White Paper

Equipment Safety

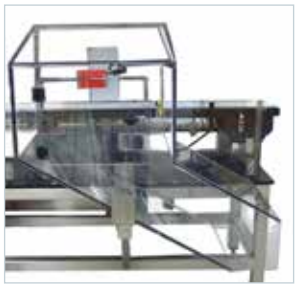
For Product Inspection Equipment

Content overview

This paper is intended as a general guide on the topic of equipment safety, for users and suppliers of product inspection equipment. It should be thought of as a framework for discussion on the topic, assisting both users and suppliers in meeting their shared responsibility for equipment safety. It presents current thinking on the topic. Standards are under continual review and modification. Each application presents its own unique challenges, which may require tailored solutions and interpretations.

METTLER TOLEDO

Why a Discussion on Safety for Product Inspection Equipment?



The standards for equipment safety cover the full range of industrial equipment. A significant part of that is packaging equipment, and a further subset of packaging equipment is product inspection equipment. Within a packaging line with fillers, cartoners, case packers, etc., some of these machines are at the $1M level. Product inspection equipment is a relatively small part of the line as far as the equipment investment is concerned, but it is no less important. All companies, regardless of size using product inspection equipment as standalone devices need to ensure the equipment is safe for use. Product inspection equipment serves as the eyes and ears. Your eyes and ears are only a small part of your overall being, but you appreciate their importance.

Regardless the monetary value or the size of a piece of equipment, the safe use of a simple conveyor is just as critical as the safe use of a palletizer. The same rules apply to all equipment. By reviewing and understanding the safety standards, the user is able to determine which portions apply to the products provided, and focus on those areas to provide a better, safer product. With better knowledge of the standards, the equipment involved, and the needs of customers, smart application of the standards supports solutions that are suitable for a wider range of territories and not focused on only one part of the globe.

What is Safe?

The U.S. safety standard for packaging machinery, ANSI B155 – 2011, states in its foreword, "There is no such thing as being absolutely safe, that is, a complete absence of risk…. All machinery contains hazards, and some level of residual risk."

> "Safe" is the state of being protected from recognized hazards likely to cause serious physical harm. There is no such thing as being absolutely safe, that is, a complete absence of risk, and therefore there is no machinery, including packaging machinery, that is absolutely safe in the sense of being completely devoid of all conceivable risks. However, the risks associated with those hazards should be reduced to an acceptable level. To achieve this goal, senior management should allocate appropriate personnel, time and resources to permit the risk assessment process to be successfully completed. Senior management holds the ultimate responsibility to determine the level(s) of acceptable risk. - ANSI B155 – 2011

Every human being encounters hazards each day and we manage to identify the hazards, determine the risks, and decide on actions to reduce the risk to acceptable levels. Crossing a street involves potential hazards and harms, evaluation of consequences, and methods to reduce risk to an acceptable level. Those are the elements of a risk assessment.

The notion of "zero access" and "perfectly safe" are nice goals, but unrealistic. Access to a machine is necessary to operate, clean and maintain the machine. For a packaging machine, material must go into the machine and go out of the machine.

The determination of "safe" is a judgment shared by the supplier and the user, and this is reinforced with various standards. According to ANSI B155, the information discovered in the supplier's "hazard-based" risk assessment should be used as the starting point for the user's "task-based" risk assessment. A clear statement of what the supplier is providing is the first, and most important, step in this communication effort. The risk assessment is one communication tool, along with the manuals, drawings, and the safety circuit documentation, that allow the supplier to assist the user in understanding how the machine is constructed.

What Do Customers Expect?

In addition to safe equipment, customers have a reasonable expectation of knowing:

- The standards applied in evaluation of the safety of the equipment
- The specifics of equipment construction
- The environments appropriate for the equipment
- The capacities for the equipment
- The hazards present and the residual risks with the equipment
- Their responsibilities for areas of transfers and integration guarding, or other safety measures
- The safety circuit category, how it was qualified, and how it was validated, and how it needs to be maintained

What is Driving the Increased Interest in Safety?

Reputable suppliers and conscientious users have always followed good safety practices. As people have become more aware of potential hazards and methods to provide safe equipment have improved, the meaning of the term "safe" has changed over time.

There are a few notable items that have increased visibility of equipment and workplace safety. OSHA (Occupational Safety and Health Administration) is a government agency, under US law, that makes the employers responsible to provide a safe work environment for its employees. This in turn causes the employers (company responsible for the workplace) to place requirements on their suppliers for safer solutions.

The Machinery Safety Directive in the EU took a different approach, requiring all suppliers to evaluate their products against European Norms (ENs) to ensure the equipment produced was safe. The supplier must make a determination of which Norms are appropriate for the equipment built, and declare conformity, through its officers, that the requirements in the Norms were met.


INTERNATIONAL STANDARD

ISO 13849-1

Safety of machinery — Safety-related parts of control systems —

Part 1: General principles for design

ISO

Insurance companies also play a major role in driving equipment safety requirements. When an insurer (also known as an "underwriter") instructs its insurees that the equipment in the insuree's facility must meet certain industry standards, it indirectly places the requirement on the equipment supplier. UL and NFPA are two such insurer-based organizations, which set standards for equipment suppliers to follow.

