Understanding Machine Safety Guidelines

Table of Contents

Table of Contents

Sponsor Overview

Pneumatic and Electric Drive Technology for Factory & Process Automation

Festo is a leading global manufacturer of pneumatic and electromechanical systems, components and controls for process control and factory automation solutions, with more than 55 national headquarters serving more than 180 countries. With over 40 years of innovation in the United States and over 80 years globally, Festo has continuously elevated the state of manufacturing with innovations and optimized motion control solutions that deliver higher performing, more profitable automated manufacturing and processing equipment.

Our dedication to the advancement of automation extends beyond technology to the education of current and future automation and robotic designers with simulation tools, teaching programs, and on-site services.

Festo is globally recognized as a symbol of expertise in factory automation and process control. We can help decrease process costs by engaging Festo as an extended workbench and benefitting from our expertise with regard to pre-assembled pneumatics, customized product designs, and system solutions.

Festo enables its partners to obtain more intelligent automation solutions from a single source. In addition to tried and tested pneumatic drive units, Festo also provides both servo-pneumatic and electric drive units.

Our intelligent systems for status monitoring and machine diagnosis (condition monitoring solutions) are made up of sensors, software, controllers, and visualization.

These solutions can greatly reduce maintenance and servicing costs. With a comprehensive line of automation components, custom components and complete electromechanical and pneumatic motion controlled multi-axis systems.

Festo can support your most complex automation requirements.

For more information on Festo:
http://www.festo.us

15 Steps to Help with European Union's Machinery Directive, EN/ISO 13849-1

Table of Contents

Machine safety compliance is more flexible and interpretive than in the past. Basic definitions of the machinery directive and the following 15 steps can clarify.

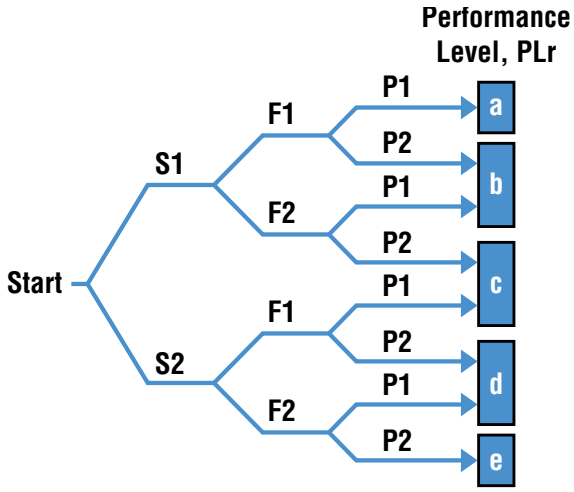
Michael Guelker

Machine safety is serious business, and understanding relevant machine safety standards should be considered a starting point. With so much at stake—from employee safety to litigation costs—an original equipment manufacturer (OEM), machine builder, system integrator, or end user needs to learn as much as possible. Machine safety is regulated by a host of national and international safety standards and enforced by government agencies.

In the U.S., the Occupational Safety and Health Administration (OSHA) and National Fire Protection Association (NFPA) are the primary agencies, while the International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) originate in Europe but hold increasingly global influence. All these regulations, standards, and agencies cause confusion for machine builders and end users.

When an accident occurs and a worker is injured or killed, lawsuits and OSHA investigations often follow. Attorneys and OSHA will ask the question: What did the company do to ensure that the machine was as safe as possible? In most cases, if a lawsuit occurs, the machine builder, automation equipment manufacturer, and the systems integrator may also be named in the lawsuit.

Fortunately, machine safety regulations are becoming more standardized. In 2012, the NFPA brought NFPA 79 into alignment with the European Union's Machinery Directive (EN/ISO 13849-1). NFPA 79 deals with safety-rated programmable logic controllers (PLCs) and safety buses, so this was a major step. Today, if equipment vendors, machine builders, systems integrators, and end users follow EN/ISO 13849-1, it's a good start toward protecting workers and surviving lawsuits. Machine safety remains a complex and subtle task, but the rules are becoming clearer and safety equipment more capable.



The accompanying chart shows various elements of the standards that apply to machine safety. Courtesy: Festo

Since the 1970s, when few safety regulations existed, machine safety regulations have followed a difficult, contentious path toward standardization. The major problem was that the standards were not keeping up with safety technology. The original NFPA 79 regulations required the use of hardwired components, such as emergency stop pushbuttons. It was amended in 2002 to allow the use of safety PLCs and software-based controllers, and in 2007 to allow drives and other equipment designed for safety to be used as switching elements. Finally, in 2012, NFPA 79 adopted new rules and regulations that brought it into alignment with IEC

15 Steps to Help with European Union's Machinery Directive, EN/ISO 13849-1 (cont.)

Table of Contents

standards and the National Electrical Code (NEC). Meanwhile, similar events were happening in Europe with the EN 954-1 safety standard, which had been in place for many years, but did not address programmable electronic safety equipment nor consider failure probabilities. Efforts were made to replace EN 954-1 with the new EN ISO 13849-1 and EN 62061 safety standards as part of the European "Machinery Directive" as far back as 2009. Since December 2011, all machine and process safety systems sold in Europe must conform to EN ISO 13849-1 and EN 62061 safety standards. The accompanying chart shows various elements of the standards that apply to machine safety.

ISO/IEC Machine Safety Standards

EN ISO 13849-1 Safety-related parts of control systems: Principles for design

EN ISO 13849-2 Safety-related parts of control systems: Validation

EN ISO 12100 General principles for design - Risk assessment and risk reduction

EN IEC 60204-1 General requirement for electrical equipment of machines

EN ISO 11161 Integrated manufacturing systems

EN IEC 61508 / 62061 Functional safety of electrical/programmable electronic safety related systems

EN 13849-1 has wide applicability as it applies to all technologies including electrical, pneumatic, hydraulic, and mechanical. This standard provides requirements for the design and integration of safety-related parts of control systems, including some software aspects. The standard applies to a safety-related system but can also be applied to the component parts of the system.

Common terminology

Explanations of common machine safety terms follow.
PLr: Performance Level required

DCavg: Diagnostic Coverage average

MTTFd: Mean Time To Failure dangerous

CCF: Common Cause Failure – failure of many components from one event

B10: Time by which 10% of a population of a product will have failed

A full and detailed study of EN ISO 13849-1 is needed before it can be correctly applied. The following overview provides 15 steps to EN ISO 13849-1 requirements:

1. Create a technical file: Documentation of every step in the process must be maintained for both the end user and possible future litigation.

2. Design with safety in mind.

3. Determine the limits of the machinery.

4. Identify all potential hazards.

5. Perform a risk assessment: The manufacturer has to

15 Steps to Help with European Union's Machinery Directive, EN/ISO 13849-1 (cont.)

Table of Contents

perform a risk assessment for the machinery. Based on the outcome of this risk assessment, the risk level can be determined. Risk reduction and residual risk can be estimated.

6. Perform risk reduction, by design and/or safety measure. Example safety measures are: guard, light curtain, door.

7. Identify residual risks: Document the residual risks in the manual.

Safety Categories - related PL (Table 7 from EN ISO 13849-1:2006)

Category	PL	DCavg	CCF	MTTFd
B	a	None	No	No
	b	None	No	No
1	c	None	No	No
2	a	Low	No	No
	b	Low	No	No
	c	Low	No	No
	b	Medium	No	No
	c	Medium	No	No
	d	Medium	No	No
3	b	Low	Yes	Yes
	c	Low	Yes	Yes
	d	Low	Yes	Yes
	c	Medium	Yes	Yes
	d	Medium	Yes	Yes
	d	Medium	Yes	Yes
4	e	High	Yes	Yes

PLr (performance level required) is used to denote what performance level is required by the safety function, as the name suggests. To determine the PLr, the EN ISO 13849-1 standard provides a risk graph into which the application factors (Severity of injury, Frequency of exposure, and Possibility of avoidance) are input. The output is the PLr (a, b, c, d, or e). Courtesy: Festo

8. Determine the PLr (Performance Level required): PLr is used to denote what performance level is required by the safety function. To determine the PLr, the standard provides a risk graph into which the application factors (Severity of injury, Frequency of exposure, and Possibility of avoidance) are input. The output is the PLr (a, b, c, d, or e).

