SIS 101 - What is Risk?

15 minutes

In this course:

Overview

Implementing a safety instrumented system (SIS) can be a big job. Considering the importance of plant safety, it's also a task you want to get right the first time. If you understand the basic concepts of plant safety and safety instrumented systems before you begin, you'll have a better idea of where you're headed and what kinds of questions to ask yourself and others as you proceed.

This course introduces perhaps the most basic of those concepts: risk. We'll address the kinds of risks typically considered in plant safety programs, as well as how such risks are identified and evaluated.

Hint

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

- The two parts of identifying hazardous risks
- What makes up inherent risks
- How risks are quantified
- Who determines tolerable risk

What's at Risk

In safety standards such as IEC 61511, what's at risk is identified as **personnel** and the **environment**. However, most companies use an expanded list of **risk categories** that can also include:

- Public safety and health
- Liability costs
- Production interruptions and quality issues
- Equipment damage and repair costs

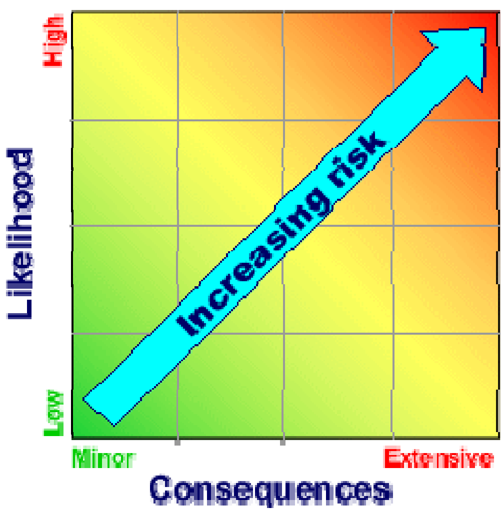
What is IEC 61511?

IEC 61511 - which you'll learn about in SIS 103 - is an international safety standard issued by the International Electrotechnical Commission. Although the IEC is based in Switzerland, its standards are used in the whole world - not just Europe. The IEC standard that most of us in process automation are familiar with is IEC 61131-3, which describes control system programming languages.

Identifying Risks

A key step in maintaining or improving safety is to identify the risks that threaten it.

As the diagram indicates, identifying risks requires answering both parts of the question, "What's the **likelihood** a harmful event will happen, and what are the **consequences** if it does?"



Risk is determined by both the likelihood and the consequences of an event.

The challenge is to identify risks in advance so that they can be reduced or eliminated – for example, by changing a product's formulation or reducing the quantities of hazardous material present.

The task of identifying and ranking risk is often done in stages of increasing thoroughness. The following table lists some of the more common techniques.

Risk identification techniques	When you might use them
• Safety Review • Checklist • Preliminary Hazard Analysis • What-If • Abbreviated HAZard and OPerability (HAZOP) study	Used in preliminary hazard evaluation studies to provide a general overview of existing risks. (Usually not too time consuming.)
• What-If/Checklist • Detailed and complete HAZOP study • Failure Mode and Event Analysis	Used to develop a more detailed analysis of potential risks.
• Fault Tree Analysis • Event Tree Analysis • Cause Consequence Analysis • Human Reliability Analysis	Used in conjunction with quantitative risk analysis to establish a high level of detail about risks. (Usually used only for specific areas or unit operations.)

Inherent Risk

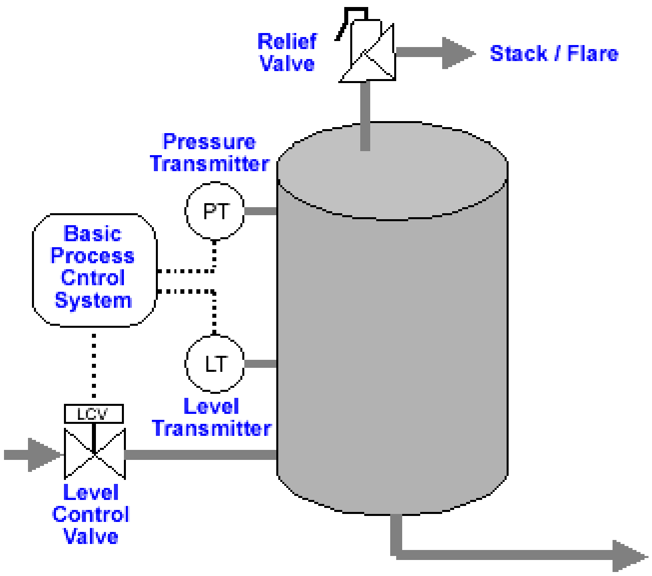
Most process facilities have many pieces of equipment that each contribute to what's called **inherent risk** – in other words, risk that exists because of the nature of the process, including the equipment and materials present.

For example, the inherent risks of riding in a car include accidents caused by driver errors, flat tires, or (however unlikely) fuel fires.

Evaluating the entire process helps determine the **likelihood** of an occurrence, and evaluating the materials (type and quantity) helps determine the **consequences** of the risk.

Let's see how inherent risk applies to a process industry example – a pressurized vessel containing ammonia.

(continued on next page)



Looking at the entire process reveals several inherent risks that could lead to an ammonia release, including possibilities for:

- Tank rupture from overpressure and/or seam failure
- Leaking at pipe joints, valve packing, and/or sensor taps
- Failure of the transmitters, control valve, and/or basic process control system (such as a DCS or PLC) to maintain the correct volume and pressure in the tank

Each of these risks has a **likelihood**. The **consequences** depend largely on the dangers of human exposure to ammonia – including eye and respiratory system irritation.