Most recently, a worldwide standard, ISO 13849 (Safety Related Parts of Control Systems (SRP/CS)) has piqued interest in machine safety with requirements for safety circuits with a particular "safety category". This standard makes specific requirements for the design and qualification of the combination of components related to equipment safety. ISO 13849 is international in scope, and based on industry need. ISO 13849 requires risk assessment as the initial step in determining the level of safety circuit appropriate for the equipment.

Determination of required performance level (PL_r) For each selected safety function to be carried out by a SRP/CS, a required performance level (PLr) shall be determined and documented. The determination of the required performance level is the result of the risk assessment and refers to the amount of the risk reduction to be carried out by the safety-related parts of the control system. The greater the amount of risk reduction required to be provided by the SRP/CS, the higher the PLr shall be.
- ISO 13849-1, Section 4.3

General Alignment of Countries with Safety Standards

Standards Applied in Various Countries				
EU-Based		**US-Based**	**Countries with Unique Requirements**	**Rest of World**
Austria	Lithuania	Canada	Australia	Those countries not identified in the first three columns generally follow IEC* standards
Belgium	Luxembourg	Chile	Brazil	
Czech Republic	Malta	Colombia	China	
Denmark	Netherlands	Costa Rica	Japan	
Estonia	Poland	Ecuador	Russia	
Finland	Portugal	Mexico	Ukraine	
France	Romania	Panama		
Germany	Slovakia	Peru		
Greece & Greek Cyprus	Slovenia	Philippines		
Hungary	Spain	Puerto Rico		
Ireland	Sweden	Saudi Arabia		
Italy	Turkey	United States		
Latvia	United Kingdom	Venezuela		

*International Electrotechnical Commission

Standards

A standard is a set of requirements for a particular equipment area, with a defined scope of application.

There are two principal spheres of influence for safety standards - The EU and the US.

In the EU, the standards are written by European standards bodies and generally implemented in a country through legislation. In North America, the US standards organizations have the most weight. Other countries have their own standards for workplace and equipment safety, but in general, there is reasonably good alignment to either EU or US requirements.

Common Standards Used in Product Inspection Equipment		
General Directives	Machinery Safety Directive 2006/42/EC, EMC Directive 2004/95/EC, Low Voltage Directive 2006/95/EC	
	EU-Based	US-Based
Machine Safety	EN 12100	ANSI B155 -2011
Electrical Safety	EN 60204-1	NFPA 70, NFPA 79
Risk Assessment	EN 14121	ANSI B11 TR3
Guarding	EN 294, EN 349, EN 953	ANSI B15, ANSI/ASME B20
Lock-out/Tag-out		ANSI Z244
Ingress Protection	ISO 60529, NEMA	
Electromagnetic Immunity	EN 61000-6,2,3,4	
Hazard Warnings	ISO 3864	ANSI Z535
Safety Circuits	ISO 13849-1, -2	

The Machinery Safety Directive is the "parent" document for safety in the EU. It describes a "self-declaration" process, through which the supplier decides the standards that are appropriate for its product, and applies those standards in design and qualification of the equipment. The "self-declaration" results in the tagging of the equipment with the familiar CE Mark. By itself, the Machinery Safety Directive does not provide detailed requirements for safe equipment. It is a general document that directs to more specific directives and standards (Norms), that are appropriate for the equipment being declared.

The process of marking a product CE permits sale of the product in EU countries.

CE Declaration of Conformity	
Type: XS3	
Manufactured by METTLER TOLEDO Complies with the following directives and standards: • European Parliament and Council Directive 2006/42/EC, dated 17-05-2006 for bringing into line the member states' legal and administrative stipulations relating to machines. • Council Directive 2006/96/EC (electrical equipment designed for use within certain voltage limits) • Council Directive 2004/108/EC (electromagnetic compatibility)	
The following harmonized standards were applied:	
EN12100-1	SAFETY OF MACHINERY
EN 12100-2	SAFETY OF MACHINERY
EN 60204-1	ELECTRIC EQUIPMENT OF MACHINERY
EN 61000-6-2	ELECTRO-MAGNETIC IMMUNITY
EN 61000-6-3	ELECTRO-MAGNETIC IMMUNITY
EN 61000-6-4	ELECTRO-MAGNETIC IMMUNITY
EN 13849-1,-2	SAFETY RELATED PARTS OF CONTROL SYSTEM
EN 953	SAFETY OF MACHINERY - GUARDS
ISO 3864	SAFETY MARKINGS
Manufacturer: METTLER TOLEDO, Ithaca, NY USA	

In recent years, there has been a significant amount of "harmonization" that has occurred between the EU and US. This is driven quite a bit by industry itself, seeking to use a common set of solutions, rather than requiring a unique solution for each country. A good example of harmonization is the alignment between EN60204-1 and NFPA 79. These two standards have long been the source for debate between electrical designers in Europe and North America, with some grey areas - and some areas of outright conflict. Today, the organization of the two standards is remarkably similar, and the language used has far fewer differences than before. The key to proper application for equipment that requires compliance in both the EU and North America is a clear, thorough understanding of the differences in the standards.