9. Choose the appropriate Category (B, 1, 2, 3, 4) and architecture you need to achieve the required PL. Clause 6 of ISO 13849-1 provides the definitions of the categories.

i. Categories B and 1 are single-channel with no monitoring.

ii. Category 2 includes monitoring at certain times (start-up, new cycle, etc.).

iii. Categories 3 and 4 are dual-channel with monitoring.

1. Cat 3 detects some, but not all faults.

2. Cat 4 must detect every fault. Also see: "Safety Categories - related PL (Table 7 from EN ISO 13849-1:2006)."

10. Choose the components for this Category architecture. Need B10 values of components used – get official document from the supplier.

11. Calculate MTTFd (Mean Time To Failure dangerous), based on B10 values. Need following information:

i. Days of operation per year

ii. Hours of operation per day

15 Steps to Help with European Union's Machinery Directive, EN/ISO 13849-1 (cont.)

Table of Contents

iii. Time between successive cycles in seconds

iv. B10 value from supplier of component

v. Expected life time of the machinery

12. Evaluate your safety system design

13. Validate your designed machinery using EN 13849-2. This must be done by a person other than the designer of the safety systems. This doesn't mean that a third party has to be involved. A colleague who has no involvement with the design can perform the task as evaluator.

14. Create an overview of the Essential Health and Safety Requirements (EHSRs) you have filled.

15. Create a user manual with the appropriate information. This should show how to transport, commission, use, service, adjust, dismantle, and scrap in a safe way.

Free machine safety software tool

SISTEMA is a software tool for EN ISO 13849-1 implementation. SISTEMA stands for Safety Integrity Software Tool for the Evaluation of Machine Applications. Its use will greatly simplify the implementation of the standard. It was developed by the BGIA in Germany and is free for use. It requires the input of various types of functional safety data, which is done automatically when using a manufacturer's SISTEMA data library. It also helps create the documentation package.

This synopsis of relevant machine safety standards should be considered as a starting point to understanding machine safety. With so much at stake, from employee safety to litigation costs, those involved need to learn as much as possible about machine safety and related standards.

About the Author

Michael Guelker is a Festo Corp. product manager.

Edited by Mark T. Hoske, content manager, CFE Media, Control Engineering and Plant Engineering, mhoske@cfemedia.com.

Machine Safety Compliance: Start with Design

Table of Contents

From ergonomics and e-stops to OSHA and output, here are the essential considerations for machine safety compliance. Safety starts with design.

Allan Manzer

An important first step when considering safety as part of machine design is understanding the scope of what the machine is being designed to deliver. Safety in design is critical to the end products as well as to the machine's profitability, whether the equipment is designed to deliver compressed air; cuts or forms metal parts; assembles parts; or makes widgets. Safety in design includes an understanding of the machine throughput information (how many parts per hour). Evaluate the complexity or simplicity of the machine's loading and unloading process (manual or automatic), and in-feed and out-feed requirements (how do raw materials get into the machine and finished parts get out of the machine) during the design phase.

E-stops (emergency stop buttons) need to be designed to be easily accessible and labeled clearly to allow for a quick shutdown in an out-of-control situation. Courtesy: Optimation

Floor space requirements can best be determined during the design stage as well. Consider the machine footprint, such as how much space is needed for the machine, the operator, material handling machine access (such as forklift, conveyors, etc.), production component marshalling, material storage, access for removing end product components, and packaging materials; and how waste will be handled. What services will be needed to power and operate the machine, such as air, electricity, water, vacuum, etc.? Consider what is needed as well as the source for these services.

Include ergonomics during the design phase. Adjustable equipment should be able to be operated by any person. Adjustability must be designed into the operator's panel and input stations allowing for risk-free, user friendly, and efficient operation of the equipment.

One guide for the ergonomics engineering solutions is the book, "Kodak's Ergonomic Design for People at Work." There are currently no OSHA or European ISO 18001 standards for ergonomic design, but that doesn't mean citations cannot be issued by OSHA in the U.S. OSHA will issue citations to companies for poor design via its General Duty Clause, which states the employer must provide a workplace free from recognized hazards. Industrial illnesses caused by repetitive motion, such as carpal tunnel syndrome, are considered recognized hazards by OSHA.

Along with ergonomics, the Americans with Disabilities Act (ADA) must be considered during design. The U.S. Department of Justice's revised regulations for Titles II and III of the ADA Act of 1990 were published in the Federal Register on Sept. 15, 2010. The Department has assembled an official online version of the 2010 ADA Standards

Machine Safety Compliance: Start with Design (cont.)

Table of Contents

for Accessible Design (2010 Standards) to compile the information in one easy-to-access location. It provides the scoping and technical requirements for new construction and alterations resulting from the adoption of revised 2010 Standards in the final rules for Title II (28 CFR part 35) and Title III (28 CFR part 36).

Keep ergonomics in mind: machines should be able to be operated by any person. Design adjustable controls to make the machine efficient and user friendly. Courtesy: Optimation

The Justice department has also compiled guidance on the 2010 standards from the revised regulations for Titles II and III. This explanatory information from the regulations addresses the scoping and technical provisions of the 2010 standards. The new requirements can be found at ADA.gov or within the U.S. Department of Justice Civil Rights Division.

Regulatory considerations

Beyond safe machine design, a health, safety and environmental (HSE) plan is needed. Front-end loading, a thorough planning proactive approach to machine design, can help bring to mind everything that needs to be considered. The HSE plan, if thorough, will raise a high percentage of the safety concerns so these issues can be resolved in the earliest phases. Use the HSE plan to facilitate the construction of the operating facility and help answer questions raised during this phase of engineering as well. HSE plans are not required by OSHA's 29 CFR 1910 General Industry, 29 CFR 1926 for Construction, nor by ISO 180001. They only require that all hazards be recognized and addressed prior to starting construction and starting equipment.

OSHA provides the requirements for exit routes, emergency action plans (emergency access, egress, exits, and emergency response signage, etc.) and fire prevention plans in Subpart E of 29 CFR 1910.33 through 1910.39. Since safety standards differ by country, designers should consider the country in which the machine will be located and operated. If the machine has running or moving parts that would require guarding, related regulations are spelled out in 29 CFR 1910.211 through 29 CFR 1910.219 Subpart O. All operating hazards must be identified during design so that interlocking guards can be included to protect those who will operate the machine and require access for maintenance activities. Electronic stops (e-stops) also need

Recognize what it will take for a mechanic to perform service maintenance and repair on your machine. Poor accessibility can lead to extended downtime and potential injuries. Courtesy: Optimation

Machine Safety Compliance: Start with Design (cont.)

Table of Contents

to be designed and labeled so equipment can be immediately shut down if an out-of-control situation were to occur. OSHA provides direction for lockout/tagout (LOTO) and hazardous energy control in 29 CFR 1910.147 Subpart J. OSHA requires that new equipment be designed such that personal protective equipment (PPE) would not be required for machine operators to be safe in Subpart I, 29 CFR 1910.132. The standard directs that new equipment shall design out any hazards that could be serious enough to require PPE if at all feasible. It should be noted that feasibility is not necessarily a cost or a convenience issue. Safety standards related to electrical safety are found in Subpart S at 29 CFR 1910.301 through 399.

