

SIS 102 - Reducing Risk

15 minutes

In this course:

- 1 Overview
- 2 Necessary Risk Reduction
- 3 Safety Integrity Level (SIL)
- 4 Protection Layers
- 5 Safety Instrumented Systems
- 6 Putting It All Together
- 7 Summary

Overview

In the previous course we learned that **inherent risks** are those present in the process itself (including equipment and materials), and **tolerable risks** are defined by the number and frequency of injuries, deaths, and financial losses we are willing to accept.

When inherent risk is greater than tolerable risk, the first choice should be to eliminate the risk. If it can't be eliminated, it must be **minimized or mitigated** — by active means such as relief valves or safety systems, or by passive means such as containment dikes or bunds.

But how safe is safe enough?

Without a good understanding of the risks, there's a temptation to over-engineer risk-reduction solutions, which can eat into profits. The potential costs of *under-engineering* safety can be even higher.

That's why it's important to identify **how much** the risks need to be reduced, and then design a solution that delivers the **appropriate level** of protection. Those are the topics we'll focus on in this course.



Hint

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

- The two approaches to determining necessary risk reduction
- The purpose of safety integrity levels
- How safety layers prevent or mitigate risks

- What constitutes a safety instrumented system

Necessary Risk Reduction

How much do we need to reduce the risk? There are two ways of finding an answer: quantitative and qualitative.

Quantitative. We could quantify all the inherent risks that are associated with each hazardous event and compare the sum to the level of risk that has been defined as tolerable.

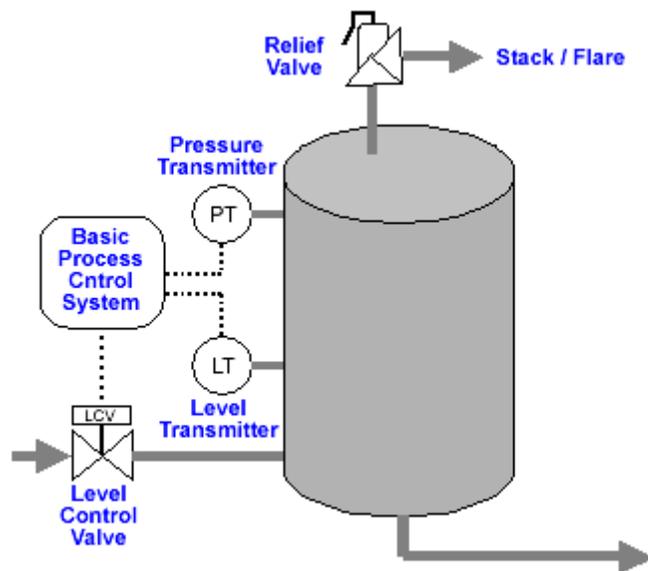
For example, we may want to reduce the frequency of a fatality from once every 10 years to once every 10,000 years. In other words, we want to reduce risk by a factor of 1000 — which is why you'll frequently see references to the **risk reduction factor** or **RRF**.

Although this approach is used increasingly often, it raises two challenges.

- You need to collect a lot of data to make the calculations meaningful.
- You have to express specific, quantified levels of risk that you're prepared to tolerate, such as one severe injury per year. That can make people — and companies — uncomfortable.

Qualitative. The second way of assessing the required risk reduction is to use qualitative rankings like those in the example **consequence** and **likelihood** models introduced in SIS 101.

Remember the ammonia tank example in that course? There we defined the likelihood of a tank rupture as "medium" and the consequence as "serious."



There are several ways to do this qualitative assessment, including risk graphs and hazard matrices. For example, we can use a hazard matrix like the one below to identify the required level of risk reduction — in this case, level 2.

Likelihood	High	2	3	Risk too high -- redesign process
	Medium	1	2	3
	Low	Not required	1	3
		Minor	Serious	Extensive
		Consequences		

Typically, corporate risk management personnel develop these matrices and the guidelines for using them. The values in the matrix are called safety integrity levels, or SILs. The next topic explains what the matrix numbers mean.

Safety Integrity Level (SIL)

The Safety Integrity Levels shown in the preceding matrix identify the level of **risk reduction** required for a particular **safety function**.

(A **safety function** is the capability to reduce or eliminate the risk of a specific condition or hazard. In our ammonia tank example, it's the capability to prevent an over-pressure condition from rupturing the tank.)

Each SIL is defined as a range of risk reductions arranged in orders of magnitude (which avoids splitting hairs):

Safety Integrity Level	Target Risk Reduction Factor
4	>10,000 to \leq 100,000
3	>1,000 to \leq 10,000
2	>100 to \leq 1,000
1	>10 to \leq 100

Adapted from IEC 61511-1 Table 3
NOTE: SIL 4 rated applications are not typically used in the process industries, and the standards caution that a single programmable system shouldn't be used for SIL 4 applications.