Topic	**EN 60204 Reference**	**NFPA 79 Reference**
Power Introduction and Disconnect		
Function and type of Disconnect	5.3.5 - Can be a switch, fused or unfused, circuit breaker, or a plug of an accepted form. 5.3.3 - isolate the electrical equipment from the supply 5.5 - for disconnecting electrical equipment to enable work to be carried out without a risk from electrical shock or burn	5.3.3.1(4) - Simultaneously disconnect all ungrounded conductors of the power supply circuit. Can be switched, fused or unfused, circuit breaker, or a plug of an accepted form. 5.5.1 - for disconnecting electrical equipment to enable work to be performed when it is de-energized and isolated.

Understanding the standards is key to proper application. The example above demonstrates how material from two similar standards might be compared to understand how standards are common, and where standards differ.

Safety Organizations

There are two forms of safety organizations involved with equipment safety: statutory, and industry-based.

Statutory organizations are state, or government bodies, usually with the force of law behind them. They are created to construct, implement, and enforce standards for safety. Examples of these are shown in the panel below.

Safety Standards Organizations

ISO	International Standard for Organization	Swiss-based, international, commercial and industrial standards
ANSI	American National Standards Institute	US-based, private, non-profit standards
CEN	European Center for Standardization	EU-based, non-profit, european standards and norms (ENs)
IEC	International Electrotechnical Commission	International, non-profit, electrical standards
NFPA	National Fire Protection Association	US, trade association, standards
UL	Underwriters' Laboratories	US-based (global reach), commercial safety consulting and certification
TÜV	Technische Überwachungsvereine (Technical Inspections Organizations)	EU-based (global reach), commercial safety consulting and certification
BSI	British Standards Institution	UK-based commercial standards group
OSHA	Occupational Health and Safety Administration	US-government agency; oversees workplace safety

Industry-based organizations have no legal authority. They are cooperative efforts by equipment users and suppliers to develop standards.

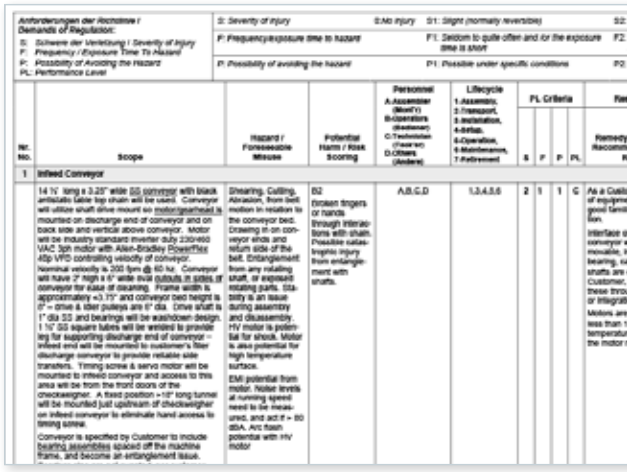
In addition, there is another set of organizations that act as arbiters on compliance. These are Nationally Recognized Test Laboratories (NRTL). The NRTLs function to evaluate equipment to determine if the equipment meets the requirements of standards, for which the supplier claims compliance. NRTLs can evaluate equipment to document the supplier's claim that the equipment is in compliance, or as reinforcement to the supplier's CE claim of conformity.

Terms of Art

Safety has a language of its own. Most of the terms have similar meanings in their language of origin, but the nuances are critical. To demonstrate the differences seen, a "hazard" can mean a sharp curb that cuts a tire, or the part of a golf course where you do not want your ball to land. In safety, hazard means a "potential source of harm". In turn, "harm" means a physical injury or damage to health".

"Each standard has a "Definitions" or "Glossary" section with terms commonly used in that standard. The more general standards have the broadest sets of definitions, and these are excellent sources for developing your own 'safety vocabulary'. One practice to establish your organization's vocabulary is to create a list of the terms you will use and identify the sources for those specific definitions (e.g., 'Acceptable Risk - ANSI B155' and, "Actuator - EN 60204-1').

Risk Assessment



A risk assessment is an evaluation of a product, or an element of a product, to determine the hazards, related harms from the hazards, the probability of harm occurring, and how to reduce the effects of those hazards to a safe level. The risk assessment process involves the following steps:

- Definition of the scope of the item being assessed
- Declaration of intended use for the equipment
- Declaration of unintended use, and foreseeable misuse
- The hazards presented by the item
- The potential harms from those hazards
- The personnel involved with the item
- The stages of the equipment lifecycle where the hazards and harms are prevalent
- The Performance Level associated with the item, determined by,
  - The Severity Level, S1 or S2
  - The Frequency for required access, F1 or F2
  - The Possibility of Avoiding the Hazard, P1 or P2
- The steps taken to reduce risk to an acceptable level
- The verification that the risk reduction was effective

The steps shown above are consistent among the different standards where risk assessment methods are described.

