

SIS 203 - Verification & Validation

15 minutes

In this course:

- 1 Overview
- 2 Verification
- 3 Validation
- 4 A Structured Approach
- 5 System Decomposition
- 6 Test Planning
- 7 Documentation
- 8 Summary

Overview

We all know that the best design is only as good as its implementation. That's why designing a safety instrumented system (SIS) to meet safety requirements isn't enough. You also have to prove that

- each step of the design effort meets the appropriate requirements as defined in the safety requirements specification (SRS)
- the installed SIS will carry out its safety function.



These two activities are called **verification** and **validation**. Verification takes place at each step in the safety lifecycle, while validation occurs after the system is installed and before it's put into service.

Both activities help you remove as many **systematic failures** from the SIS as possible. Systematic failures are those "built into" the system as a result of human error, as opposed to random failures that happen when equipment breaks down.

This course shows how verification and validation provide a high level of assurance that the SIS will operate in accordance with its safety requirements specification (SRS). You'll also learn ways to structure verification and validation efforts to make them more manageable, and how good documentation practices can help you produce (and maintain) the proof that your SIS is properly designed and implemented.

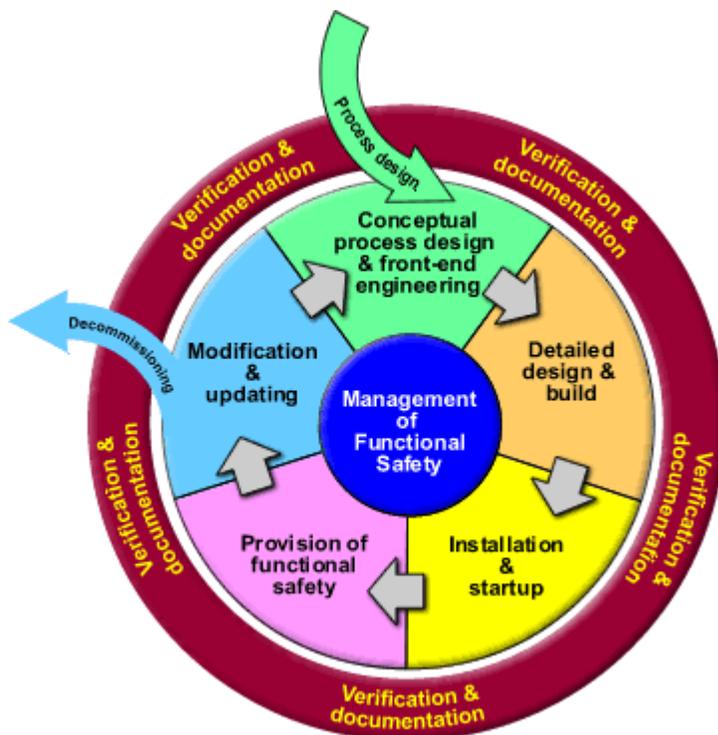
Hint

Pay special attention to ...

- The difference between verification and validation
- How to "decompose" the SIS into subsystems
- How validation models like IQ-OQ-PQ can help
- What to include in your test plans
- What good documentation achieves.

Verification

Verification occurs at the end of every step of the safety lifecycle. It demonstrates that the work has met all the objectives and requirements for that specific activity.



Verification (and documentation of the results) takes place at each stage of the safety lifecycle.

Verification may be carried out through analysis, testing, or a mixture of the two. Activities might include

- Reviews of documents from all phases of the safety lifecycle to ensure compliance with the objectives and requirements
- Design reviews
- Tests of the designed products to ensure that they perform according to their specification. This is

especially valuable for modular components — such as the code for a voter algorithm — that will be reused many times.

- Integration tests performed when different parts of the system are put together.

Verification activities and their results are thoroughly documented to show not only that the design met requirements, but also that you checked to be certain it did — and made any necessary fixes.

Validation

Validation builds on the verification activities by adding thorough testing of the completed SIS to prove that everything works as it should. It demonstrates that every safety function in the SIS, as well as the SIS itself, meets every requirement in the safety requirement specification (SRS).

While verification is performed throughout the project and can be carried out wherever the work is being done, validation happens only on site, after the system has been installed and commissioned.

Among other things, validation tests may include confirming that...

- The system functions properly in all relevant modes of operation (start-up, shutdown, automatic, semi-automatic, and so on)
- The SIS satisfactorily performs under normal and abnormal operating modes as defined in the SRS
- Interaction of the BPCS and other connected systems doesn't affect or restrict the SIS's ability to respond
- Sensors, logic solvers, and final control elements (including redundant channels) perform as required
- The SIS performs appropriately on invalid process values, such as "out of range" sensor values
- The SIS performs as designed on loss and restoration of utilities, such as electrical power, instrument air, or hydraulics.

Validation requires precise planning to identify and document the procedures, measures, and tests that will be used, as well as the order and schedule of the tests and the competencies required of the staff who will perform them.

It's a big job that can require a lot of resources. But when you remember that the SIS exists to protect your community, neighbors, family, co-workers, and environment, doing anything less isn't an option.

