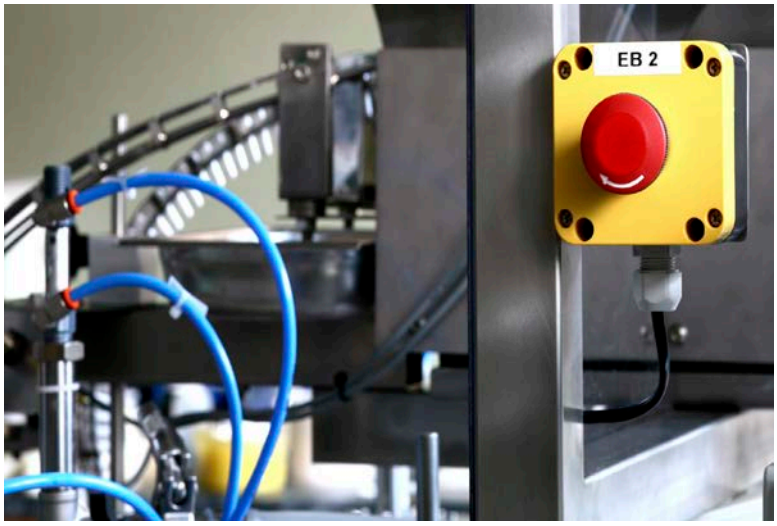
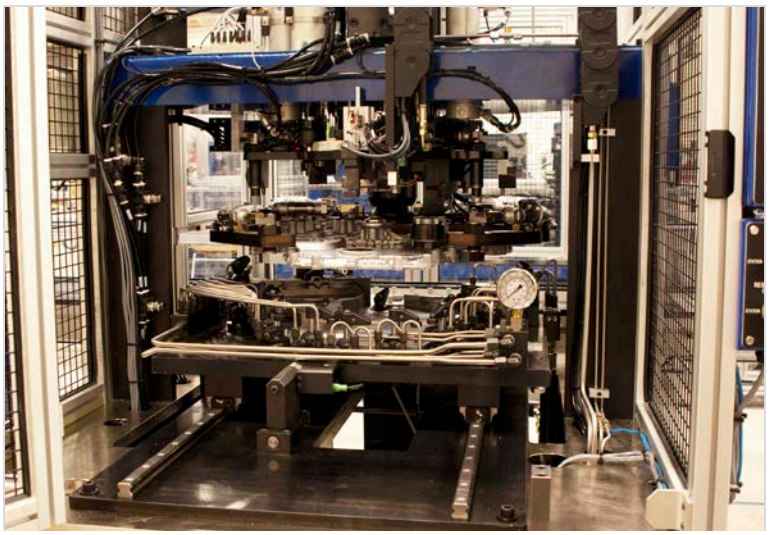




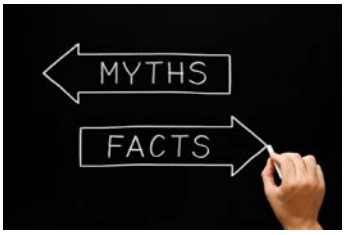
Five Myths about Safety in Machinery

Addresses specific myths about the EU Machinery Directive 2006/42/EC, commonly known as the “EC Machinery Safety Directive”, and its impact on builders and users.

Safety has been a hot topic in automation and especially motion control for as long as I have been in the industry. The publication of EU Machinery Directive 2006/42/EC has focused even more attention on the subject. Also known as “The EC machinery safety directive”, it includes within its scope nearly all machinery, including medical machinery, lifting hoists, mobile equipment, machine tools and packaging equipment just to name a few.

EU Machinery Directive 2006/42/EC seeks to harmonize machine safety requirements across this entire range of products. It’s important to note that directives are ratified by the EU as a whole, then each member country is expected to implement its own local laws, regulations and standards to enforce the directive. So the directive is subject to interpretation by lawmakers and regulatory authorities and standards organizations and to further interpretation by companies that design, build and use machinery.

Two alternative European standards have been developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in compliance with EU Machinery Directive 2006/42/EC. These are EN ISO 13849-1 and EN 62061 respectively. ISO 13849-1 provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems. EN 62061 is a machine-specific standard within the IEC 61508 framework for designing electrical safety systems. With many different organizations and individuals involved in interpreting and implementing the directive, it’s not surprising that confusion and erroneous interpretations have arisen.



This article will address five specific myths about the EU directive and explain the related impact on builders and users of machinery.