These standards are examples of OSHA performance standards, which describe what needs to be done to achieve compliance. ISO 18001 provide overarching high-level guidance and does not provide direction on how to perform these types of work.

OSHA isn't the only standard enforced. Other standard writing organizations documents are referred to and/or incorporated into OSHA regulations. Many of the American National Standards Institute (ANSI) standards, as well as those from the National Fire Protection Association (NFPA), are incorporated by reference into the OSHA standards, which make them enforceable by OSHA. These are only two of many incorporated standards that must be considered during the design phase for machine compliance.

Production considerations

A key component to the functionality of the machine is the design of and usability of the operator's station and the accessibility of the machine components to maintenance personnel who will need to service and repair the machine.

Many machines are designed with production rates in mind, and this can lead to re-design once operations and maintenance begin. Re-design because of complications with operators or other humans can be very costly, resulting in injury, quality issues, low production rates, and machine shutdown time. The same issues arise when a machine is designed without considerations for how the machine will need to be serviced, repaired, and maintained. Some designers do not have a good understanding of what it takes for a mechanic to gain access to the motors, gearboxes, chains, sprockets, and the like, so servicing can be completed quickly and, in many cases, without shutting down the equipment.

Machine Safety Compliance Reference Table

Standard Topic	Standard ID.	Standard Author	Contact Info.
Machine Guarding	29 CFR 1910.211-219 Subpart O	OSHA	www.osha.gov
Exit Routes, Egress	29 CFR 1910.33-39 Subpart E	OSHA	www.osha.gov
Americas with Disabilities	29 CFR Part 35	ADA	www.ada.gov
Lockout/Tagout	29 CFR 1910.147 Part J	OSHA	www.osha.gov
Personal Protective Equipment	29 CFR 1910.132-.138 Subpart I	OSHA	www.osha.gov
Electrical Safety	29 CFR 1910.301-.399 Subpart S	OSHA	www.osha.gov
International Safety	ISO 18001	ISO	www.iso.gov
General Safety	ANSI	ANSI	www.ansi.gov
General Safety	NFPA	NFPA	www.nfpa.gov

Machine safety compliance draws upon many standards, including these. Courtesy: Optimation

Machine Safety Compliance: Start with Design (cont.)

Table of Contents

The inability for maintenance staff to easily and quickly access equipment parts that need service and or repair also can lead to extended downtime. Fixing design errors makes retrofit or re-design extensive and expensive. Failure to re-design or even just living with these problem areas (the issues not considered in the original design process) can lead to worker morale issues, dissatisfied customers, and a loss in future business.

Cost of noncompliance

Noncompliance may be disregarded as the cost of doing business. These costs can be broken down into two groups, direct and indirect costs. Direct costs are those easily identified, such as cost of wasted materials, hours spent in making inferior nonsaleable products, and wasted raw materials. Cost of injuries, insurance, and worker's compensation expenses are among examples of direct costs.

Indirect costs are more subtle and sometimes not as easy to identify. The cost of extra administrative duties, additional paperwork, incident reports and recordkeeping, extra meetings to discuss the proper resolutions to a given problem, loss of clients because of poor quality products, and negative media coverage are all consequences not easily quantified. Indirect costs can lead to lower worker morale, employee turnover, and injuries. Poor design can result in bringing in more employees or temporary employees to work on equipment not functioning properly or even doing the production work by hand because of a machine failure.

Safety compliance is the competitive edge

Professional engineers strive to design equipment and machinery so that it is "done right, the first time, without incident." Safety compliance designed and built into machinery is a proactive approach that will give companies a competitive edge for anyone who interfaces with this equipment. Engineering "done right" builds quality into the equipment.

"Done right, the first time" gives a company the quality edge, plus provides a better opportunity for achieving the desired schedule. When combining "done right, the first time, without incident," quality is achieved, schedule is maintained, and losses and waste are reduced. All these factors lead to machine safety compliance and a competitive edge.

Companies on the leading edge include safety engineering in the design phase of project work to provide a different set of eyes to look for and identify gaps that may lead to safety problems when the machine begins production. Most safety engineers would be looking for all of the issues outlined here and other safety concerns that may present themselves during the HSE planning process.

About the Author

Al Manzer is Optimation corporate safety engineer.

Edited by Mark T. Hoske, content manager, CFE Media, Control Engineering and Plant Engineering, mhoske@cfemedia.com.

Machine Safety: Design a Safer Machine with Risk Assessments

Table of Contents

Understand why and how to conduct a risk assessment on a machine to improve the design by increasing safety and productivity. Note 6 reasons why to do risk assessments, and 8 steps to conduct a risk assessment.

JB Titus

Sometimes, old habits are hard to change. What is so difficult about understanding why and how to conduct a risk assessment on a machine? See these six reasons to conduct a risk assessment and eight steps to doing a machine risk assessment.

Let's start with why risk assessments should be conducted.

Here are six reasons to conduct risk assessments.

1. It's simply a good business practice.
2. You're performing your responsibility for due diligence.
3. Your overall liability as a business is the same, regardless.
4. It's part of your existing business safety culture.
5. Industry consensus standards require risk assessments.
6. It's the law – OSHA!

If the above is reasonably clear, doesn't it seem plausible that everyone would be conducting risk assessments without hesitation? Well, it's my opinion that old habits are hard to change! Haven't we all seen situations in recent years where any or all of the example reasons above have either been MIA (missing in action) or just simply misunderstood. Having said that, we've also seen numerous case examples of companies considered "best-in-class" incorporating risk assessments into their business. Isn't this because, in part, they've concluded that there is a cost associated with not being best-in-class?

The most frequent excuse I hear from companies not conducting risk assessments is – because risk assessments are added costs to our business. Yet, don't all six of the reasons above have an avoidable cost associated with them that can shutter a business? Best-in-class companies say: yes!

Secondly, "how" to conduct a risk assessment?

There are several answers to this question. However, it begins with a real simple concept which in my experience is not universally understood. The key word is "process." A risk assessment is not a snap shot, a check mark, and generally is not a single hazard. There are some folks out there incorporating the new ISO consensus standard, ISO 13849-1; 2008, who mistakenly believe the risk graph in informative annex A is considered a risk assessment. No, this only has to do with the safety-related parts of a control system where a control function is deemed necessary to reduce risk. And, every hazard on a machine isn't usually mitigated via a control function.

So, a risk assessment is called a process because it takes multiple steps to conduct. Of all the standards, white papers, and training classes I've encountered, they all seem to average eight process steps to properly conduct a risk assessment on a machine.

Machine Safety: Design a Safer Machine with Risk Assessments (cont.)

Table of Contents

8 steps to properly conduct a machine risk assessment are:

1. Prepare and research limits of the assessment
2. Identify all tasks and hazards
3. Assess initial risk(s)
4. Risk reduction actions
5. Assess residual risk(s)
6. Acceptability of residual risk(s)
7. Validate solution(s)
8. Provide documentation

Therefore, a risk assessment is a process of logical steps designed to systematically identify and evaluate any and all hazards associated with a machine. And, not until any and all hazards are identified via a risk assessment can designs be implemented to mitigate those hazards making it a safer machine.

If all companies understood everything mentioned above, wouldn't we see a majority of them fully incorporating risk assessment into their businesses as a core function?