Risk assessment is a process. Risk assessments can be done very quickly and very badly. Good risk assessments take time and energy, and depend heavily on the knowledge and sincerity of the people conducting the risk assessments. Some suppliers fear that risk assessments will expose flaws in their designs and open them to possible action by an injured party. Smart suppliers understand that the risk assessment will identify hazards early in the equipment design and build process, and reduce their exposure to legal action. Smart suppliers also understand that identifying the hazards openly for the users will help the users develop strategies for safe use of the equipment, reducing the chance of an injury occurring.

Risk assessments are best done by a multi-disciplinary team. Three main attributes are needed with the participants:

- Knowledge of the design of the equipment
- Knowledge of how the equipment is applied and used
- Knowledge of the standards in effect for the equipment

Form a team assessing risk relies on the reasoning judgment and expertise of individuals familiar with the tasks and hazards associated with packaging machinery. To minimize individual biases (e.g., an individual attuned to noise hazards), a team approach is recommended. However, a team that is too large can lead to difficulty remaining focused or reaching consensus. - ANSI B155

It is possible that one person in the supplier's organization has all three sets of knowledge. It is unlikely that the person with all three knowledge sets does not have a pre-conceived opinion of the safety of the equipment. It is best to encourage some challenging discussion to force the different contributors to look at the equipment from different points of view.

Intended Use and Misuse

Each risk assessment should begin with a statement that identifies the intended use of the equipment. Predictable misuse, or foreseeable misuse, should be declared as well. Declaring intended use provides a framework for the user to make sure the equipment is being used in the manner for which it was designed. A passenger vehicle is intended as a machine to transport persons. A tractor is a machine used to plow, lift, drag, etc. You do not expect to drag logs with a passenger vehicle, and you can't operate a tractor safely at 100 km/h. These statements also protect the supplier, especially when combined with the declaration "The following is the intended use for this product. All other uses, foreseen or unforeseen, should be considered misuse.".

Risk Assessment by the User

The risk assessment done by the supplier is typically a "hazard-based risk assessment". The hazard-based form is to identify the hazards, harms and risks inherent to the product and the design. This form is done with a thorough understanding of the design, and a general understanding of the way the machine will be applied.

The task-based risk assessment is done by the user, with the information from the supplier's risk assessment, and a full knowledge of the way it will be applied. This takes into account the specific users, materials handled on the machine, equipment upstream and downstream, and environmental conditions.

The more complete the hazard-based risk assessment, the easier it is to perform the task-based, and the lower the overall risk to both supplier and user.

Integration of the Equipment and Risk Assessment

As stated previously, the task-based risk assessment considers upstream and downstream equipment. The supplier can reasonably expect that there will be other equipment feeding product and receiving product from the machine, however, the supplier has no control over the peripheral equipment. For this reason, it is important to clearly declare the physical and guarding boundaries for the machine provided, and advise the user of openings for material to pass through the machine. Finally, inform the user of any distances to known hazards, and reference known standards for distance/gap relationships for hazards to assist the user in decisions on integration guarding.

Installed Equipment

Capital equipment is usually modified several times over its life. There is no equipment standard that requires an equipment supplier to provide additional safety features to a machine that shipped, where that machine was compliant with the relevant standards at its time of shipment. No automobile manufacturer refitted its 1970 models with airbags. Reputable equipment suppliers will provide upgrades of safety features where there is a heightened awareness of a potential harm, but if there was no requirement at the time the machine was built, it is usual for the user to bear the expense of any upgrade.

NFPA 79 indirectly gives guidance on an important boundary; repairs vs. modifications. It states: "When changes other than repairs are made to machines that do not comply with the provisions of the standard, the changes shall conform with the provisions of the standard". This passage presents a lower level of obligation for form-fit-function replacement of equivalent parts, and modifications. Users and suppliers will therefore have to define the repair/ modification boundary for the equipment. As a general rule if the function of the machine is changed or enhanced the action can be considered a modification.

Equipment standards of both the EU and US direct the party modifying the equipment to follow the standard in place at the time of the modification. This is done through definition of the "supplier" in ANSI B155-2011, and in EN 60204-1. Suppliers include contractors, installers, integrators, rebuilders.

Modified equipment is subject to risk assessment at the time of modification, and depending on the complexity of the equipment and the reasonable ability to segregate functions, this could mean a complete rebuild of the machine, or a simple addition of a guard, ANSI B155 also defines sellers of used equipment as suppliers.

What is Safe Machine Design?

For packaging machinery the two standards that are most prominent are:

- EN 12100 – Safety of Machinery
- ANSI B155-2011 – Safety for Packaging and Packaging/Converting Equipment

The European Norm is a document with broader scope, and is more general in nature than the ANSI standard. Both standards direct that risk assessment be performed, with the results given to the equipment user.