Myth 1: ISO 13849 and IEC 61508 are Laws

ISO 13849 and IEC 61508 are standards rather than laws. Only the machinery directive itself can be considered a law (Machinery Directive 2006/42/EC). In most cases, countries enforce the machinery directive and other directives through regulatory authorities that perform a similar function to the Occupational Health and Safety Administration (OSHA) in the US.

The machinery directive does not apply to US end users, but could apply if an OEM is building and exporting to an EU country. The ISO 13849 standard provides guidelines for machine builders to comply with the EU machine directive, so it is a valuable standard to observe. ISO 13849 is intended to empower machine builders to use creative design practices to improve machine safety but in many cases it has encouraged rigidity due to fear of making mistakes.

Standards are intended to keep industry professionals aligned with requirements and to eliminate uncertainty. They are not supposed to encourage strict adherence to specific design practices. OEMs have the power and responsibility to make decisions about machine suitability within the standards. Risk assessment is the core tenant of all machine safety standards. It is important to follow a process, produce a rating system and base the design upon it. Standards don’t explicitly clarify how to rank each hazard or how to rank various mitigation options. The important part is to define and adhere to an acceptable product development process.

Myth 2: US and EU standards are Very Different

ANSI/PMMI 155 and ANSI B11.0 are the main US standards addressing machinery safety. They both follow the same core principles as EU standards such as ISO 13849. Furthermore, other standards can be used to comply with the machinery directive without contradicting ISO 13849. Organizations such as the PMMI (Packaging Machinery Manufacturers Institute), ANSI (American National Standards Institute), and RIA (Robotics Institute of America) have drafted standards that allow builders to comply with the Machinery Directive. ANSI/PMMI B155.1-2011 (B155.1) was actually drafted more recently than the current ISO 13849 and it was written specifically to harmonize with modifications expected in the next revision of ISO 13849.

The bottom line is that machinery builders have flexibility in how they design machines. Existing machine designs are in many cases adequate to meet modern safety guidelines. The design of many safety components has not changed significantly with these new standards. They have simply been validated and categorized in accordance with the new standards. Many vendors can offer mean time to fail dangerously (MTTF d) measurements for standard components. Builders can use this data to calculate the overall effectiveness of a machine safety system concurrent with any modern standard they desire. It is smart for designers to follow current standards because these are considered state of the art, but it does not automatically presume that a traditional safety method is not proper.

Core principles like risk assessment are common to all current and former standards. The risk assessment sets the performance levels of the safety systems. The builder should evaluate the current system architecture, analyze the safety chain and determine if the current design meets the newly determined performance levels.

A good design can meet multiple standards and machine manufacturers can use one risk assessment to demonstrate compliance with multiple standards. Requirements such as safety labelling can be different for different standards but these conflicts are usually relatively minor.

Myth 3: Category Levels for Safety are No Longer Applicable

Machinery manufacturers are accustomed to designing control systems based on EN954-1 categories. When the EU machinery directive was updated in 2006 it designated EN954-1 as no longer valid and not to be used by machinery builders. This incorrectly led many builders and control systems providers to believe that the safety category levels are no longer applicable or appropriate. However, ISO 13849 still places significant importance on category levels in determining the performance level of safety systems. The category levels have not changed in the new EU machinery directive. Categories ratings are still the core principle of a safety function.

The new requirements demand additional calculations to define performance or safety integration levels. These factors include diagnostic coverage, common cause failures and reliability of the hardware determined by the parameter mean time to fail dangerously. The new approach to both ISO 13849 and IEC 62061 centers on component reliability and system coverage calculations rather than purely architectural determinations of overall machine safety. Safety vendors are providing data to help with these system calculations. Current architectures based on adherence to the EN954-1 standard can relatively easily be brought into compliance with the new directive. It will most likely not change the core architecture of your safety system.

Note the new standards are still based on the safety architecture described in the well-known categories. In addition, the probability of a failure has to be considered to determine the safety level.

Myth 4: The Emergency Stop is a Safety Feature

From IEC60204-1 (section 9.2.5.4.1) Safety of Machinery – Electrical equipment of machines: *NOTE: Emergency stop and emergency switching off are complementary protective measures that are not primary means of risk reduction for hazards (for example trapping, entanglement, electric shock or burn) at a machine (see ISO 12100 (all parts))*

Many standards including NFPA 79 (part of the U.S. National Electrical Code) reference the need for an emergency stop. IEC60204-1 and NFPA 79 are generally aligned in the area of emergency-stop requirements. The note above points out that an emergency stop does not make a machine safe. All machines have risks associated with them. Functional safety is intended to reduce the operational risks associated with machines. Emergency stops are designed to be used in the event of an unplanned occurrence. Modern safety standards drive for safety systems that respond properly without the need for emergency intervention.

