# SIS 201 - Physical Design

**15 minutes**

In this course:

## Overview

Just as a basic process control system (BPCS) is more than a controller, an SIS is more than a safety PLC. Its primary physical components are sensors, logic solvers, and final control elements.

This course covers why these components are considered essential and others are not, as well as how the difference can affect your design decisions. We'll also look at two ways to establish that physical components are suitable for safety applications, the role testing plays in ensuring they'll work when needed, and how to inform the right people when there's an indication that they might not.

Throughout the course, we'll be watching for ways to ensure your SIS meets requirements without costing more than necessary.

### Hint

Pay special attention to the following:

- How distinguishing between essential and non-essential components can save you time and money.
- What's required to use non-certified safety devices.

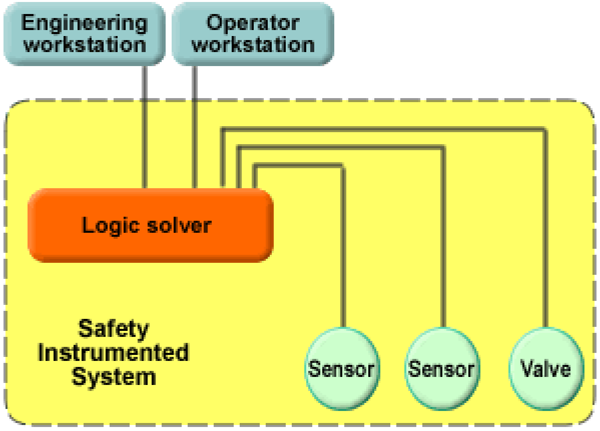
- How probability of failure on demand (PFD) affects component selection
- Potential effects of different test frequencies.

## Essential Components & Subsystems

Often when designing and specifying a basic process control system (BPCS), the temptation is to purchase as much BPCS functionality and capability — the "bells and whistles" — as the budget permits.

When designing and specifying an SIS, however, the conversation is not so much about bells and whistles as it is about the **essential** and **non-essential** components and subsystems. Understanding the difference helps you design a system with the right Safety Integrity Level (SIL) — without over-engineering the solution.

**Essential** items are the SIS components and associated elements necessary to carry out the Safety Instrumented Function — including sensors, logic solvers, final control elements, power supplies, and I/O modules. These are the items that must meet defined SIL requirements.



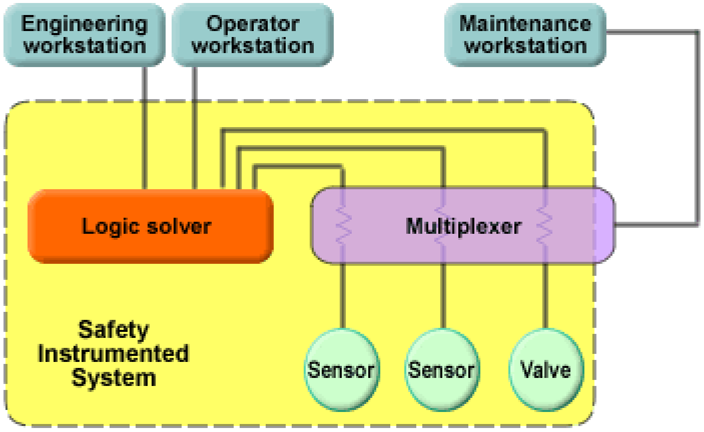
Essential components — in this example, those inside the yellow area — are the sensors, logic solvers, final control elements, and other equipment necessary to carry out the safety instrumented function.

## Non-essential Components & Subsystems

As we just learned, **essential** SIS components and subsystems are those necessary to carry out the SIF.

**Non-essential** components (also referred to as "**non-interfering**") provide support to engineer and maintain the SIS, but their presence or absence doesn't interfere with the functioning of the SIS. Examples include engineering workstations, HART multiplexers, hand-held calibrators, and maintenance workstations.

Although such components can ***support*** the safety function, they don't ***perform*** it. As a result, they **don't** have to meet defined Safety Integrity Level (SIL) requirements — as long as you can demonstrate that they can't introduce dangerous failures into the SIS.