> The outcome of a risk assessment shall be documented. The documentation shall demonstrate the procedure that has been followed, the hazards identified, and the risk reduction methods employed to reduce risks to an acceptable level. - ANSI B155

Safe machine design is too often thought of as "guarding". While proper guarding is important, conceptually the safest machine design would have no guards, as the hazards would be eliminated early in the design process. The preferred progression for reducing risk is,

- First, remove the hazard through design.
- Second, guard the hazard to prevent access.
- Third, notify the users of the hazard level and potential harm.
- Fourth, instruct or train the users to avoid the hazard.

Removing the hazard is also referred to as "designing-out". Examples of design-out are:

- Full conveyor beds to prevent access to drive assemblies
- Guards integrated into functionally required drive structures
- Moving parts over conveyors that, at a fixed elevation, are too close to allow a finger to intervene
- Moving parts over conveyors at a fixed elevation that are high enough to pass over a hand or arm.

Hazards are designed-out to make the machine safer, These solutions are usually also a lower cost, in both guarding, and also, the complexity of the required safety circuit.

Safe machine design is a set of design practices that designers follow to meet the safety standards appropriate for the machine type and location where the machine will be used. Standards give general requirements, and practices provide more specific instruction. Each supplier must take the requirements given in the standards and translate them to directions for internal use. As an example, a standard may require that the machine be "stable" with consideration for assembly, transport, and normal operation. The internal practices should direct the design personnel to use methods that might include a base footprint greater than the height of the center of gravity, and the center of gravity within the footprint of the machine.

Types of Guards - In general, there are two guard forms recognized in most standards:

- A fixed guard, which requires a tool for removal.
- A movable guard which can be opened without tools, but requires interlocking.

A variant of the fixed guard appears in ASME B20 (Safety Standard for Conveyors and Related Equipment). Defined in that standard is the "shield-guard".: a full or partial enclosure or cover, either framed or solid, made from material sufficiently rigid, to prevent accidental contact with moving parts. The shield guard recognizes that material needs to pass through areas of production, where the hazard and risk are not that great, and full closure prevents production.

When safe machine design practices are followed from the start of the design, the risk assessment is less difficult and less time consuming.

...decisions will be confirmed during the validation/verification portion of the risk assessment (see clause 6.8). If a thorough risk assessment is delivered with the machine it may be used as a starting point for the user's risk assessment. - ANSI B155

Notification of Hazards - When inherently safe design and guarding are not practical, notification of the hazards is the next step. ANSI Z535 and ISO 3864 provide the clearest directions on means to notify users of hazards in different danger zones. The familiar yellow triangles are the internationally-accepted method to identify the type of hazard. Industry safety specialists have worked with suppliers of machine markings to offer a set of icons that can reasonably relate the form of hazard (shock, crushing, radiation, laser light) to those near the machine.

ISO 3864 is the latest standard dealing with this topic, and its method to define the level of risk through a signal word and a background color is accepted for global practice. Those two elements – hazard icon + signal word – in combination, can usually address the notification needs for most hazard zones.

ISO 3864 also shows a three-panel format, with the two elements identified above, and a third panel with instruction on the type of hazard and possible consequences. The additional verbal notice is less favored by companies who use equipment across countries with different languages. With these users, the hazard icon with the signal word in the language of the "destination country" (Machinery Safety Directive term), is the preferred method.

What is Safe Electrical Design?

Complementing the safe machine design methods, safe electrical design takes the requirements of broad-based standards and translates the requirements into practices for electrical design. An example of this is the requirement set for grounding (also referred to as earthing). The requirement may require a grounding conductor with current capacity equal or greater than the largest current-carrying conductor in a circuit. The specific methods to meet the requirement would be a statement of the sizes of the conductors, the color and material of the conductor, location, the means of attachment, and the labeling methods.

Safe electrical design is for all parts of the machine, but is mostly focused on the electrical panel. A good method to review electrical safety practices is to "follow the power", and verify the proper application and safe implementation of each component, device, and conductor.

Incoming Power - There are different systems for electrical power, and these vary mostly by country. The equipment supplier should provide a thorough description of the manner used to introduce customer power into the electrical panel, along with the components used, and how they are qualified for the power form. The first component the customer's power should see is the disconnect switch. The form, Ingress Protection (IP) rating, short circuit current rating, maximum voltage allowed, number of switched poles, and how the customer's earth-ground is connected – should all be described. This level of detail forces the designers to review the details, and provides users with information to determine if the power they are providing is truly suitable for the equipment. A simple diagram of a three-pole switch with through-legs for neutral and ground (earth) is much more effective than three paragraphs.

A practice that directs safe electrical design should align with the two relevant standards for the EU and US; EN 60204-1 and NFPA 79. These two standards are more closely harmonized than fifteen years ago, but there are still differences, and while the differences may be small, the consequences of the differences can be significant. The best way for a supplier to demonstrate understanding of the standard and how it is satisfied is to have the supplier explain the requirement, the solution, and how the solution satisfies the requirement. This is not an unreasonable request and it separates those who know the requirements from those who don't.

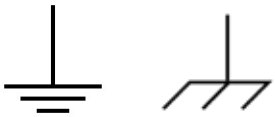
Overcurrent Protection

The entire electrical panel should be protected against overcurrent conditions, either through fusing or circuit breakers. Descriptions of these devices should state the voltage levels allowed, maximum current allowed, an any other criteria that could contribute to a fail condition.

