SIS 303 - Decommissioning

15 minutes

In this course:

Overview

Decommissioning a safety instrumented system can be thought of as a special type of modification, which means all the requirements we discussed in SIS 302 must be addressed.

However, the typical modifications we covered in that course tend to be small, and to maintain or even increase safety. When we decommission an SIS, on the other hand, **we remove layers of protection** — from a single safety function to the entire safety system. We therefore need to ensure that what's left is

- Adequate to protect against the remaining hazards
- Not disturbed (degraded) by the hardware and software we've removed
- Still efficiently configured, without confusing layers of "dead" code

This course provides tips on how to do just that.

Hint

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

- The differences between full and partial decommissioning

- What the decommissioning plan should include
- Good and bad practices for decommissioning software
- The roles of testing, validation, and documentation.

Total or Partial?

SIS decommissioning can be either **total** or **partial**.

Total decommissioning happens when the protection provided by the SIS is no longer needed — typically because the process it was designed for is no longer used.

In this case, decommissioning is relatively straightforward: The plant is shut down and the SIS removed. There may still be personnel hazards, such as from unpleasant chemicals, but the process hazards are gone because there is no process.

Partial decommissioning can occur when process modifications — for example, switching to a less-hazardous additive or eliminating an exothermic reaction — reduce the number of safety functions that the SIS must provide.

For this situation, decommissioning involves removing the SIS sensors, final control elements, logic solvers, and software that are no longer needed without affecting the components that are still required to protect against the remaining hazards.

Making sure you remove the right pieces — and ***only*** the right pieces — calls for careful planning.

Decommissioning Plan

Before decommissioning begins, IEC 61511 requires that qualified individuals work together to develop, assess, and approve a complete decommissioning plan. The plan should include

- Who will identify, supervise, conduct, and approve decommissioning activities and milestones, and how they will do it
- How remaining SIS functional safety will be assessed, including an updated review of hazards and associated risk assessments
- How functional safety will be maintained if decommissioning activities must occur while the process remains operational
- How decommissioning of one physical unit affects adjacent operating units and facility services and utilities.

The plan should also include a detailed cross-reference to the safety requirements specification (SRS) documentation, identifying which paragraphs and other documentation are affected by the decommissioning.

In short, decommission planning must include the same attention to detail as the original SIS design and any modifications.

Software Issues

Criteria and procedures for retaining or removing sensors and final control elements are fairly straightforward. Decommissioning software is more complex because the interrelationships between different pieces of code may be less apparent.

No dead code. One common mistake is to "comment out" or "branch around" the unneeded software under the guise that "we might need it in the future." Instead, unneeded code must be removed and/or reconstructed.

Software auditors don't like — and when it comes to SIS software, won't tolerate — what's generally referred to as "dead code" residing in the logic solver. Besides complicating safety functionality audits, dead code provides more opportunities for systematic failures. If the software isn't there, it can't go wrong or interfere with the safety function. It also won't take up processor time to scan and execute, and memory to store.

Similarly, the use of "dummy" or "virtual" inputs is considered a bad software practice. For example, if an **AND** element includes a now decommissioned input, resist the temptation to replace the input with a register value. Instead, reconstruct the **AND** element with the appropriate number of inputs required to satisfy the remaining SIS logic.

"**What does this do**?" While you shouldn't leave old code in the system, you also have to be sure that you're not removing SIS functionality that's still needed. You may find yourself asking frequently, "What if what I'm about to do prevents the SIS from doing its job?"

This question is much easier to answer when you have the documentation we've been talking about in every course — from initial requirements and design specs through detailed records of any modifications. Without it, you'd have to reverse-engineer the code or, worse, guess at the purpose of every line.

Clear, concise, comprehensive documentation makes the job easier, quicker, and safer. All those hours you put into designing, implementing, and documenting the software will pay big dividends in being able to confidently decommission a part of it.

The PlantWeb Advantage

The DeltaV SIS stores and executes each safety instrumented function (SIF) in a separate, self-contained software module. To decommission an SIF, you simply remove that individual module — with no impact on the other SIFs.

DeltaV's Version Control and Audit Tracking feature automatically records the change, so documentation is easier, too.

Testing

Testing is just as important for decommissioning as it was for the earlier stages of the SIS lifecycle.

The persons developing the decommissioning plan should review the test plans used to originally commission the SIS, modify them as needed, and create new ones when necessary — all with the intent of ensuring that the functional safety provided by the remaining SIS is not compromised.

If SIS decommissioning takes place while the process remains operational, you may also need intermediate testing plans. For example, if decommissioning activities occur only during the day shift and the SIS is to provide functional safety during the second and third shifts, intermediate testing will be required to ensure the SIS is re-commissioned for second and third shift coverage.

Revalidation

As we learned in SIS 203, validation is an activity that proves the SIS works as designed. It involves a complete input-to-output test designed to deliver an IEC 61511-compliant SIS solution.

Once partial decommissioning activities are complete, any remaining safety functions that could have been affected by the work must be revalidated. With some systems this could mean repeating the full functional safety validation.

Documentation

It should come as no surprise that all decommissioning activities need to be documented to the same high standards as the other work that has been done on the SIS.

We've also seen how important that earlier documentation can be to the decommissioning effort. When current documentation actually reflects the state of the current SIS, confidence in the decommissioning plan soars.

Conversely, if SIS documentation is not current, then decommissioning plan development must be put on hold until a complete audit of the SIS can be completed and all documentation brought up to "as built" status.

Summary

SIS decommissioning requires the same level of careful planning and attention to detail as any other stage of the safety lifecycle, for the same reason: mistakes can cost lives. In this course we learned that

- The most important goal of SIS decommissioning — especially partial decommissioning — is to ensure adequate protection from any remaining process hazards.
- IEC 61511 requires a complete, approved decommissioning plan before work begins.
- In decommissioning SIS software, special care is needed to remove exactly the right code — leaving behind neither too much nor too little for the SIS to do its job.
- Testing and validation are just as important to decommissioning an SIS as they were to putting it into service.
- Good documentation is not only required; it also makes decommissioning easier.