About the Author

For more than 30 years, J.B. Titus has advised a wide range of clients on machine functional safety solutions, including Johnson & Johnson, Siemens, General Motors, Disney, Rockwell Automation, Bridgestone Firestone, and Samsung Heavy Industries. He holds a BBA from Oklahoma University in Industrial Management and an MBA from Case Western Reserve University in marketing and finance.

Machine Safety: 13 Terms to Know for Compliance with Functional Safety, ISO 13849-1

Table of Contents

Knowing these 13 machine safety terms will help in efforts to comply with the international standard, ISO 13849-1: 2006, Safety of machinery, Safety-related parts of the control system. Many large companies have become early adopters of the new quantitative approach for designing machine control systems.

JB Titus

Since the international community passed ISO 13849-1: 2006, Safety of machinery, Safety-related parts of the control system, many large companies have become early adopters of the new quantitative approach for designing machine control systems. In so doing technical design personnel within these companies have had to learn several new terms required for compliance with the new standard.

13 machine safety terms you should know

B_{10D} value: number of switching opertions on which 10% of the sample fail	PFH: Probability of Failure per Hour
CCF: Common Cause of Failure	PFH_d: Probability of Failure per Hour dangerous
DC: Diagnostic Coverage	PL: Performance Level
DC_{avg}: Diagnostic Coverage average	PL_r: Performance Level Required
Designated Architecture: Predetermined structure of an SRP/CS	SIL: Safety Integrity Level
MTBF: Mean Time Between Failure	SRP/CS: Safety-Related Parts of a Control System
$MTTF_d$: Mean Time To Fail danferous	

Table shows machine safety terms related to ISO 13849-1: 2006, Safety of machinery, Safety-related parts of the control system.
Courtesy: Control Engineering Machine Safety Blog, J.B. Titus

ISO 13849-1 enables all safety-related control circuits (electrical, pneumatic, and hydraulic) to be designed for designated safety functions to meet ascertained performance levels for mitigating a hazard level to an acceptable level. To achieve high reliability levels for each safety function, the complete circuit (SRP/CS) must be designed using algorithms. These algorithms account for all components and devices in a safety-related circuit [such as sensors, logic solvers, output devices, etc.] using these variable terms and the look-up charts and graphs included in the standard. The actual process is far more detailed, however, the goal is to derive a Performance Level (PLa, b, c, d or e) that equals or exceeds a PL required (PLr) for each safety function. The required terms are:

1. **$B10_D$ value:** number of switching operations on which 10% of the sample fails – Suppliers provide this value for their components because it's required to calculate the overall performance level for a safety circuit. $B10_D$ only applies to the dangerous failures of the considered component and the value is usually given for a lifetime of 10 years.

2. **CCF:** Common Cause Failure – A common cause failure is generally when a single failure or condition affects the operation of multiple devices that would otherwise be considered independent.

3. **DC:** Diagnostic Coverage – This involves the combination of both hardware and software and testing of the related diagnostics. Diagnostic coverage is the ratio of the probability of detected dangerous failures to the probability of all dangerous failures.

4. **DC_{avg}:** Diagnostic Coverage average – Average diagnostic coverage for the above.

Machine Safety: 13 Terms to Know for Compliance with Functional Safety, ISO 13849-1 (cont.)

Table of Contents

5. **SRP/CS:** Safety-Related Parts of a Control System – This term refers to all safety-related control elements regardless of the type of technology (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery. It does not specify safety functions or performance levels.

6. **Designated Architecture:** Predetermined structure of an SRP/CS – One of the first steps in designing the SPR/CS is selecting the system architecture to be used for the safety system. ISO 13849-1 leads you through this process for the architecture and determining the PLr (Performance Level required) for each safety function.

7. **MTBF:** Mean Time Between Failure – This value should be provided by the component supplier and represents the mean time between two failures for that component.

8. **$MTTF_d$:** Mean Time to Fail dangerous – The same as above except that this value is only concerned with dangerous failures.

9. **PFH:** Probability of Failure per Hour – This value should be provided by the component supplier and represents the probability of failure per hour for that component to help detect random hardware safety integrity.

10. **PFH_d:** Probability of Failure per Hour dangerous – This value should be provided by the component supplier and represents the probability of failure per hour for that component to help detect random hardware safety integrity.

11. **PL:** Performance Level – The ability of SRP/CS to operate a safety function and reliably achieve that safety function. Typically a PLa, PLb, PLc, PLd, or PLe.

12. **PL_r:** Performance Level required – The result of determining the designated architecture is to in part determine the performance level required for a safety function. The PLr effectively becomes the goal for designing the actual safety circuit for that safety function.

13. **SIL:** Safety Integrity Level – This term has historically been used by safety component and device manufacturers and in the process industry sector for several years when designing safety systems and circuits. It is a requirement of IEC 61508.

Safety organizations, automation suppliers, and consultants (to mention a few) can offer courses on the new ISO 13849-1 compliance requirements. Courses are also offered for professional certifications as an FSE (Functional Safety Engineer) or CFSE (Certified Functional Safety Expert). Collectively, I view these evolutionary steps in machine safety as positive advancements for increased safety and potentially increased profits. Having said that, I suggest that we don't underestimate the related impact of functional safety on all industrial companies: domestic or international and small, medium or large. Advancing from a qualitative system designing safety-related circuits to a quantitative system involving algorithms with multiple terms is not a simple task for all participants across the spectrum.

About the Author

For more than 30 years, J.B. Titus has advised a wide range of clients on machine functional safety solutions, including Johnson & Johnson, Siemens, General Motors, Disney, Rockwell Automation, Bridgestone Firestone, and Samsung Heavy Industries. He holds a BBA from Oklahoma University in Industrial Management and an MBA from Case Western Reserve University in marketing and finance.

How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process

Table of Contents

International standard EN ISO13489-1 provides a framework for assessing risk and documenting safety. This white paper explores safety, summarizes the key steps necessary to lower risk, and highlights how integrated safety components can simplify machine design.

Frank Langro, Director Marketing and Product Management, Festo

Frank Latino, Regional Product Manager, Festo

Machine safety is serious business and should be at the forefront of any machine builder's design process. Aside from protecting property, equipment, and companies from litigation, most importantly machine safety requirements are in place to protect people. Instead of creating added expense machine safety can actually save a company large amounts of money by preventing worker injuries and deaths. In order for companies to sell their machines it has become a best practice to document the steps they take to lower the risk of injury from the machines they manufacture. This white paper explores the process of documentation and lowering risk and summarizes a five step documentation process based on the EN ISO 13489-1 standard. The paper will help to clarify the confusion over documentation and further safety at all levels of the OEMs design process.

In the U.S., when an accident occurs and a worker is injured or killed, lawsuits and OSHA investigations follow. Attorneys and OSHA will ask the question: What did the company do to ensure that the machine was as safe as possible? If a lawsuit occurs, the machine builder, automation equipment manufacturers, and the systems integrator may also be named in that suit. This potential makes it vital to document the process followed to ensure safety.

Simply building in safety to avoid a law suit, however, is not how most companies operate. Engineers do not want to be responsible for causing a customer unacceptable losses in productivity, damaging products or the environment, and most importantly injuring a worker. The attitude in the industry today is that designing and building safe machines goes without saying: safe machines are a key to local and international sales, and can provide a competitive edge.

Fortunately, machine safety regulations are becoming more standardized. In 2012, the National Fire Protection Association (NFPA) brought NFPA 79 into alignment with the European Union's Machinery Directive (EN ISO 13849-1). NFPA 79 deals with safety-rated programmable logic controllers (PLCs) and safety buses. Today if equipment vendors, machine builders, systems integrators, and end users conform to the EN ISO 13849-1 standard, that conformance provides an internationally recognized process for lowering the risk of injured workers, damaged products, environmental harm, and lawsuit liabilities. Machine safety remains a complex and subtle task, but the rules are becoming clearer and safety equipment more capable.