Assessing Risk

Assessing risk, though potentially subjective, is usually done using an established corporate risk **assessment model** developed by competent people – such as engineers, chemists, and lawyers – who are trained to assess and quantify cause, effect, and liability.

Developing a risk assessment model for each at-risk category requires establishing a **consistent means of describing** both an event's *likelihood* (frequency) and its *consequence* (severity). When developing risk assessment models, it's a good idea to use broad quantifications – such as orders of magnitude rather than exact values – to avoid getting bogged down "splitting hairs" about overly precise levels of risk.

Likelihood. The consequences of an event can be severe, but the likelihood of its happening may be low. To ensure that different groups of people within the same company establish approximately the same risk rankings for similar events, the model should include a consistent, quantified measure of event likelihood or frequency. For example, a low likelihood might be defined as less than 1 chance in 10,000 of the event occurring during a year.

Sample likelihood risk assessment model:	
Likelihood	**Type of events**
Low (e.g., less than 1/10,000 annually)	Events such as multiple failures of diverse instruments or valves, multiple human errors in a stress-free environment, or spontaneous failures of process vessels.
Medium (e.g., 1/10,000 - 1/1000 annually)	Events such as dual instrument or valve failures, or major releases in loading/unloading areas.
High (e.g., more than 1/1000 annually)	Events such as process leaks, single instrument or valve failures, or human errors that result in small releases of hazardous materials.
Adapted from IEC 61511-3, Table C.1 - Frequency of hazardous event likelihood	

Consequence. The model should also include a way of evaluating and defining the consequences for each at-risk category. For example, the table below shows one way consequences might be defined in terms of number of injuries or amount of property damage.

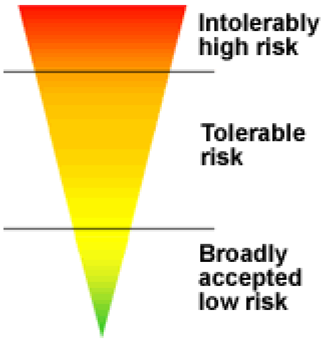
Sample consequence risk assessment model:	
Consequences	**Impact**
Minor (e.g., injury or more than $120,000 of damage or lost production)	Minor damage to equipment. No shutdown of the process. Temporary injury to personnel and damage to the environment.
Serious (e.g., hospitalization or more than $250,000 of damage or lost production)	Damage to equipment. Short shutdown of the process. Serious injury to personnel and the environment.
Extensive (e.g., death or more than $1,000,000 of damage or lost production)	Large-scale damage to equipment. Shutdown of a process for a long time. Catastrophic consequence to personnel and/or the environment.
Adapted from IEC 61511-3, Table C.2 - Criteria for rating the severity of impact of hazardous events.	

For the ammonia tank example, the **likelihood** of an ammonia release is determined by combining the likelihood of risks like those listed in "Inherent Risks." In this case, we've determined that the total risk of leaks is **medium** (between 1 chance in 1000 and 1 chance in 10,000).

The **consequences** of such an event are determined primarily by the amount of ammonia released and resulting potential for affecting plant personnel and the public. In our example, we've determined that a tank rupture and resulting ammonia release would be considered **serious**.

This relatively simple model is only one example of how risk might be assessed. We'll look at another, more quantitative model in SIS 102.

Tolerable Risk



We all know there is a point where risk becomes "intolerably high." Likewise we know there's a point where risk becomes broadly accepted as negligible. Between those two points is the **tolerable risk** area.

Each of us makes decisions about what constitutes tolerable risk in our own lives – for example, deciding to stop or go through a traffic light that just turned yellow. (Traffic fatality risk is 2 in 1,000 person years.)

In a process plant, workers are often exposed to multiple and simultaneous risks. The purpose of a plant safety program – including safety instrumented systems – is to ensure this exposure is tolerable at all times.

So what are the appropriate numbers for tolerable risk in a plant environment? There is no one "correct" answer; the plant owner/operator must decide the tolerable risk criteria for the plant.

IEC 61511 describes tolerable risk as *risk which is accepted in a given context based on the current values of society*. Most companies include injuries, deaths, and dollars among the factors they consider. "Best estimates" of what constitutes tolerable risk may be based on research results of similar circumstances and events at other sites and industries. Other times, tolerable risks are available from sources such as U.S. Occupational Safety & Health Administration (OSHA), the American Conference of Governmental Industrial Hygienists (ACGIH), the U.S. Environmental Protection Agency (EPA), or similar agencies in other countries.

Some references list the highest points of tolerable risk as 1 fatality per 1,000 years of exposure for workers, and 1 fatality per 10,000 years of exposure for the public. Those same references rate 1 fatality per 100,000 years of exposure as negligible risk. However, individual world areas, countries, and companies frequently apply lower acceptable risk numbers.

Tolerable risk is determined by consequences as well as likelihood. For the ammonia-tank example, we'll use locally acceptable levels of human exposure to ammonia. For site workers in the U.S., OSHA says the maximum exposure is an atmospheric concentration of 50 parts per million (ppm) over an 8-hour period.

Other limits may also have to be considered. For example, what if there's a school nearby? For public exposure, the ACGIH allows only 25 ppm of ammonia over the same time period.

Numbers like these help determine the **necessary risk reduction** an SIS must achieve – which we will address in the next course.

Summary

In this course you've learned that:

- Risks consist of likelihood and consequences.
- Inherent risks are those present in the complete process, including equipment and materials.
- Quantifying risk requires using an established risk assessment model.
- Tolerable risks are the numbers of injuries, deaths, or dollar loss (and their frequency) that we are willing to accept.