WHITE PAPER

Selecting Safety Components Properly

Facility, system, and machinery safety are important factors to prevent injury and loss of productivity in the workplace. Safety component ratings ensure that the proper device is selected for your application. Understanding these ratings will make this decision much easier.

By Kevin Kakascik, AutomationDirect

AUTOMATIONDIRECT.com
The #1 Value in Automation.™

WHITE PAPER

If you've been working with industrial automation equipment for any length of time, you've likely seen various ratings and certifications from different agencies. The more common ones are UL, cUL, CE, CSA, and IEC. When you are browsing the spec sheet of a safety component, there will be additional ratings that look like the chart below.

Safety Data - Values per EN ISO 13849-1	
Category	Up to 4
Performance Level	PLe
$MTTF_d$	220.9 years
DC_{avg}	99%
Safety Data - Values per IEC/EN 62061 / IEC/EN 61508	
SIL	Up to 3
HFT (Hardware Failure Tolerance)	1
DC_{avg}	99%
SFF	$1.08E^{-10}$
PFH_D	$5.81E^{-5}$

Figure 1: An example of a component's safety ratings from its specification sheet

Safety ratings aren't that complicated, and this white paper will explain them, so you have a better understanding.

Before beginning, it is important to perform a safety risk assessment and an audit of your facility and the equipment around which you intend to design a safety system. Without this step, you won't have the knowledge required to select products, and the safety specifications won't mean anything.

Proper safety device selection requires a comprehensive risk assessment as the foundation. Only after hazards are identified and evaluated can the appropriate safeguarding devices be specified.

WHITE PAPER

Figure 2: A safety risk assessment is the first step in selecting the appropriate safety components

This can be done in-house, but if you've never done it before, it's best to hire an independent contractor to perform the service with you. It will typically involve a team of employees familiar with the facility, system, and machinery, in conjunction with the person performing the assessment. Hiring an experienced safety auditor is often the best route, especially when someone's life could depend on it.

Most likely, you will be following ISO 13849-1, and during this study, a Required Performance Level, denoted as PLr, will be determined. This can be calculated by quantifying the Severity of Injury (S), the Frequency/Exposure (F) to the hazard, and the Possibility of Avoidance (P).

The Severity of Injury (S) can be two levels:

- S1 means that the severity is slight and normally a reversible injury.
- S2 is serious, which is an irreversible or permanent injury, up to and including death.

Frequency/Exposure (F) also has two levels, where:

- F1 means the frequency of exposure is seldom, and/or the exposure time is short.
- F2 is continuous, or the exposure duration is long.

Lastly, the two levels for the Possibility of Avoidance (P) are:

- P1, where the hazard can possibly be avoided under specific conditions.
- P2, where avoiding the danger is nearly impossible.

As you may notice, these levels are subjective and not definitive. For example, with a hazard that can cut skin, would the Severity of Injury be defined as S1 or S2? While the cut itself will heal, it might scar, and therefore some people might consider this to be S2 because the scar is irreversible. Because of this ambiguity, the answer to this may vary from company to company, and possibly even site to site. The key here is consistency. Your team needs to come up with clear documentation on how the severity is defined.

We have to remember that the only way to make a machine 100% safe is to use hard guarding and put it in an inaccessible room; however, the machine would not be usable, there would be no way to feed it raw materials or get finished goods out, not to mention there is no way to clear a jam. For this reason, the Required Performance Level is going to reflect the amount of acceptable risk to that company.

Once you have these three levels determined for each hazard, you can graph them out, as shown below, to calculate the PLr.