Safety through the years

Since the 1970s, when few safety regulations existed, machine safety regulations have followed a difficult, contentious path toward standardization. The major problem was that the standards did not keep pace with safety tech-

How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process (cont.)

Table of Contents

nology. The original NFPA 79 regulations required the use of hardwired components, such as emergency stop push-buttons. It was amended in 2002 to allow the use of safety PLCs and software-based controllers, and again in 2007 to allow drives and other equipment designed for safety to be used as switching elements. Finally, in 2012, NFPA 79 adopted new rules and regulations that brought it into alignment with IEC standards and the National Electrical Code (NEC). Meanwhile, similar events were happening in Europe with the EN 954-1 safety standard, which had been in place for many years, but did not address programmable electronic safety equipment and didn't consider failure probabilities.

Efforts were made as far back as 2009 to replace EN 954-1 with the new EN ISO 13849-1 and EN IEC 62061 safety standards as part of the European Machinery Directive. Since December 2011, all machine and process safety systems sold in Europe must conform to EN ISO 13849-1 and EN 62061 safety standards. The accompanying chart shows various elements of the standards that apply to machine safety.

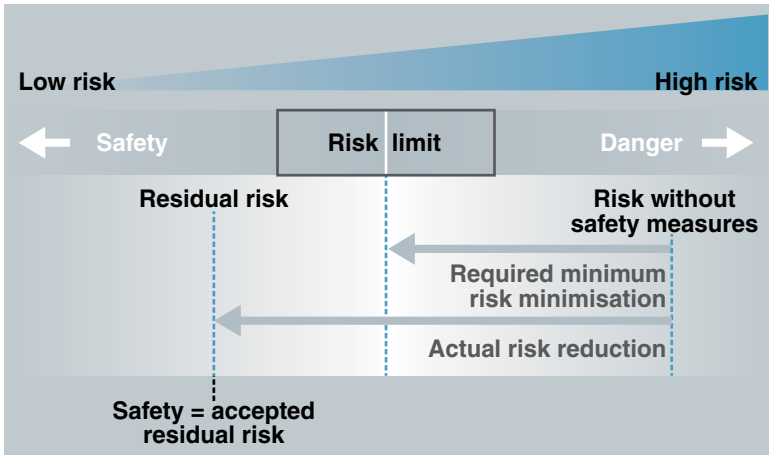
Key ISO/IEC Machine Safety Standards

EN ISO 12100-1 and EN ISO 12100-2	Governs safety of machinery. Part 1 describes basic terminology, while Part 2 lists technical principles and specifications.
EN ISO 14221	Defines risk assessment
EN IEC 60204-1	General requirement for electrical equipment of machines
IEC EN 61508	Functional safety of electrical/electronic/programmable electronic safety related systems
EN IEC 62601	Functional safety of electrical/electronic/programmable electronic safety related systems (based on 61508)
EN ISO 13849-1 and EN ISO 13849-2	Safety-related parts of control systems
IEC 61784-3	Safety networks

EN ISO 13849-1 is the starting point for risk reduction

Unlike many of the other international standards, EN ISO 13849-1 covers multiple technologies that can be used within the Safety Related Control System including electric, pneumatic, hydraulic, controls, and mechanical components. This standard is internationally recognized, and it is a Performance Level (PL) focused standard whose outcomes can be equated to IEC Safety Integrity Level (SIL) standards, which gives it even greater usefulness. EN ISO 13849-1 is the one standard that can cover most, if not all, concerns of the machine manufacturer (OEM) in factory automation safety controls.

What is safety?

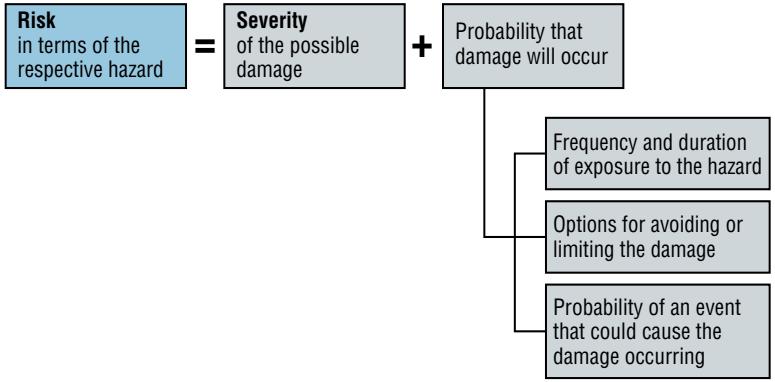


How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process (cont.)

Table of Contents

Safety is the difference between the risk limit, the absolute minimum to avoid danger, and the residual risk, the level of risk the OEM accepts to keep employees, products, the environment, productivity, and the company safe. Each OEM has to decide its unique sweet spot in terms of accepted residual risk. Standards help with this determination.

What is risk?



The above chart succinctly defines risk as the combination of severity and the probability of occurrences. The probability of occurrence depends on three factors:

- Frequency of the duration of exposure to the hazard
- Options for avoiding or limiting damage
- The probability of a safety related event triggering event

OEMs that follow international standards such as EN ISO 13849-1 and document the processes used will reduce the probability that loss/damage will occur. Compliance can protect the OEMs, their customers, and their customer's employees from financial or physical harm. Furthermore, these companies will create a culture that rewards employees who make the safety of people, products, organizations, and the environment a high priority.

Beginning the process of designing safety-based systems

An excellent place to begin the risk assessment and documentation process is by following the ISO 12100 standard for the safety of machinery – general principles for design and risk assessment and risk reduction. ISO 12100 specifies basic terminology, principles, and a methodology for achieving safety in the design of machinery. It specifies principles of risk assessment and risk reduction to help designers in achieving this objective. These principles are based on knowledge and experience of the design, use, incidents, past accidents, and risks associated with machinery. Procedures are described for identifying hazards, estimating and evaluating risks during relevant phases of the machine life cycle, and for the elimination of hazards or sufficient risk reduction. Guidance is given on the documentation and verification of the risk assessment and risk reduction process.

In its simplest sense, beginning the safety process requires that every aspect of the machine that may cause loss/damage to people, products, and the environment are identified. ISO 12100 helps to organize the risk assessment process. The next step is to look at the requirements for the control of functional safety systems.

How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process (cont.)

Table of Contents

EN ISO 13849-1 control system risk assessment

Every standard for functional safety related control systems, whether it is Performance Level (PL) based or Safety Integrity Level (SIL) based such as IEC 61508, 61511, or 62061, requires a risk assessment to determine if the identified PL or SIL categorization is met. The main difference between PL and SIL concerns considerations of demand – how frequently a machine or process action occurs. SIL takes into account low demand mode, i.e., low frequency operation, which is prevalent in the process industries, and also high frequency demand as well. PL covers high frequency demand and is primarily aimed at production machines in factory automation.

An EN ISO 13849-1 derived PL can be equated to SIL level. However, a SIL from one of the IEC standards, for example IEC 62061, cannot be used to derive a PL rating. There is no equivalent PL for a low demand SIL, but there are SILs for every PL.