And fortunately, there are ways to make the task more manageable.

A Structured Approach

You recall that IEC 61511 defines **what** you must do and why, leaving it to you to determine how to do it. You can organize and conduct the verification and validation processes in whatever way makes sense for your situation — as long as you produce documented evidence that the SIS complies with the SRS.

But rather than going through all the effort to create a unique validation approach, consider adopting one that is already commonly used in industry. Although not defined in IEC 61511, one widely used example is the structured approach prescribed by the U.S. Food & Drug Administration (FDA) to validate basic process control systems.

This well-understood, well-documented model breaks the work into three phases: **installation qualification (IQ)**, **operational qualification (OQ)**, and **performance qualification (PQ)**.

- **Installation Qualification** tests and documents that the individual physical aspects of the SIS solution — devices and subsystems — are installed correctly. It occurs before power is introduced.

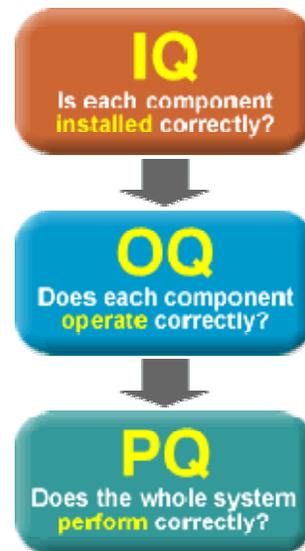
For the ammonia tank example we introduced in an earlier course, IQ could include confirming that the pressure sensors installed on the tank are the correct model, have the required safety-related documentation, have been installed according to the design and manufacturer specifications, are wired correctly, and have all switches and jumpers set properly.

- **Operational Qualification** tests and documents that the individual physical and software aspects of the SIS solution work the way they should. Like IQ, OQ tests devices and subsystems.

For example, you might check that each sensor has the correct voltages, that the partial-stroke testing is correctly configured in the valve controllers, and that the logic solvers have their configuration downloaded and are reporting no errors.

- **Performance Qualification** tests and documents that the SIS as a whole is capable of performing the defined safety functions according to the SRS.

PQ is an integrated test of procedures, personnel, processes, and the complete SIS. It occurs after all IQ and OQ activities for both physical (hardware) and functional (software) aspects of the SIS have been completed. Any problems found during PQ must be investigated, fixed, and documented.



Because IEC 61511 represents a framework for applying good practices to achieve a robust SIS solution, adopting existing good practices like the IQ-OQ-PQ approach makes more sense than creating them from scratch.

You can further simplify the effort by conducting testing on a safety function-by-safety function basis. This "decomposition" of the system is what we turn to next.

System Decomposition

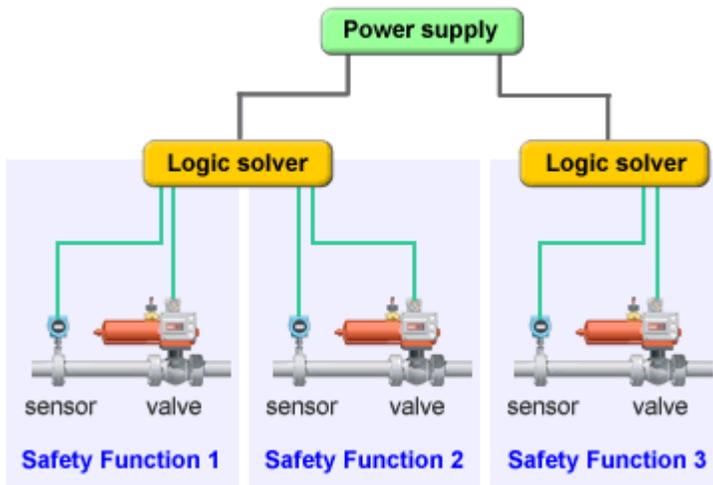
Verifying and validating a complete SIS can seem like (and be) a daunting task — unless you break the work into manageable chunks.

One way to do this is by **decomposing** the SIS solution into its safety instrumented functions (SIFs) and identifying the devices and subsystems that carry out each SIF. Looking at each component separately makes it easier to identify and document the required skills, test equipment, testing structure, and signoff sheets for specific parts and subsystems.

For example, you'll find that some parts and subsystems, such as sensors and final control elements, are specific to a safety function. Others, such as AC and DC power, grounding systems, and communications, are more "generic."

You can therefore structure your efforts to first confirm that the generic elements are providing the necessary services or capabilities to support all safety functions. Once you know that's the case, you can then verify that elements unique to each safety function are also working properly. This approach avoids re-testing the same generic elements for each safety function.

For the system shown in the diagram below, for example, decomposition enables you to validate the power supply only once, without having to test it again for each of the safety functions it supports.



The same principle applies to the logic solver on the left in the diagram. Once you've established that its generic capabilities are operating correctly (for example, that there are no diagnostic errors, the power supplies are okay, and the network is working), you don't need to retest these same functions for every SIF the logic solver supports. However, you must validate that every SIF works correctly in accordance with the safety requirements specification.