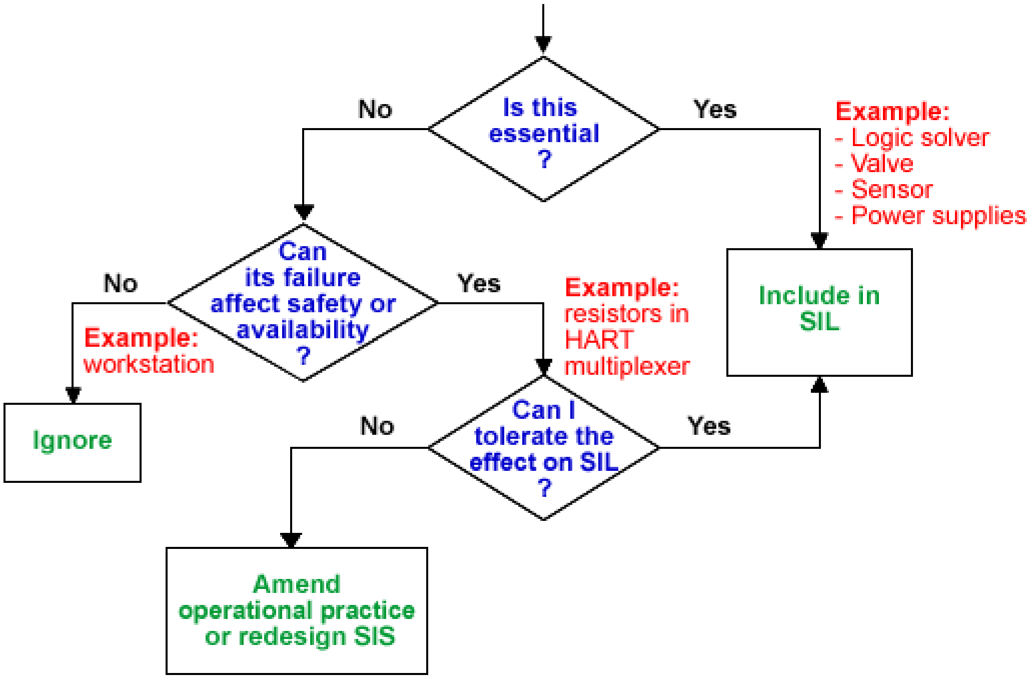


Nonessential components — like those outside the yellow area in this diagram — are not required to meet SIL requirements.

In most cases, such as an engineering workstation, it's obvious the component or subsystem is non-essential. Others can be less obvious.

Look again at the illustration above. In practice, the HART multiplexer includes an I/O termination panel where resistors are used to extract the digital information from the 4-20mA sensor signal. Because the sensor signal does not pass through the electronics of the multiplexer to reach the logic solver, the multiplexer electronics aren't considered part of the SIS, and thus they don't have to meet SIL requirements. A failure in the resistors could affect safety, so they should be included in the SIL calculations.

You can use the following flowchart to help determine if a component or subsystem is essential or non-essential.


Is this essential ?
No
Yes
Example:
- Logic solver
- Valve
- Sensor
- Power supplies
Include in SIL
Can its failure affect safety or availability ?
No
Yes
Example: workstation
Example: resistors in HART multiplexer
Ignore
Can I tolerate the effect on SIL ?
No
Yes
Amend operational practice or redesign SIS

## Certified Or Proven In Use?

IEC and ANSI/ISA safety system standards give you two options when selecting safety system devices:

- Use devices that have been independently certified as compliant, or
- Produce historical documentation demonstrating that a non-certified device is SIS capable. This option is commonly called "prior use" or "proven in use."

Let's take a closer look at each of these options.

## Certified Or Proven In Use?
**Certified**

To achieve certified status, the device's manufacturer submits it for extensive third-party analysis to verify that it conforms to IEC 61508. These third parties are known as notified certifying bodies.

The evaluation includes testing and analysis of device hardware, software, and engineering and manufacturing processes, and seeks to establish

- how the device reacts to a wide range of potential failure conditions
- whether the device produces errors under those conditions
- whether those errors can be routinely detected
- whether the errors are safe or unsafe

Certified devices always include a *Safety Manual* that informs the end user how to safely install, configure, and operate the certified device. The safety manual also identifies the limitations of device functionality — in other words, what it *won't* do. (For that reason, a thin manual can be one sign of a good device.)

If you have no prior-use history for the device operating under similar conditions, using certified SIS devices is frequently the most cost-effective solution.

### The PlantWeb Advantage

Emerson's DVC6000 Fisher FIELDVUE digital valve controller has been certified by TÜV for use in SIL 3 applications, and the Rosemount 3051S pressure/differential pressure and 3144P temperature transmitters have been certified by TÜV for use in SIL 2 applications (SIL 3 applications when used redundantly).

## Certified Or Proven In Use?
**Proven In Use**

To achieve proven-in-use approval, the device's manufacturer must prove it has a quality or change-management system for the specific device. Then you have to document that you have the same device operating under conditions similar to those of the proposed SIS, such as with a basic process control system (BPCS).