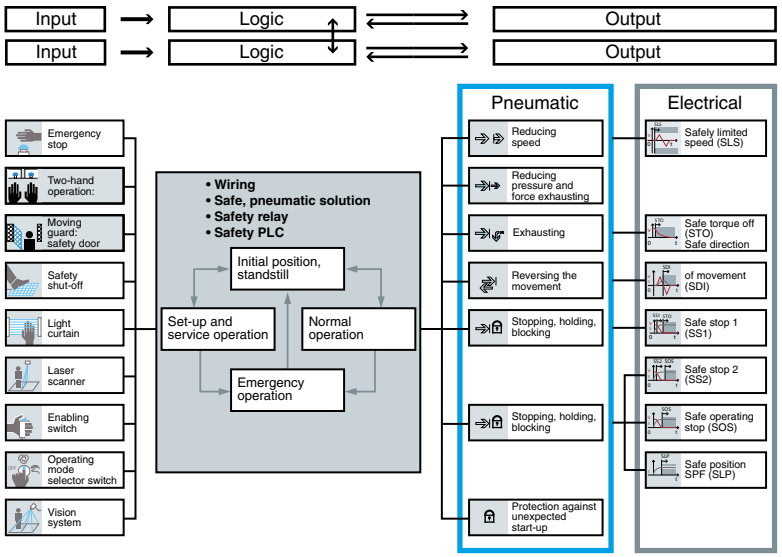
Once every functional control system involved with safety has been identified, the designers need to go back and look for ways of lowering risk. Risk reduction can be achieved through the following:

- Design Measures
  For example, changing the size of an opening so a person can't reach into the machine
- Technical Measures
  Designing functional systems – input, logic, and output – that achieve safe operation
- User Information – warning signs, alarms

Typical technical measures involve the following pneumatic or electric control functions:

- Pressurizing
- Maintaining pressure
- Reducing pressure and force
- Exhausting
- Two-hand operation required
- Tamper proof, prevent unexpected start up
- Reduced speed
- Free of force
- Stopping, holding, blocking a motion
- Reversing a motion

The functional safety control system, input logic output, is represented by the following graphic.



How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process (cont.)

Table of Contents

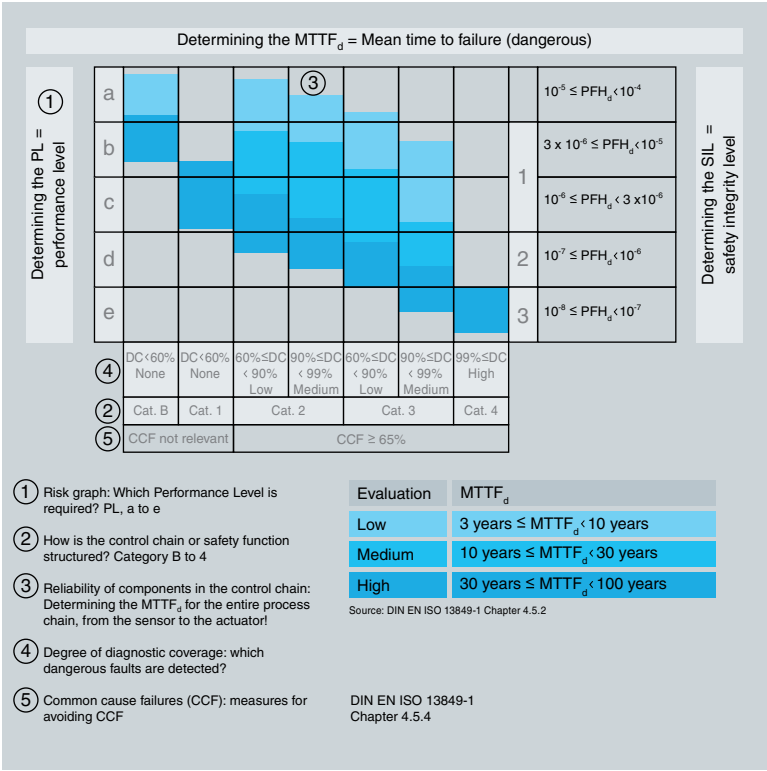
Note that the majority of the pneumatic safety functions have an analogous electric function.

Five steps for documenting a safe control system

EN ISO 13849-1 details five steps required to document the safety of each functional system involving safety on the machine. The steps are:

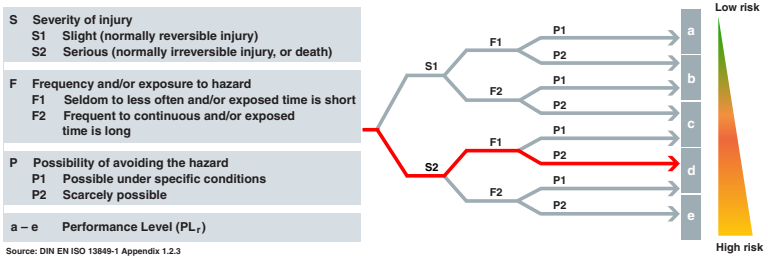
1. Determine the PL level – a to e
2. Identify the required control chain – B or 1 through Category 4
3. Select the components to be used that meet or exceed the required Meantime To Dangerous Failure – from input through output
4. Calculate the diagnostic coverage required for dangerous faults to be detected
5. Provide measures for avoiding Common Cause Failure (CCF)

The following chart provides a graphic representation of how all five steps fit together. The chart helps to identify the conditions each functional system has to meet.



Step 1: Determine the PL level – a to e

The acceptable PL of each function must be PL ≥ PLr. The OEM calculates PLr – the risk of the system – by identifying the severity of potential injury, the frequency and/or exposure to a hazard, and the possibility of avoiding the hazard or limiting the harm. A decision tree is used in the determination of PLr. The chart below shows the decision tree for a functional system that designates a PLr of d.

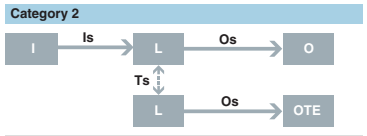


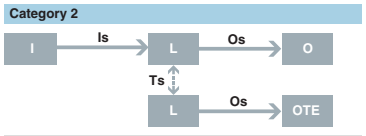
How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process (cont.)

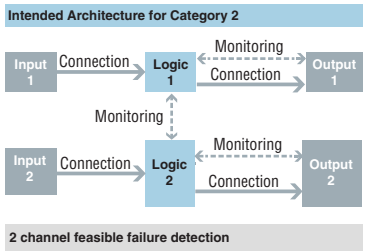
Table of Contents

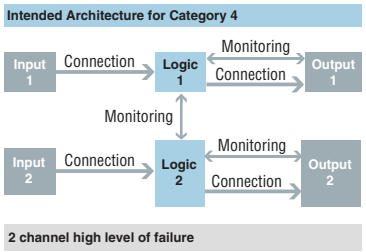
Step 2: Identify the control chain B or 1 through Category 4

Next, the designer must determine the control chain level B or 1 through Category 4 that is appropriate for the identified PL. Category B or 1 can satisfy a PL risk level c. Category B or 1 has one output (single coil) – one signal. Category 2 requires 100 tests of the system prior to each use. Category 2 is most often used in electronic systems where test signals can be sent in milliseconds to meet the 100 test requirement. Category 3 is a two channel system featuring redundancy in control and is suitable for PL of d and in some instances in e. The degree of diagnostic coverage for Category 3 includes low coverage from 60 to 90 percent of activations to medium coverage from 90 to 99 percent of activations. Category 4 is also a two channel redundant control system but its diagnostic coverage is greater than 99 percent. Category 4 is suitable for PL e. Control chains are graphically represented in the following way:



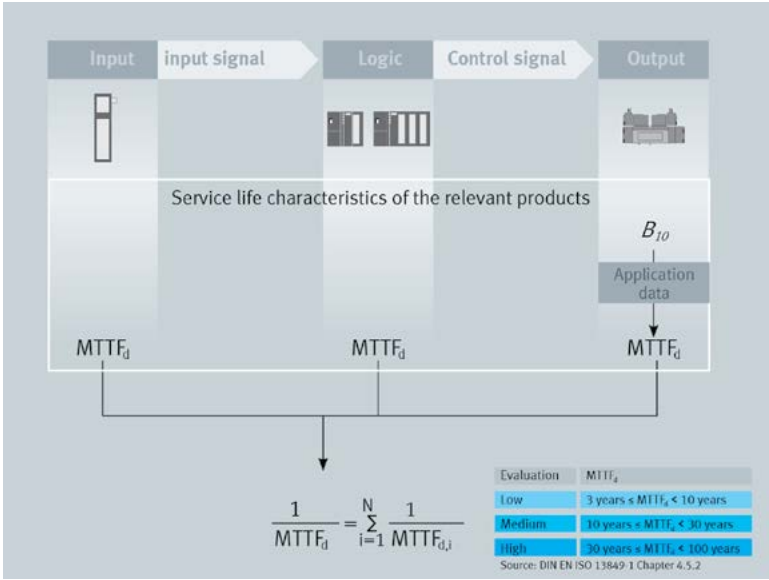






Step 3: Select the quality of the components to be used that meet or exceed Meantime to Dangerous Failure standards for the entire process chain – input through output

Steps one and two identify the PL and the control system category required for the functional safety control system. Step 3 involves the components in the control system that will be used to meet or exceed the PL and Category level. This step requires calculating Mean Time to Dangerous Failure ($MTTF_d$). The component supplier will provide the required statistical measurements to plug into the $MTTF_d$ equation. The chart below indicates a graphic representation of the process and the formulas for calculating $MTTF_d$.



How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process (cont.)

Table of Contents

$MTTF_d$ is a mean value for the duration of operation before a component fails in a manner that gives rise to a dangerous situation. This value is based upon data for the frequency of failures within a specified period of time and can be calculated from the reciprocal of the failure rate (dangerous failures [FIT]).

The $MTTF_d$ enables the finite reliability of individual subsystems, blocks, and elements to be quantified and their behavior predicted under the influence of the forces typically encountered in use. To clarify what these measurments mean in practice, the $MTTF_d$ has been divided into the ranges low, medium and high: Low 3 years <= $MTTF_d$; < 10 years; Medium 10 years <= $MTTF_d$ < 30 years; and High 30 years <= $MTTF_d$ <= 100 years. This and the remaining steps require quite a bit of computation. There is a free software program available for download that is designed to speed up the calculation process (discussed later in this paper). .

Step 4: Calculate the diagnostic coverage required for dangerous faults to be detected

Determining the diagnostic coverage involves identifying each potential source of error for a product and assigning a value to that potential error. There can be multiple sources of error for each product. The diagnostic coverage is an average of Mean Time to Failure (MTTF) and $MTTF_d$. Diagnostic coverage is typically classified in ranges when sources of error are factored in. The sources of error can be classified as:

- Not relevant for this component
- Some freedom from errors (see DIN EN ISO 13849-2)
- No error freedom guaranteed for this component

For example, a directional control value would have no error of freedom for a change in response time and some freedom for leakage. A change in flow rate would not be relevant for this component. See the following chart for an example of determining diagnostic coverage.

Products \ Sources of error	Change to the response times	Non-switching/ not switching back	Auto-switching	Leakage	Change to the leakage over a long period of use	Cracking of the housing/ connecting piece/tubing	Change to the flow rate without assistance (adjustable)
Directional control valves							
Shut-off/non-return/quick exhaust/shuttle valves							
Flow control valves							
Pressure regulators							

Not relevant for this component

Freedom from errors (see DIN EN ISO 13849-2)

No error freedom guaranteed for this component

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}}$$

DC<60% None	DC<60% None	60%≤DC < 90% Low	90%≤DC < 99% Medium	60%≤DC < 90% Low	90%≤DC < 99% Medium	99%≤DC High

How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process (cont.)

Table of Contents

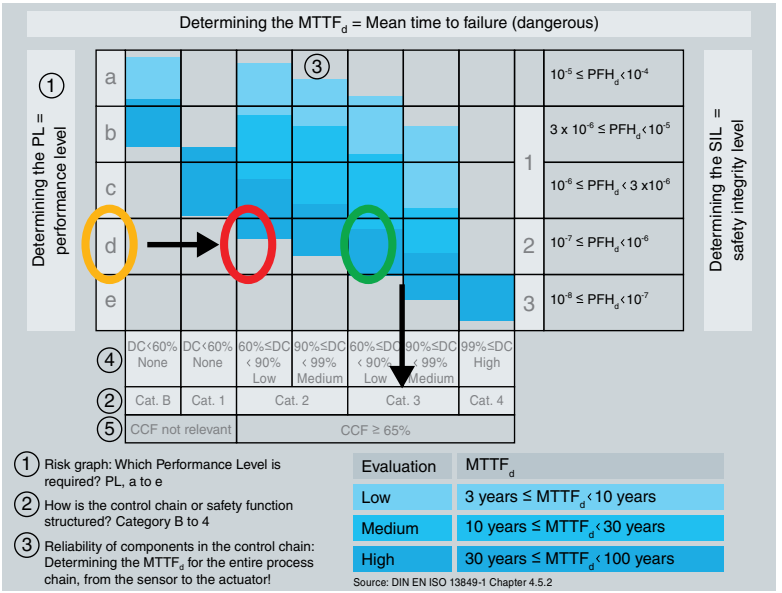
Step 5: Provide measures for avoiding Common Cause Failure (CCF)

Common Cause Failure (CCF) describes failures of a control system of redundant design that are attributable to a common cause such as common parts/common failure, contamination, electromagnetic interference, pressure, or more. Such failures are relevant only on two-channel sub-systems (as in Category 2, 3 or 4). The standard provides a points-based method for the quantitative assessment of measures against CCF. The point count must be ≥ 65 percent. The following chart provides an example of the points system.

Common Cause Failures CCF

No.	Measure against CCF	Points S
1	Separation/Segregation	
	Physical separation between signal paths: separation in wiring/piping, sufficient clearances and creepage distances on printed-circuit boards.	15
2	Diversity	
	Different technologies/design or physical principals are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, measuring of distance and pressure, digital and analogue. Components of different manufacturers.	20
3	Design/application/experience	
3.1	Protection against over-voltage, over-pressure, over-current, etc.	15
3.2	Components used are well-tried and attention has been paid to the ambient conditions	5

Putting it all together



Determined PLr required | **Not suitable due to test requirement** | **Suitable Category**

The chart above shows the overall assessment of a funtional system that was determined to require a PL of d. In this example, Category 3 safety circuits were specified because the 100 times test for Category 2 could not be applied. The $MTTF_d$ in Category 3 was judged to be medium to high,which is within the limits of the standard. The Diagnositc Coverage was between low and medium, which was also acceptable. The CCF was above 65 percent. The chart also show that this functional system meets the requirments of SIL 2.

How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process (cont.)

Table of Contents

The Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA)

A free software tool is available to help with the five steps of the risk reduction effort. The SISTEMA software utility provides developers and testers of safety-related machine controls with comprehensive support in the evaluation of safety in the context of ISO 13849-1. The tool enables OEMs to model the structure of the safety-related control components based upon the designated architectures, thereby permitting automated calculation of the reliability values with various levels of detail, including that of the attained Performance Level (PL).