Decomposing the system into its parts and subsystems also makes it easier and more efficient to use material from product manufacturers, third-party consultants, and public sources to create your test plans.

For example, the IQ test plan for a safety-certified pressure transmitter can be developed by referring to the relevant sections of the manufacturer's installation documentation, augmented with an appropriate IQ verification signoff sheet.

The pressure transmitter's OQ test plan can be similarly developed based on the manufacturer's safety manual and calibration requirements.

The PlantWeb Advantage

Emerson Process Management's public web sites provide access to documentation you can use to help achieve IEC 61511 compliance.

For example, for help in developing IQ and OQ test plans for a Rosemount 3051S series pressure transmitter, you can visit www.rosemount.com/document/ and download the installation guide for that instrument...including the section on use in Safety Instrumented Systems.

Similar information on other SIS products is also available online. A good starting point is www.EmersonProcess.com/SIS.

Test Planning

Each phase in verification and validation testing must confirm that the corresponding development phase has fully met each of its objectives. Reaching that goal demands thorough and rigorous planning.

For example, you should be sure to consider and document

- Testing strategy — including test scenarios, expected results, and how to deal with any discrepancy corrections

- Testing process — including criteria for declaring a test complete
- People requirements — how many, for how long, and with what skills
- Technology requirements — tools, analyzers, and supporting software needed.

Although SIS equipment suppliers are generally responsible for testing embedded and utility software before you receive the products, your plan should cover how installed SIS devices will be re-tested following changes (including upgrades) to such things as the operating system, utilities, firmware, and communications protocols.

It's also a good idea to have testing conducted by different people from those who designed and implemented the system. An independent tester is more likely to exercise the equipment and software in ways the designer and implementer didn't anticipate, such as inputting both legal and illegal data values.

Keep in mind that IEC 61511 doesn't define **how** to do all this, so it's likely you'll need to consult other sources or enlist outside assistance in developing a comprehensive software test plan.

There's no reason to be embarrassed to ask for help. Knowledgeable suppliers and consultants can provide tools and expertise that can help make achieving IEC 61511 compliance easier. Additionally, new technologies and product designs can simplify or even automate much of the testing and documentation effort.

The PlantWeb Advantage

Besides easy-to-access documentation to help achieve IEC 61511 compliance, Emerson can also provide the services of its certified safety specialists when you need additional resources or expertise.

Verification and validation efforts also benefit from technologies built into Emerson's smart SIS — from easy confirmation of device installation, configuration, and operating status to automatic documentation of system configuration changes.

Documentation

Through several courses, you've been reminded that IEC 61511 requires documenting each phase or activity in the SIS safety lifecycle.

For each phase, the documentation should show what the inputs were, how the objectives were met, and that the outputs met the requirements. In short, it's your proof that you've ensured the safety solution has the form, fit, and function to mitigate the identified hazards. Documentation is especially important in verification and validation, where it's your proof that the implemented SIS meets the requirements.

For documentation to be usable and maintainable, it must be well organized. Good documentation practices, such as those defined in the ISO 9000 quality-management standard, are designed to ensure control of document creation, review, approval, distribution, and storage. Although IEC 61511 doesn't specifically address how documentation should be assembled, it does require the following:

- Results of the hazard and risk assessment
- Assumptions used when determining the safety integrity levels
- Safety requirements specifications (SRS)
- Traceability between documents and the SRS
- Application logic including certified modules used

- Design documentation
- Modification information and/or documentation
- Records of qualification verification and validation
- Commissioning and SIS validation procedure(s)
- SIS operating procedures
- SIS maintenance procedures
- Proof test procedures
- Results of assessments and audits

"Completing the paperwork" isn't usually high on anyone's to-do list, but it's an essential part of an SIS project. And if there is an incident followed by investigation, your SIS documentation will help determine what went wrong and how it can be prevented or mitigated in the future.

Perhaps you can push some of your other paperwork aside, but not the SIS documentation.

The PlantWeb Advantage

Emerson Process Management's smart SIS includes capabilities designed to ease documentation creation and management. For example,

- DeltaV SIS Configuration Studio includes fully documented, TÜV-certified function blocks, application logic documenter, login password protection, and automatic audit trail.
- AMS Suite software provides login password protection. It can automatically prompt for inspections and tests to be conducted, track proof-test and inspection results, and alert for and track changes to field devices.
- Valves fitted with Fisher FIELDVUE DVC6000 digital valve controllers can be set up for automatic partial-stroke testing, with results recorded and reported using AMS Device Manager.

Summary

In this course you've learned that...

- Verification and validation confirm that the SIS complies with the safety requirements specification (SRS).
- Verification happens at each stage of the safety life cycle. It confirms that the work done during that stage meets the appropriate requirements.
- Validation occurs after the system has been installed and commissioned. It demonstrates that the completed SIS will carry out its safety function.
- The IQ-OQ-PQ model provides a proven structure for dividing verification and validation efforts into logical (and manageable) phases.
- System decomposition offers an additional method for breaking the work into manageable chunks.
- Planning all the tests required for verification and validation is a major (and important) task in itself.
- Every test and its results must be documented — and the documentation must be usable and maintainable.