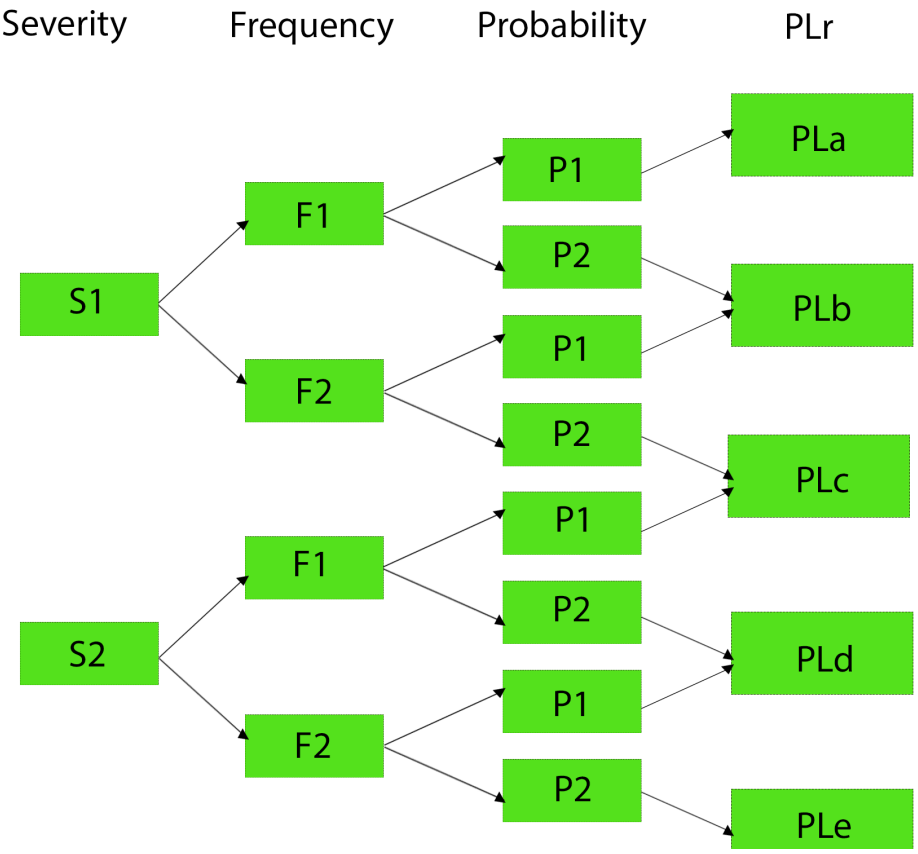

Figure 3: Graph to calculate PLr from risk assessment data

This chart from ISO 13849-1 shows how to determine your system's PLr. The PLr will be expressed as PL, followed by a lowercase letter a through e. Only after you've completed your safety risk assessment and consulted with this chart, will these certifications actually mean something.

PLr	Description of Required Performance Level
PLa	Low risk reduction
PLb	Low-to-medium risk reduction
PLc	Medium risk reduction
PLd	High risk reduction
Ple	Very high risk reduction

Figure 4: PLr chart from ISO 13849-1

It's worth noting that if you are following IEC 61508 and 62061, then instead of working with Performance Level, you will be working with Safety Integrity Level, expressed as SIL. SIL is ranked from 1 through 4 and is another valid certification method. However, most facilities in the United States follow ISO 13849-1, so Performance Level is the more common method used for risk assessment and component selection.

European installations and some process facilities in the United States will use IEC 61508. In those instances, SIL will be pertinent and determined during the safety risk assessment in place of PLr. Safety Integrity Level is the probability that a safety system's performance will function properly over time.

The definition of SIL includes the word "performance," and that's no coincidence, since PL and SIL do overlap when it comes to their application, but they are distinct ratings. SIL is defined in IEC 62061 for Process/Machine, and PL is described in ISO 13849-1 for Machinery.

PL pertains more to architecture, while SIL is based on the probability of failure. Safety Integrity Level requires the statistical models of failure rates, if failures can be detected, and if failures will result in an unsafe condition. Because of this, it is more suited for continuous process applications instead of discrete machinery.

Below is a chart explaining the different levels of SIL ratings and their usage.

Level	Description	Typical Use
SIL 1	Basic risk reduction	Low-risk systems
SIL 2	Moderate	Industrial applications
SIL 3	High	Critical systems
SIL 4	Very high	Specialized industries

Figure 5: SIL chart from IEC 61508

Both PL and SIL are dependent on a component's safety Category. Category is defined in ISO 13849-1 and specifies the circuit architecture. These categories are B, 1, 2, 3, and 4. Categories B and 1 are the lowest level of safety architecture and are reserved for single-channel devices. The difference between Cat B and Cat 1 is that Category 1 uses more reliable components. The remaining Categories, 2 through 4, are dual-channel components with varying levels of diagnostic coverage, such as cross-fault detection. Category 4 is the highest level of diagnostic coverage.

What is significant about Category is that only a certain level of PL and SIL can be achieved from lower categories. The person who is responsible for selecting the components can judge whether a device will meet the required PL or SIL rating quickly without diving deep into the specifications of a product. The following chart shows the maximum realistic levels of PL and SIL that can be achieved from each Category level.

Category	Achievable PL	Achievable SIL
Cat B	PLa or PLb	SIL 1
Cat 1	PLc	SIL 1
Cat 2	PLd	SIL 2
Cat 3	PLd or PLe	SIL 3
Cat 4	PLe	SIL 3

Figure 6: Maximum achievable PL and SIL for each Category

Note that SIL 4 isn't mentioned in the chart. This is because it is the highest level of integrity defined in IEC 61508 and is not in IEC 62061. It is rarely used and not affordable or realistic for most applications and facilities. SIL 4 would normally only be applied in specialized situations such as nuclear facilities or aerospace.