A common question asked by OEMs and integrators is: "What is the required safety level of the emergency stop function?" Answering this question requires evaluating the residual hazard left in the machine. Evaluation starts with a risk assessment. Severity and exposure are determined during the risk assessment and directly relate to the safety integration level (IEC 61508) or performance level (ISO 13984). A key consideration is that severity and exposure is based on the residual hazard. This is the hazard left after other risk mitigation steps have been taken. This could require design changes, hard guarding, or control reliability based interlocks applied to eliminate or reduce the hazard.

The takeaway is that the emergency stop may be in the Safety Integration Level 2 (SIL2) or PLd realm of required safety level. For example, since a redundant control reliable safety interlock eliminates personnel from exposure to a hazard, the emergency stop only has to guard against residual risk. Since the exposure is low, a SIL2 or PLd safety level is appropriate. An emergency stop requires human intervention so it is not a reliable way of reducing risk or eliminating a hazard. The primary effort should go into reducing hazards without the intervention of personnel.

Myth 5: OSHA Recognizes and Enforces the EU Machinery Directive or ISO or IEC Standards

OSHA has its own standards so the EU machinery directive and ISO and IEC standards are not applicable to machines sold for use in the US. OSHA 29CFR1910 contains both general requirements and specific machine level requirements. These requirements have changed very little in comparison with international standards. It is entirely possible for machine builders to design machines that comply with both OSHA requirements and the EC machinery directive.

The most controversial difference in OSHA standard is "For The Control of Hazardous Energy (Lockout/Tagout) (29 CFR 1910.147)". Lockout/Tagout (LOTO) as it is defined in the OHSA standard is a mandatory requirement and one that can seem to limit some of the freedoms afforded by designers using functional safety standards. A key section highlighting a potential conflict between standards is as follows:

1910.147(a)(2)(ii)(B)
An employee is required to place any part of his or her body into an area on a machine or piece of equipment where work is actually performed upon the material being processed (point of operation) or where an associated danger zone exists during a machine operating cycle.

Note: *Exception to paragraph (a)(2)(ii):* Minor tool changes and adjustments, and other minor servicing activities, which take place during normal production operations, are not covered by this standard if they are routine, repetitive, and integral to the use of the equipment for production, provided that the work is performed using alternative measures which provide effective protection (See Subpart O of this Part).]

The interpretation of “minor changes and adjustments” is one that many builders and operators are currently wrestling with. Modern safety systems and standards are creating an environment where personnel can be kept safe using active controls rather than traditional LOTO. Control systems utilizing SLS (safe limited speed) can allow an operator to perform tasks without the removal of energy.

Determining if a task is minor or routine is beyond the scope of this article. An example of a potential source of conflict may be changing a die out of a machine. If the die needs to be swapped frequently, an operator may consider this routine and minor from their business perspective. OSHA may feel differently. OSHA offers ten different interpretations here. For the time being there is not a definitive guide on LOTO and how modern systems using reliable safety solutions might address LOTO requirements. This is a topic that US-based machine operators and those providing machines to US operators want to see resolved.

Conclusion

This article is intended to educate machine builders and operators about the new safety standards. The most frustrating part of the new standards is the fear that they have instilled into the industrial machinery market. Navigating the requirements is complicated, partly by the myths that have been addressed in this article. This has led some organizations to take a very conservative approach or, worse yet, not to do anything. In reality, machine safety is the responsibility of OEMs, end-users and technology vendors as a whole. No single standard or law will guide anyone completely through the process. Because so much of the machine safety is left up to those involved in the design, integration, and use of a machine it is important to take an empowered role in getting it right. Although safety may seem like a burden at times, designing safety into a machine is a systematic process very similar to other aspects of machine design.

References: (EC)- http://ec.europa.eu/enterprise/sectors/mechanical/documents/legislation/machinery/index_en.htm#h2-2
(B155.1) http://www.pmmi.org/Resources/SafetyDetail.cfm?ItemNumber=3358

ABOUT KOLLMORGEN

Kollmorgen is a leading provider of motion systems and components for machine builders around the globe, with over 70 years of motion control design and application expertise.

Through world-class knowledge in motion, industry-leading quality and deep expertise in linking and integrating standard and custom products, Kollmorgen delivers breakthrough solutions unmatched in performance, reliability and ease-of-use, giving machine builders an irrefutable marketplace advantage.

For more information visit www.kollmorgen.com, email support@kollmorgen.com or call 1-540-633-3545.