Qualifying Components

A good method to qualify components is to follow the power from the disconnect, all the way through the panel to low voltage devices, or devices supported by, but external to the panel. Each device should be able to handle the range of voltage supplied through the disconnect. It should also be able to accept the full current level from the main current limiter, or have additional means to limit current to a lower level.

Grounding (Earthing)



Grounding, or Earthing, is the practice of providing a direct current-path to the earth, there are two types of grounds; protective earth (PE), and functional earth (FE).

The purpose of a PE is to reduce a dangerous electrical condition to a "zero-potential" state, in a rapid, safe manner. It is a short-circuit to the earth, the biggest electrical capacitor we have. A well-designed electrical panel will never use the conductors provided for PE. When the PE conductors are used, they create a short-circuit condition, and an overcurrent condition that will cause the current-limiting devices to open.

FE is the method used to shield electrical devices from interference by placing the components and enclosure at an equipotential state (all devices at the same voltage).

A reliable supplier should be able to describe the methods used for grounding, the conductors used for grounding, and how the electrical panel is tested as a complete system for ground-path integrity and for wire insulation effectiveness.

Wiring Practices

Users should expect that the equipment supplier can provide description of the wiring methods used in panel construction. This would include:

- Conductor material and form
- Insulation type and protection rating for temperature, fluid contact, and voltage level
- Wire sizing for different current levels
- Termination methods for wires
- Labeling methods for wires and terminals
- Terminal types and limitations for use
- Organization of wiring for segregation of power, signal, communications
- Methods of packaging wires on the panel and maximum fill level.

These should be readily available and not difficult for one technical person to explain to another technical person.

Emergency Stop

An Emergency Stop, or E-stop, is part of a safety circuit. E-stop Categories are commonly Category 0 or Category 1. E-stop Categories are well defined in EN 60204-1 and NFPA 79, and the definitions are virtually identical.

A **Category 0** E-stop drops power to all actuators in a machine, when the E-stop switch is "open" (off). A Category 1 E-stop causes all motion in a machine to stop, but requires a secondary action to drop all power before entering the danger zone. The potential hazard with a Category 0 is that the energy in the system is not brought to a zero-state in a controlled manner, and that uncontrolled motion can create further danger. The selection of the appropriate E-stop Category is left to the design personnel, but in general a Category 0 is preferred unless maintaining power through a Category 1 action permits a safer, more controlled stop.

What is a Safety Circuit?

Safety circuits are not new in product inspection equipment. The implementation of ISO 13849-1,-2 increased awareness of safety circuits. The Machinery Safety Directive and ANSI B155-2011 identified the need for safety circuits. ISO 13849-1,-2 were first released in 2006 to begin replacement of EN 954. The transition period ended at the end of 2011 and ISO 13849 is now fully in effect.

ISO 13849 is a standard that has acceptance worldwide and across all industries. The packaging equipment industry has endorsed its use through the industry-directed safety standard ANSI B155-2011 - Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery.

The safety circuit is that part of a control system that initiates actions or takes actions related to the safety of the machine. It may include the emergency stop, interlock switches, valves that de-energize pneumatic or hydraulic devices, contactors for motors or other actuators, motor controllers, safety relays, and safety PLCs. The complexity of the safety circuit is driven by the level of hazard presented in the machine (defined as performance level in the risk assessment), and the complexity of the machine.

Safety Categories as Given in ISO 13849-1

ISO 13849-1 provides direction on how to design and qualify a safety circuit. It also directs to ISO 13849-2 for the

means to properly validate the safety circuit. To comply with ISO 13849-1, one must also comply with ISO 13849-2.

There are five categories for safety circuits in ISO 13849-1: B, 1, 2, 3, and 4.

Category B is "Basic", and is for simple machines with low hazard levels. In its simplest form, a Category B safety circuit could be a single E-Stop that interrupts power to a motor.

At the other end of the spectrum, Category 4 requires redundancy, diagnostics, proven components, proven design technique, with the user made aware of a failure in the safety circuit, before the next use of the safety circuit is required.

Category 4 is not safer than Category B, as long as a Category B circuit is appropriate for the application. Application of a Category 4 safety circuit on a machine needing only a Category B will likely increase the chances the circuit will fail, and when it does, it will require greater effort and expense to restore the circuit to a functional level. A safety circuit that is more complex than required is also more likely to be circumvented by the user.

There are six criteria to characterize the five different categories for safety circuits:

i. The general architecture of the circuit - the structure of the circuit and it complexity

ii. The failure mode of the circuit - what will occur if the safety circuit fails

iii. Principles used to achieve safety - how the safety circuit reaches its qualified level

iv. Component life (individually and collectively) - reliability of components

v. Diagnostic Coverage - the ability to detect and react to a safety circuit failure

vi. Common Cause Failure (CCF) attributes - capability of the circuit to withstand independent failures

This table is a quick summary of safety circuit categories and their characteristics.