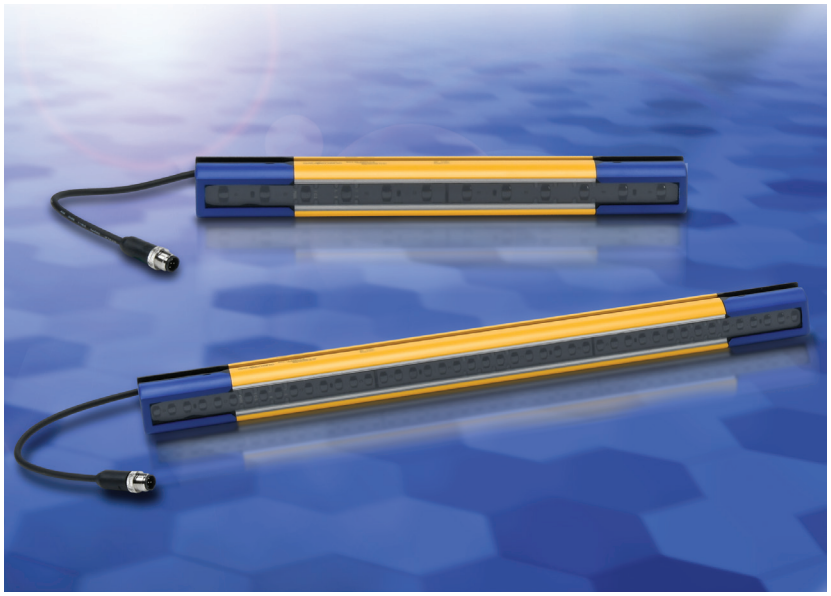

Figure 7: A Type 4 light curtain provides the highest structural rating of any safety device.

PL is based on the qualitative risk assessment and analyzes the capability of safety-related components of a safety control system to perform a safety function under predicted conditions. These ratings are also denoted as PLa, PLb, PLc, PLd, and PLe, with PLa being the lowest and PLe being the most capable.

It is also important to note that simply throwing components together in a system or machine with appropriate safety ratings will not make it safe. The system's design needs to ensure they will operate as intended. This is where an experienced machine safety specialist comes in. If you don't have someone in-house to design the system, hiring an outside safety engineer is a great idea.

Figure 8: These Safety Extension Relays are rated for Category 3, PLe, SIL 3, but if they are used by themselves alone as a safety relay, it will be impossible to reach the required PL ratings.

WHITE PAPER

Where do these component ratings come from?

Looking at Figure 1, you'll see that additional specifications were provided. These are $MTTF_d$, DC_{avg}, HFT, SFF, and PFH_D.

$MTTF_d$ is the Mean Time to Dangerous Failure, which estimates the average time until a device fails to a hazardous state. The component manufacturer provides this rating.

DC_{avg} is the Average Diagnostic Coverage, which is determined on the component level by the manufacturer, but for a system, this falls to the integrator or machine builder. It is based on $MTTF_d$ data and the certainty that, in the event of a component failure, the device's self-diagnostic or the system's ability to detect the fault will put the device, machine, or system into a safe state. This value will be determined based on both the definition from ISO 13849-1 and IEC 62061. This value will usually be listed twice on a device's spec sheet. Often, they will be the same value, but in some cases, they will differ due to various standards.

HFT, or Hardware Fault Tolerance, is certified by an independent agency. This describes the component's ability to operate safely, even in the event of a fault condition. This value is expressed as a number:

- 0 indicates no fault tolerance, and a single fault will result in a hazardous condition
- 1 means there is redundancy and the system can tolerate at least one fault and still operate safely.

This metric is primarily used for SIL determination.

Safe Failure Fraction, listed on specification sheets as SFF, is a measure of a component's likelihood of failing in a state that doesn't compromise safety. The definition of this metric from IEC 61508 is the ratio of safe failures and dangerous failures detected divided by the total failure rate. This value is determined by a 3rd party agency and is used as part of the component's SIL determination. Since this is a ratio, the final spec is expressed as a percentage, with the most common values being 60%, 90%, and 99%. The higher the number, the less likely the device is to fail in an unsafe state.

PFH_D, or Probability of Dangerous Failure per Hour, is another metric used to establish a device's SIL per IEC 62061. It is also governed by a 3rd party agency. This rating is quantitatively determined by the rate of random hardware failures that could cause a system to stop operating as a functional safety device. This value is also used to determine a component's PL per ISO 13849-1. This is usually expressed as an exponential range, from 10-8 to 10-5, and relates to SIL: the lower the PFH_D value, the higher the safety rating. So, the lower the PFH_D (Probability of Dangerous Failure per Hour), the safer the product.