This permits us to establish the required SIL in one of two ways:

1. We can assess the consequences and likelihood of a hazard in qualitative terms, as we did on the preceding page of this course. That gives us a broad spread of required risk reduction. For example, a qualitative evaluation that indicates SIL 2 requirement means we need to reduce risk by a factor between 100 and 1000.
2. We can precisely calculate the required risk reduction, which gives us the SIL of the safety function in question. For example, if our calculations indicate our required risk reduction factor is 500, then we know we need to provide a SIL 2 level of protection.

A key benefit of the IEC 61511 standard is that it helps end users implement the **appropriate level of safety at the lowest cost**. Accurately evaluating the risks and determining the appropriate SIL assignment for each safety function helps you avoid investing in more — or less — protection than you need.

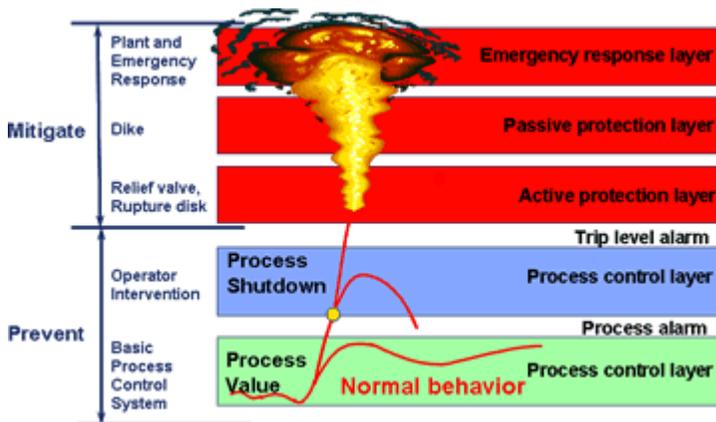
Protection Layers

So how do we achieve the necessary level of risk reduction? By adding **protection layers**.

Safety standards define a protection layer as "any independent mechanism that reduces risk by control, prevention, or mitigation." The sum of the protection layers provides what is called **functional safety** — the functionality that ensures freedom from unacceptable risk.

Control of the process (to avoid situations that could lead to incidents) is usually provided by a Basic Process Control System (BPCS). The BPCS is any system that responds to input signals in order to control a process. It's most often based on loop controller(s), a DCS, PLC, or a hybrid automation system.

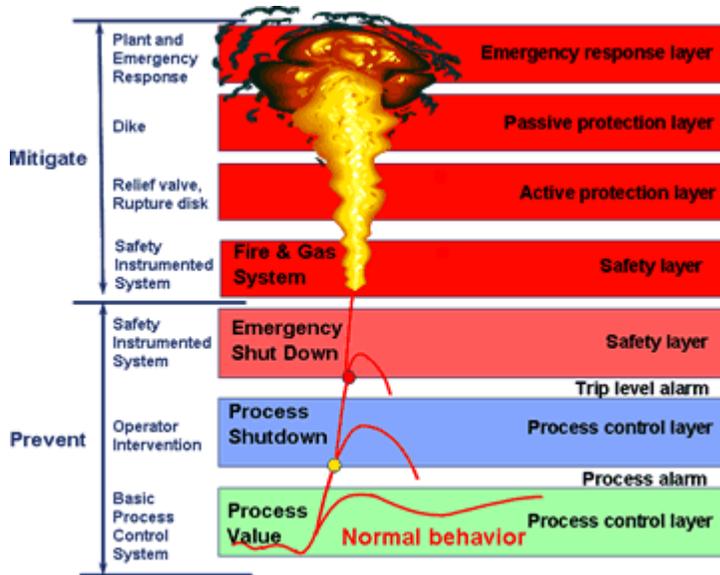
Additional, independent protection layers for **prevention** and **mitigation** might include those shown in this diagram.



The ammonia tank example already has a BPCS and a relief valve installed. The BPCS helps prevent conditions such as tank overpressure that could lead to a release. The relief valve does its job by venting excess ammonia vapor to the stack/flare — avoiding a tank rupture and major spill, but with the risk of exposing plant personnel and the public to harmful ammonia vapors.

What we need is another layer of protection, one that will prevent the situation from reaching a point where the relief valve is needed. That layer is a **safety instrumented system (SIS)** — a term encompassing solutions that may also be called emergency shutdown systems, safety shutdown systems, fire and gas systems, or burner management systems.