Additionally, you must document usage and failure history for the device to determine mean time between failure (MTBF). This documentation must support

- Your claim that the device is capable of meeting the defined SIL requirements, and
- The Probability of Failure on Demand (PFD) numbers — discussed in our next topic — that you used to calculate the loop's required Safety Integrity Level (SIL).

Prior use documents device history under actual use conditions. These conditions should extend beyond the device to include process connections, primary elements, and installation practices. For plants that have this data available, prior use can often meet the needed safety requirements most cost-effectively.

As a rule of thumb, more-complex devices should be certified. If a device is programmable, then it's likely to be complex.

### The PlantWeb Advantage

Collecting and maintaining prior use data can be challenging and expensive. That's because

- Manufacturers change product designs, which may prevent you from relying on experience from using an earlier design.
- Traditionally, suppliers haven't given users safety manuals showing how to properly use and proof test products in safety applications.
- There may be little or no safety-failure data available on the product.

For many Emerson devices, however, Emerson can help users collect and manage the data they need to build their prior-use case, including

- Failure mode effects and diagnostic analysis (FMEDA) to show the failure modes (dangerous or safe) and rates
- Beta calculations to give common cause failure probabilities
- Safety manuals to provide instructions on proper use and test procedures
- Proof of management of change
- Proof of operational hours
- Online tracking of hardware and software changes
- Hardware and software change notifications.

## Probability Of Failure On Demand

An SIS can't carry out its function unless each of its components works properly when needed. But the reality is that all equipment carries some risk of failure. (If it didn't, you wouldn't need an SIS, would you?)

That's why understanding each component's failure rate, or **average probability of failure on demand (PFDavg)**, is essential in designing a system to provide a given level of risk reduction. You want components with a PFD that's low enough to provide the right risk reduction factor (RRF), but not so low that you wind up with an over-engineered (and overly expensive) system.

Let's consider the ammonia tank example from SIS 101. Assume we install a system that is designed to prevent tank rupture, and 1 time in 10 it fails to work when needed (PFD=1/10, or 0.1). With no system, the tank would have ruptured 10 times; with the system in place it will rupture only once. We have therefore reduced the risk by a factor of 10 — and discovered that PFD=1/RRF.

As you saw in SIS 101, each safety integrity level (SIL) describes a range of target risk reduction factors. We can now add a third column to the table we introduced in that course:

| Safety Integrity Level | Target<br>risk reduction factor | Target average probability of failure on demand (PFD$_{avg}$) |
|---|---|---|
| 4 | >10,000 to <=100,000 | 1/10,000 to 1/100,000 |
| 3 | >1,000 to <=10,000 | 1/1000 to 1/10,000 |
| 2 | >100 to <=1,000 | 1/100 to 1/1000 |
| 1 | >10 to <=100 | 1/10 to 1/100 |

Adapted from IEC 61511-1 Table 3

Knowing a device's PFD will help you decide whether to include it in your design. But what happens once the SIS is operational?

## Proof Testing

Essential components of an SIS must be tested periodically to prove they will work when needed — or to reveal any problems so the system can be restored to its designed safety functionality.

How often you should conduct these tests depends on the component's average probability of failure on demand (PFD$_{avg}$). The more frequent the tests, the greater the assurance the component is in working order — which means a lower PFD$_{avg}$ and therefore a higher risk reduction factor (RRF).

Conducting a full system proof test is usually possible only when the process is shut down. Although such complete system tests are needed periodically, you can reduce the frequency of required shutdowns by conducting interim tests of what are typically the greatest contributors to PFD$_{avg}$: the final control elements.

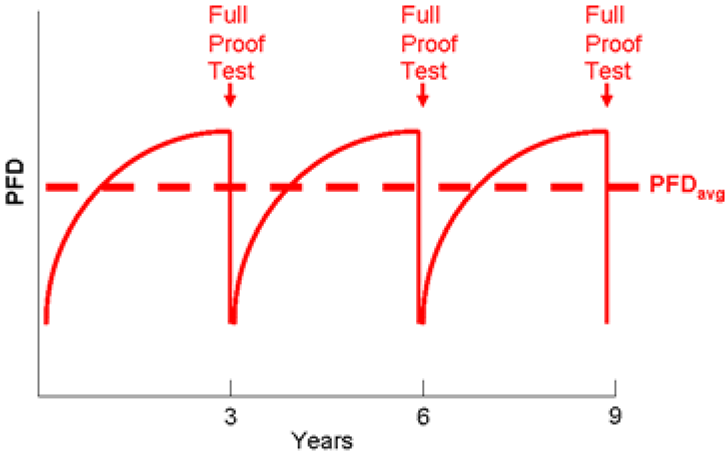
Keeping the SIS in compliance therefore requires choosing from three options:

1. Engineering the SIS so that it doesn't need testing during the long periods between plant shutdowns. With plants operating two, three, or more years between scheduled shutdowns, this can be a potentially expensive option — and may be impossible to achieve in practice.