WHITE PAPER

Safety Certification Agencies

These ratings, except for $MTTF_d$ and DC_{avg}, are certified by various agencies or labs, such as TÜV Rheinland, TÜV SÜD, CSA, UL, Bureau Veritas, and DNV. OSHA enforces safety standards in the United States. Typically, OSHA only gets involved after an incident or complaint. It's best to avoid accidents or unsafe conditions, so as previously mentioned, performing a proper risk assessment or hiring someone to do so is extremely important.

Making these ratings work with your system design

Based on the results of the safety risk assessment performed, you will have either a qualitative or quantitative requirement for either the minimum PL (PLr) or SIL rating of all components required. Be sure to select components at or above the level of your safety assessment results. Then verify that your system meets the requirements needed.

Say the results of your qualitative assessment require a PLr of d or greater. A component rated Category 3 and PLc wouldn't be appropriate for the system. However, a device rated for Category 4 and PLe would certainly be acceptable if the rest of the architecture is correctly designed.

Application Example—Automated Sawmill

The proposed system is a saw that will rip (cut lengthwise) the same-length logs that are being fed to it from a simple conveyor. The conveyor will be loaded from existing equipment that has already been validated through a safety risk assessment. This means that the feed conveyor and saw will need to be assessed separately.

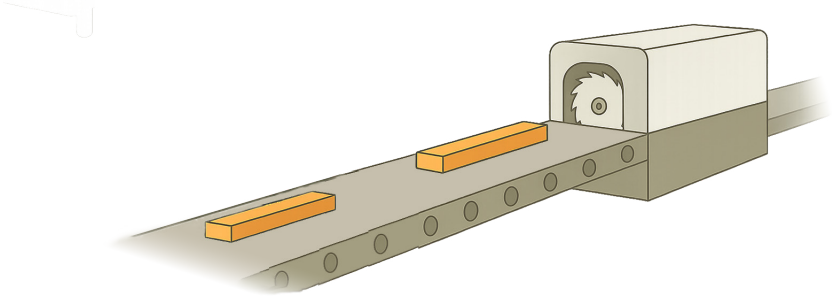

Figure 9: Illustration of proposed sawmill addition

For the saw, we understand how dangerous it can be. However, every part of the equipment will be protected by physical barriers except for the entrance and exit. The saw is also equipped with its own safety system and an external safety interlock as an added feature. If the safety interlock signal is removed, power will be removed from the saw blade motor, and a built-in clutch/brake will cease motion of the spinning cut hazard. The saw will also be locked out and unable to restart.

A quick check of the internal safety components of the saw tells us that the components are rated for Category 4, PLe, and SIL 3. However, we still need to protect the entrance and exit of this machine.

The feed conveyor will have workers constantly walking around it, clearing jams that occur from the boards, and moving other equipment, but this machinery appears less lethal to everyone.

During the safety risk assessment, the committee agrees on the severity of a potential injury, the frequency of the risk, and the possibility of avoidance for both pieces of equipment.

For the saw, the risk assessment determined that the severity would be S2, as any injury would most likely be permanent; the frequency would be F2, since the saw is running non-stop, but the possibility of avoiding the hazard is P1, because the hazard is easily avoidable. In fact, a person would need to access the saw's entrance or exit to get injured. Graphing these levels using the chart in Figure 3 gives a PLr of PLd for the saw.

Next, the PLr for the conveyor can be determined. This time, there was some disagreement on the severity of the injury. Half of the committee stated that any injury inflicted by the conveyor would be reversible; however, the others argued that the belt pulley could amputate a finger. S2 was the final determined severity for the conveyor. Everyone agreed that the Frequency of the hazard was continuous and assigned F2. The risk assessment team was split on the possibility of avoidance, so to be conservative, everyone voted to raise this to a P2 level. Graphing this out using Figure 3, the PLr ends up being PLe.

Even though the hazards for the conveyor seem less severe, it was determined in the end that this piece of equipment had a higher PLr due to its accessibility. For device selection, the designated safety engineer decided on a safety light curtain with muting capability to protect the entrance and exit of the saw, making sure that the device met a minimum of Cat 3, PLd. The conveyor was protected by a cable pull safety switch with a minimum safety rating of PLe, Category 3 or 4 to cover the perimeter of this section.

Figure 10: Cable pull safety switch

WHITE PAPER

About AutomationDirect

Since 1994, AutomationDirect has been a distributor offering thousands of industrial automation products for electrical control systems, including PLCs, operator interfaces, AC drives, motors, stepper systems, sensors, safety components, motor control, enclosures, and more. Their prices are typically well below the list price of more traditional automation companies because of their model and focus on efficiency. Most of their products are stocked for same-day shipping. Plus, get free two-day delivery on orders over $49; some limitations apply.

For more information, contact them at 800-633-0405 or visit *www.automationdirect.com/safety*