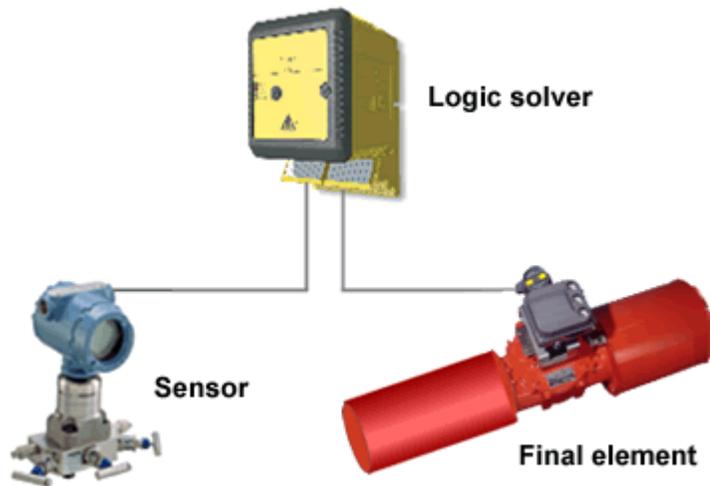
(continued on next page)



Safety Instrumented Systems

The safety instrumented system (SIS) provides an independent protection layer that is designed to bring the process to a safe state when a hazardous condition occurs. Where used, it's an integral part of plant operations and, for some plants, may be a regulatory requirement.

An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s). All three components must be present — and working properly — for the system to do its job.



Despite its structural similarity to a basic process control system, the SIS is fundamentally different from the BPCS. The BPCS exists to produce a quality product by keeping the process running smoothly. The SIS, on the other hand, exists to monitor for unsafe process conditions and take appropriate action — typically, shutting down the process.

The SIS is also separate from the BPCS. This separation reflects not only their different functions, but also the importance of maintaining SIS integrity even when the BPCS is changed frequently. Safety standards do permit carefully controlled communications to occur between components and systems, so it's permissible to

implement an integrated, yet separate, BPCS and SIS installation.

The PlantWeb Advantage

Emerson has extended the proven innovations of its PlantWeb digital architecture to safety instrumented systems.

Emerson's smart SIS is the first to provide an integrated approach to complete safety loops — from sensor to logic solver to final control element — so you can avoid the risks and headaches of piecing together independent components.

It's also the first to use digital intelligence to enable more automated safety loop testing, equipment diagnostics, and other features that increase system availability while reducing life-cycle costs and easing regulatory compliance.

Intelligent design also enables appropriate levels of integration with Emerson's DeltaV digital automation system when it is used as the BPCS — for example, using the same operator interface and configuration tools — while maintaining the separation required by safety standards.

Putting It All Together

Let's see how everything we've learned so far applies to the ammonia tank example.

If the ammonia tank has an overpressure condition (a functional error), functional safety will be satisfied if the prevention or protection systems reduce the tank's pressure to within its established safe operating limits before the mitigation systems are needed.

Earlier in this course, we determined that the functional safety target for the ammonia tank's SIS is SIL 2. This means that the target level of risk reduction must be between 100 and 1000.

We'll consider that the BPCS adds some level of risk reduction, although IEC 61511 tells us that the maximum level of risk reduction from a non-safety-related control system is a factor of 10.

Although we don't want to incur the expense of over-engineering the SIS, we also want to make sure we have adequate protection. So we'll be slightly conservative in our assumptions:

1. Total required Risk Reduction Factor (RRF) = 1,000
2. Risk Reduction Factor assigned to BPCS = 2
3. The relief valve will not be considered, because if it activates there's a risk that students at the nearby school will be exposed to the escaping ammonia vapors.

The total RRF is the product of the RRFs of all independent layers of protection. In our example, the RRF required of the new SIS therefore becomes $1,000 / 2 = 500$, which still corresponds to a SIL 2 rating (between 100 and 1,000).

Reducing the risk by less than this will lead to an intolerably high probability of a hazard. But implementing a higher-rated safety function (for example, one that provides SIL 3 protection) adds unnecessary costs for designing, purchasing, installing, testing, and maintaining the SIS.

Summary

In this course you've learned that:

- Necessary risk reduction can be determined using either quantitative or qualitative methods.
- Safety integrity levels (SIL) are statistical representations of the risk reduction needed to reach tolerable risk
- Independent protection layers are the mechanisms that control, prevent, or mitigate a hazardous condition.
- A safety instrumented system (SIS) uses sensors, logic solvers, and final control elements to monitor the process for unsafe conditions, and take it to a safe state if needed.