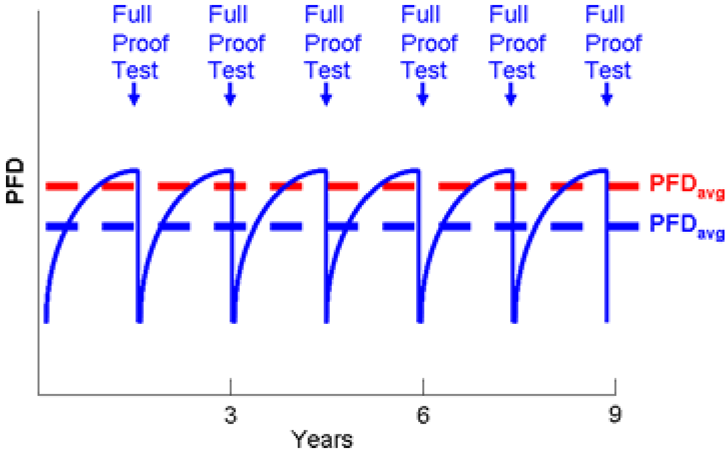
2. Installing bypass lines around each final control element to facilitate full proof testing while the process remains in operation. This is also an expensive option, and one that leaves the process unprotected during test periods. There's also a risk that bypass lines may be left open inadvertently after testing is completed.

3. Using manual or automated **partial-stroke valve testing** (which doesn't require a process shutdown) to reduce the PFD$_{avg}$. Reliability analyses usually show that valve-related problems, such as a stuck stem or plug, are the greatest contributor to the PFD$_{avg}$ of the total SIS. A partial-stroke test can detect such problems — or prove that they don't exist.

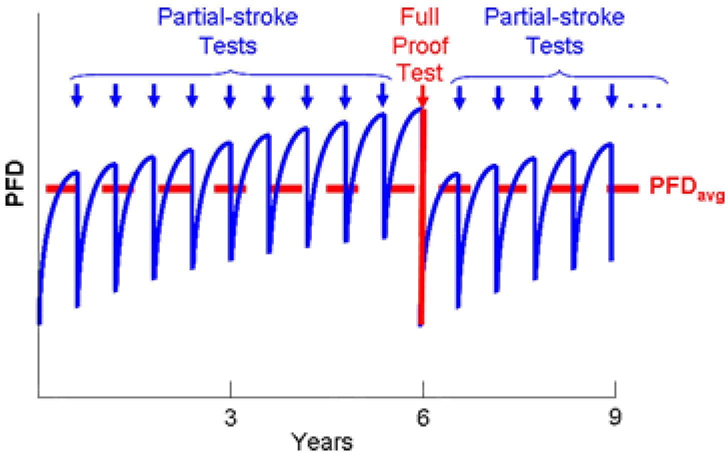
The three diagrams that follow illustrate how more-frequent testing can reduce PFD$_{avg}$ or extend the intervals between full proof tests.



Probability of failure on demand (PFD) increases over time but returns to its original level when a full proof test shows that everything works correctly — in this case, during an every-three-years shutdown.



Running the same test twice as often lowers the average PFD. As a result, you may be able to use the same equipment to meet a higher SIL requirement, or less-expensive equipment for the same SIL.



Another approach is to run full proof tests only half as often, but use frequent partial-stroke testing to maintain the same average PFD.

Intelligent SIS valve controllers and logic solvers can work together to automate partial-stroke testing, making it easier and more affordable to conduct such tests more often. Such automated tests also avoid the safety risks associated with sending someone into the field to run the test, and the risk that the emergency shutdown valve won't be available if it's needed during the test.

Intelligent valve controllers and logic solvers also make it easier to detect potential problems by comparing current test results to those from the previous test or when the valve was installed.

For more on this topic, see the Exida report "The effects of partial-stroke testing on SIL levels."

### The PlantWeb Advantage

Emerson's smart SIS is designed to **automate** partial-stroke testing, avoiding the higher costs and potential risks of manual tests — including added labor, exposing workers to hazardous conditions, and even reducing safety by failing to follow proper procedures.