Cat	Architecture	Failure Mode	Principles (Performance Levels Possible)	Component Life ($MTTF_d$)	Diagnostic Coverage	CCF
B	Uses components and design practices that follow standards in place. Basic safety principles apply.	Failure of the safety circuit can lead to a loss of the safety function	Mostly component selection (a,b)	Low to medium	None	Not a factor
1	In addition to "B", the application of well-tried components, and well-tried principles.	Failure of the safety circuit can lead to a loss of the safety function, but probability is low.	Mostly component selection (b,c)	High	None	Not a factor
2	In addition to "1", a means to periodically check the safety function is part of the control system.	A fault can lead to a loss of safety function, but the loss is detected between checks	Mostly by structure of the circuit (a,b,c)	Low to high	Low to medium	Requires a score of ≥65 of 100 on segregation, diversity, knowledge and experience of the designers, immunity from environmental factors (e.g., shock, vibration, EM fields) see Annex F
3	In addition to "1", a single fault does not cause the loss of the safety function (redundancy), and, whenever practicable, the occurrence of the single fault is detected	A single fault can occur, but the safety function performs. Some faults are detected. A combination of individual faults can lead to loss of the safety function	Mostly by structure of the circuit (a-d, b-e)	Low to high	Low to medium	
4	In addition to "1", a single fault in any of the parts does not lead to loss of the safety function, and is detected on or before the next use of the safety function. If that detection is not possible, combined faults do not lead to a loss of the safety function.	The safety function is always performed, even with a single fault. Detection reduces probability of safety function loss. Faults are detected in time to prevent loss of the safety function.	Both component selection and structure of the circuit (a-e)	High	High	

The Safety Circuit Process

Prior to creating a safety circuit, a risk assessment must be conducted for the machine controlled by the safety circuit. The risk assessment will discover the hazards, identify the performance level required for the safety circuit, and describe the safety actions to reduce the risk. Following the safety circuit process, the risk assessment will be used again, to determine the effectiveness of the safety actions.

There are three stages in the safety circuit process: **Design**, **Qualification**, and **Validation.**

Design is the selection of the circuit architecture and components needed to achieve the required performance level. It must be done by a person with knowledge of the standards, and who is practiced in safety circuit design. Research must be done on each component in the safety circuit to establish the suitability of the components for their reliability under the conditions of operation. Conditions of operation include both the machine environment and the electrical environment where the circuit is placed.

In the design phase, the two characteristics of the circuit considered are components and structure.

Component **Qualification** takes into account:

- The operating conditions for which the component was qualified
- Failure mode
- The projected life of the component

For all of these, the component manufacturer should be able to summarize the information in the data sheet, with verification of the data by an independent, Nationally Recognized Test Laboratory (NRTL).

Operating conditions may include current limits, voltage limits, electromagnetic field susceptibility, temperature, and IP ratings.

Failure mode is how the device will fail. An example of this is an E-stop switch with "forcibly-guided contacts". This description tells the designer that, on event where the contacts fail through fusing, the next mechanical action on the switch will cause the switch to open through mechanical destruction of the switch.

Component life is evaluated by repetitive testing. The most credible component data are provided by an NRTL. A set of components is cycled until they fail. The value $B10_d$ is the number of cycles before the first 10% of the components fail dangerously. These data are then used with information on how the component will be used to determine the number of years the device is expected to last. The number of operations a device will be used in application is estimated by the designer (as part of the safety team), considering the number of cycles per hour, the number of hours per day, and the number of days of operation per year. The value "Mean Time to Dangerous Failure" ($MTTF_d$) is the resultant value for the component's life, and this is measured in years.

Structure considers how the components are used in combination. Structure considers:

- Single, or dual channel architecture
- Redundancy
- Diagnostics

The number of channels in the circuit is characteristic of the complexity of the system. A single channel solution is limited to Category B, Category 1, and Category 2 circuits. The inherent limitation of the single channel is its ability provide a means to support the circuit should the single channel fail. It is a redundancy of the channel.

Redundancy can apply to components and channels. For components, the redundancy can be built into the device itself, such as a redundant set of contacts in an E-Stop switch. It can also be external to the device, such as a set of redundant motor contactors between the safety relay and a motor control device. In both cases, the second contact device is used as a back-up, in the event that the first device fails.

Diagnostics involves the ability of a device to communicate its status as functioning, or failed. With a pneumatic valve, the signal from the safety relay to open the valve may be sent, but the physical act of opening the valve cannot be confirmed without some indication from the valve that the position has changed, or that the air pressure has dropped. More complex devices such as motor controllers have built-in diagnostics, and these support compliance with Category 3 and Category 4 requirements.

Common Cause Failure (CCF) is a term used to describe the capability of the circuit to withstand faults in design and protection that lead to the failure of the safety circuit to function properly. Examples of these are:

- Segregation of signals through different paths to prevent one action to cause multiple signals to fail
- Diversity of components and construction methods to eliminate one mode of failure to cause multiple faults in the system. This is analogous to "belt and suspenders"
- Design and application experience – do the design personnel have the appropriate knowledge and experience required?
- Assessment/Analysis – has the circuit and its components been evaluated for how they will fail, and the consequences of those failures?
- Environmental Conditions – are the components able to withstand the conditions presented by the environment, and can the circuit withstand the anticipated electromagnetic conditions (EMC)?


