properly, it avoids the safety risks of inadequately planned, haphazardly implemented, and undocumented changes — like those that led to the Flixborough disaster.

To achieve these objectives, IEC 61511 says SIS modifications must be made in a way that ensures

- All changes are properly planned, reviewed, and approved in advance, and
- The required safety integrity of the SIS is maintained in spite of any changes.

It's worth noting that IEC 61511 takes a holistic view of SIS modification management. Besides changes to SIS hardware and software, changes to the physical process plant, the basic process control system (BPCS), and the process itself must also be analyzed to determine their impact on safety, and appropriate actions taken to maintain safe operations.

Planning

Before you can make any changes to the SIS, you must have clear modification management procedures that define how changes will be authorized and controlled.

In fact, without these procedures — established as part of the original safety life cycle planning process — the installed SIS is not validated. They're also one of the things auditors are likely to ask about after a safety incident.

These procedures will guide you through the process of identifying the work to be done and the hazards that will be affected. This includes analyzing the impact of the modification on the functional safety of the plant.

If the planned changes have a negative effect on safety, you should return to the beginning of the safety life cycle and repeat your process hazard analysis work. If not, you can carry on with planning the modifications — including the details of how changes will be carried out and how you will verify the results.

Now that you know what you're going to be doing and that there is no negative impact on safety, you can start the work. Or can you?

Communication

Before you can begin actually making modifications, you must get proper authorization. This might be from more than your own management, and will probably be required from Operations as well. After all, if they are running the plant, they need to know exactly what is happening.

The requirement to keep Operations in the loop is illustrated by the Piper Alpha disaster. One of the causes was that the platform operator did not know that a compressor had been removed from service and the piping blanked off. When the secondary compressor failed, he opened valves to route the oil to the first compressor, not knowing it was out of service. This ultimately led to the worst offshore oil disaster in history.

While it may seem obvious, it's also essential to make sure the people who will make the change thoroughly understand what they are to do and are properly trained and qualified for the tasks involved. The same goes for any other groups — such as Maintenance — whose work will be affected either during or after the modification.

Think you've finished? Then you've overlooked a key aspect of every stage in the safety lifecycle.

Documentation

Planning for any SIS modification will depend heavily on documentation developed during earlier stages of the safety lifecycle. And the more thorough and well-organized that documentation is, the easier the task will be.

To give anyone working on the SIS in the future the same advantage, the modifications you make should be equally well documented. This documentation should include

- A description of the modification
- Why the change was made
- The hazards that might be affected
- How the modification will impact the SIS
- All of the approvals you collected along the way
- Details of all changes to the configuration, both hardware and software
- Descriptions of tests to verify that the modification worked the way it should, and the results
- Descriptions of tests to verify that the modification had no impact on the rest of the SIS, and the results.

Don't forget to also update any secondary documentation affected by the change, such as manuals, drawings, instrument records, and purchasing specifications for replacement parts. A good change-control checklist can help here.

Finally, make sure both the primary and secondary documentation are distributed to the people who need them, and that any obsoleted documents are removed from use.

The PlantWeb Advantage

Emerson's smart SIS eases documentation by doing much of the work automatically. For example,

- instrument changes done through AMS Suite: Intelligent Device Manager software are automatically recorded.
- DeltaV's Version Control and Audit Trail function tracks all changes to system configuration, not only providing automatic documentation but also easing comparisons of different versions.
- The DeltaV SIS also analyzes any new software downloaded to the logic solver to identify which software modules and I/O are affected — so only those portions need re-validation.

Summary

Careful modification management is essential for the SIS to do its job. In this course you learned that

- Established modification management procedures are required for SIS validation.

- All modifications must be properly planned, reviewed, and approved before any changes can be made.
- Changes to the process, plant, and BPCS — as well as the SIS itself — must also be analyzed for their potential impact on safety.
- All changes must be properly communicated and documented.