Relevant parameters such as the risk parameters for determining the required performance level (PL_r), the category of the Safety-Related Part of a Control System (SRP/CS), measures against common-cause failures (CCF) on multi-channel systems, the average component quality ($MTTF_d$) and the average test quality (DC_{avg}) of components and blocks, are entered step by step in input dialogs. Each parameter change is reflected immediately on the user interface with its impact upon the entire system. The final results can be printed out in a summary document.

Many of the leading functionally integrated safety systems providers, such as Festo, offer for free download safety driven parameters in a format compatible with the SISTEMA data base. Rockwell offers Safety Automation Builder, which also integrates with SISTEMA. This supplier effort saves significant time for the OEM design team as they document their efforts to assess risk. The IFA, the German creator of SISTEMA, collaborates with the American National Standards Institute (ANSI) to further globally acceptable safety standards in this effort.

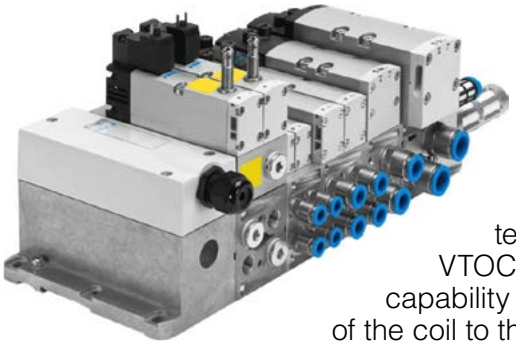
Integrated functional safety systems – new solutions from component suppliers

Traditionally, the design team specifies all the various components and is responsible for assembling the entire input-logic-output system. In this scenario failure data would have to be collected from each manufacturer. Today a number of leading suppliers are designing and manufacturing functionally integrated safety systems. This means the OEM can specifiy one, not multiple, part numbers, which saves considerable amounts of time, expense, and inventory. It makes computations much easier. It also ensures uniformity across various installations. This is particularly important for multi-national companies with many different plant locations.

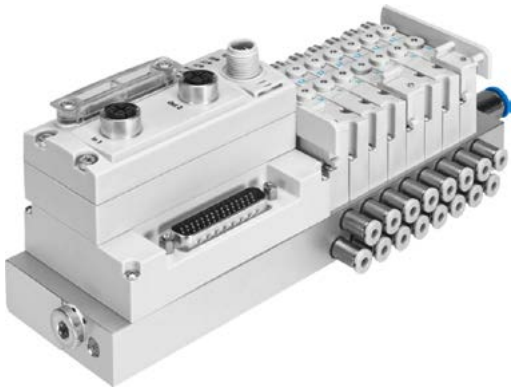
For example, the Festo VTSA valve terminal provides directional pneumatic valves, in this case, ISO standard valves, with integrated pneumatic features and electronic sensor feedback for valve shift. This combination allows the OEM to use safety I/O devices to control specific functions of a valve terminal and obtain the required feedback for Category 3 and 4 installations. These safety functions include preventative start-up by blocking pilot air and solenoid power, safe exhausting through control and monitoring of an integrated exhaust valve, and also safe reversing through control and monitoring of a dedicated redundant valve pair tailored for one actuator.

How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process (cont.)

Table of Contents



In the case of the VTUG and VTOC, Festo engineered a unique modularity option for these electric multipin pneumatic value terminals. VTUG and VTOC terminals have capability to access both pins of the coil to the interface. This provides a variety of benefits. First, it can isolate both sides of the coil. This may be necessary in a safety application, where any chance for a short to actuate a coil must be eliminated. This also facilitates custom requirements, such as inserting diodes to restrict current flow in certain conditions. This custom assembly will be done by Festo on the mating board and housing. This valve solution provides the OEM with multiple ways to integrate a safety related part of the control system and achieve the safety levels desired. Image below of the VTUG valve terminal.



Many other technical advances have been developed in recent years that make the machine safety task much simpler, at least from a hardware, software, and systems point of view. Some of these advancements include the addition of safety I/O and a safety PLC. This preserves the original PLC-based control system. Furthermore, many of today's PLCs combine machine control and safety functions in a single controller, thus simplifying everything from initial design to wiring, installation, and commissioning. It also simplifies diagnostics, since technicians only have to deal with one system where diagnostics can be handled through programming.

There are increasing numbers of sensors and control devices that can be incorporated into the overall system along with diagnostics to identify problems. The safety and control networks can accommodate dozens if not hundreds of devices on a machine – far more than is possible through hardwiring – making the safety system even more capable.

Integrated safety systems simplify programming because both machine control and safety functions are programmed in the same language. Programmers don't need to learn one language for the control PLC and another for the safety controller; the entire system can be implemented in one software package.

Safety functions can be varied based on machine design and intended use. For example, a "slow-down" mode could be made available so that it allows workers access to components when a machine is running in a safe way- This is important because some problems simply can't be diagnosed when a machine is off. The slow-down mode allows a maintenance technician to diagnose and repair a machine in a safe way without bypassing important safety measures. This is a great example of how employing proper safety measures can actually increase productivity.

How to Lower Risk and Document the Safety of Factory Automation Systems through a Five Step Process (cont.)

Table of Contents

In some cases, it is difficult and expensive to hardwire safety sensors to safety I/O because of limited access, long distances, and limited space. Wireless safety devices eliminate these problems because they are easier and faster to install than hard wiring and take up little space.

The journey toward greater safety and compliance to national and international standards can lead the machine builder to an overall more effective and efficient design and to a machine solution with a competitive edge.

Additional information on safety can be found on the Festo machine safety page under "Applications" on the company's website. To discuss these issues in person, call Festo at 800-993-3786.

About Festo

Festo is a leading manufacturer of pneumatic and electromechanical systems, components, and controls for process and industrial automation. For more than 40 years, Festo Corporation has continuously elevated the state of manufacturing with innovations and optimized motion control solutions that deliver higher performing, more profitable automated manufacturing and processing equipment.

Connect with Festo:

Table of Contents

About Festo

Full Range of Standard and Customized Products

With a comprehensive line of more than 30,000 automation products, Festo can support the most complex automation requirements.

- Pneumatic Drives
- Servo Pneumatic Technology
- Handling & Vacuum Technology
- Air Preparation, Pneumatic Connections and Tubing
- Valve and Valve Manifolds
- Sensors and Machine Vision
- Control Technology
- Electromechanical Components

Industry Specific Expertise

Whether designing new machinery or modernizing existing systems, Festo can provide the resources you need to meet your unique requirements in every stage of industrial production and manufacturing.

- Automotive
- Biotech/Pharmaceutical
- Electronics/Light Assembly
- Flat Panel/Solar
- Food & Beverage
- Lab Automation
- Printing, Paper & Converting
- Water/Wastewater

Complete System Solutions

Our experienced engineers provide complete support at every stage of your development process, including: conceptualization, analysis, engineering, design, assembly, documentation, validation, and production.

- Engineering & Design
- Handling & Custom Assembly
- Control Systems

Training & Consulting

Our dedication to the advancement of automation extends beyond technology to the education of current and future automation and robotic designers with simulation tools, teaching programs and on-site services. Festo Didactic is the knowledge and learning division of Festo Corporation. Didactic's charter is to provide automation technology training for manufacturing employees at our industrial customers worldwide.

From basic training packages to the planning, control and handling of complex networked CIM systems and complete, fully equipped learning centers – we can create a customized offer to suit your personal requirements for efficient learning and guaranteed results.

Web Resources

For more information about Festo Corporation:
www.festo.us
Festo Corporate Overview
New Product Highlights
Social Media

Key Company Contact:
Phone: 1 800 99 FESTO
Fax: 1 800 96 FESTO
Email: customer.service@us.festo.com