INTERNATIONAL STANDARD

ISO 13849-1

Safety of machinery — Safety-related parts of control systems —

Part 1:
General principles for design

ISO

The methods to **Qualify** the safety circuit are described in ISO 13849-1. The first level of qualification is to make sure the components used are sufficient for the application. This means gathering manufacturers' data on the number of cycles the part is projected to last. The target information is $B10_d$, which is the amount of time until the first 10% of the components of a given form will fail. Based on the planned use of the component in the circuit, the expected life of the components and the circuit as a whole will be determined through calculations given in the standard.

Validation is the documented method to test the effectiveness of the safety circuit. The requirement for validation is made in ISO 13849-1, and the method is declared in ISO 13849-2.

For each action that causes a predictable response, the action is made and the response is verified. Examples of this are opening interlocked doors and pressing an E-stop. For these actions, it may be expected that contactors for motors will open and valves will open for pneumatic devices. These effects must be checked, and signals for those actions must be verified.

The validation plan is not only used when the machine is built. It is a part of the documentation package that is used by the customer when the machine is installed, when a component is replaced, or when the circuit is modified by use of a substitute component.

Validation Testing of Safety Functions

Validation Testing Procedure:
Before each step of each test;

- ***Make sure that both guard doors are closed and the e-stop is reset.***
- ***Press the safety circuit reset button and verify that the rejector valve, the friction belt motor, and the three conveyor motors are active[1].***

1. Safety circuit connected normally, both E-Stop channels opened (i.e. E-Stop button pushed):
   a. Confirm that the three conveyor motors and the friction belt motor are disabled.
   b. Confirm that the rejector is disabled.
2. Channel 1 of the safety circuit functions individually without the channel 2; disconnect channel 1 of the E-Stop circuit.
   a. Confirm that the three conveyor motors and the friction belt motor are disabled.
   b. Confirm that the rejector is disabled.
3. Channel 2 of the safety circuit functions individually without the channel 1; disconnect channel 2 of the E-Stop circuit.
   a. Confirm that the three conveyor motors and the friction belt motor are disabled.
   b. Confirm that the rejector is disabled.
4. Short channel 1 of the E-Stop circuit to earth, then power;
   a. Confirm that the three conveyor motors and the friction belt motor are disabled.
   b. Confirm that the rejector is disabled.
5. Short channel 2 of the E-Stop circuit to earth, then power;
   a. Confirm that the three conveyor motors and the friction belt motor are disabled.
   b. Confirm that the rejector is disabled.
6. Cross-short channels of the E-Stop;
   a. Confirm that the three conveyor motors and the friction belt motor are disabled.
   b. Confirm that the rejector is disabled.
7. Open guard door #1;
   a. Confirm that the three conveyor motors and the friction belt motor are disabled.
   b. Confirm that the rejector is disabled.

Example of a validation plan for a safety circuit

Personnel are well-trained when they have demonstrated knowledge of the standards, the application environments, and the technical experience in applied safety circuits. The best test of a well-trained person is that person's ability to explain how the circuit was designed, how it was qualified, how it is validated, and how it meets the requirements of relevant standards.

If your supplier can support you with all the information mentioned above you would have all that you need for safe integration and operation of your equipment.

www.mt.com/pi
For more information

USA
Mettler-Toledo Safeline
6005 Benjamin Road,
Tampa, FL 33634
Telephone 813-889-9500
Toll Free 800-447-4439
Fax 813-881-0840
safeline.sales@mt.com

USA
Mettler-Toledo CI-Vision
2640 White Oak Circle, Unit A,
Aurora, IL 60502
Telephone 630-446-7700
Fax 630-446-7710
civision.marketing@mt.com

United Kingdom
Mettler-Toledo Safeline Ltd.
Montford Street, Salford,
M50 2XD, UK
Telephone +44 (0) 161 848 8636
Fax +44 (0) 161 848 8595
safeline.info@mt.com

Germany
PCE
Kampstraße 7
31180 Giesen, Germany
Telephone +49 (0)5121 933 222
Fax +49 (0)5121 933 124
PID@mt.com

USA
Mettler-Toledo Hi-Speed
5 Barr Road, Ithaca, NY 14850
Telephone 607-257-6000
Toll Free 800-836-0836
Fax 607-257-5232
hispeed@mt.com

United Kingdom
Mettler-Toledo Safeline X-ray Ltd
Greenfield, Royston Business
Park, Royston, Herts, SG8 5HN UK
Telephone +44 (0) 1763 257900
Fax +44 (0) 1763 257909
Email: xraysales@mt.com

Germany
Mettler-Toledo Garvens GmbH
Kampstraße 7
31180 Giesen, Germany
Telephone +49 (0) 5121 933 0
Fax +49 (0) 5121 933 456
garvens@mt.com