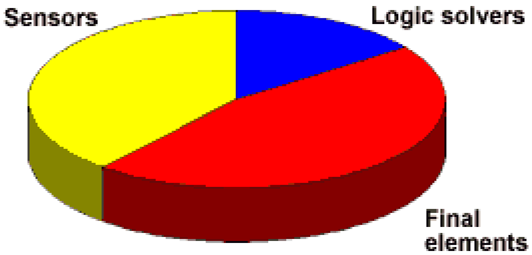
The FIELDVUE digital valve controller, used in conjunction with AMS Device Manager software, documents the original valve signature and other data, as well as partial stroke testing time, date, and results. The FIELDVUE valve controller is also part of the SIL-PAC valve actuator/controller solution available for SIS applications. The DeltaV SIS logic solver can automate the start of partial-stroke testing and collect the resulting pass-fail data.

You can also reduce proof-test frequency by choosing devices with low failure rates — such as the Rosemount transmitters and Micro Motion Coriolis flowmeters that can also be key components of our smart SIS.

## Diagnostics

Another way to increase the reliability of your SIS is by choosing components with built-in diagnostics. This is especially important for sensors and final control elements: over 85% of problems affecting the operation of an SIS are related to these field devices, not the logic solver.

Sources of SIS failures



Source: Emerson analysis of OREDA data

Devices that offer diagnostic capabilities use on-board microprocessors to monitor and report on their own status. Some can even predict potential problems in time for you to take corrective action before safety is compromised.

As devices continue to get "smarter," their diagnostic capabilities can extend beyond their own health to the surrounding process. For example, if a flowmeter simply reports that it has a problem, the Maintenance team might replace it — but that wouldn't clear a slug-flow condition, which is a process issue. Diagnostics that alert you to such conditions may enable you to resolve a process problem before it becomes a safety problem.

### The PlantWeb Advantage

The intelligent devices in Emerson's smart SIS offer a broad range of advanced diagnostics. For example, the DVC6000 SIS digital valve controller can diagnose problems in the actuator and valve as well as itself. A Rosemount 3144P SIS transmitter can signal when it detects a failed temperature probe. And a smart Micro Motion Coriolis flowmeter can detect process conditions such as slug flow, or changes in reactant density that could indicate a catalyst is being poisoned.

## Intelligent Alerts and Alarms

Partial stroke testing, diagnostics, and other technologies for identifying (or even predicting) problems in safety loops can help maintain the required $PFD_{avg}$ — but only if the right people find out about the problems in time to take corrective action.

Detection begins at the process, using intelligent devices capable of continuously monitoring device and loop health. This includes detecting conditions such as a sticky valve, low actuator air supply pressure, or a failed temperature sensor.

Who should be informed — and how — depends on the nature of a detected problem. For gradual deterioration that could lead to a problem in the future, an automatic e-mail to the maintenance team could enable them to schedule repairs appropriately. Situations that pose a near-term threat to the process or SIS reliability, on the other hand, could generate an immediate alarm to alert operators so they can take corrective action.

In all cases, creating a hard-copy record of the problem may be required to satisfy regulatory reporting requirements.

### The PlantWeb Advantage

PlantWeb Alerts notify the right people of potential problems — without flooding operators with nuisance alarms. This capability relies on diagnostics in Emerson's intelligent field devices, AMS™ Suite: Intelligent Device Manager software, and the DeltaV™ system to immediately analyze the incoming information, categorize it by who should be told, prioritize it by severity and time-criticality, and then not only tell the recipients what's wrong but also advise them what to do about it — in clear, everyday language.

With the optional SIS Reporting Messenger plug-in, detailed SIS diagnostic test results from actuator partial-stroke tests, sensor tests, and SIS loop health tests are automatically transmitted and printed.

## Summary

In this course you've learned that:

- The primary physical components of an SIS are sensors, logic solvers, and final control elements.
- Essential components and subsystems are those necessary to carry out the safety instrumented function. They must meet SIL requirements.
- Non-essential components and subsystems provide support to engineer or maintain the SIS, but they don't interfere with its functioning. They *don't* have to meet SIL requirements.
- Essential SIS components must be either certified or proven in use. Which approach is best usually depends on the complexity of the device and whether you have sufficient prior-use data.
- A component's or system's probability of failure on demand (PFD) affects its ability to provide the needed risk reduction and safety integrity level (SIL).
- More-frequent proof testing can reduce PFD, and partial-stroke testing can extend the intervals between full proof tests.
- Intelligent alarms help inform the right people when there's a potential problem with the process or system.