SAFE PAPER

autec
safety remote control

Contents

Glossary, Standards and Abstract in the pull-out

Introduction

To everybody involved in the protection of people and equipment in the workplace...

In recent years, many industrial machines have greatly enhanced their versatility and productivity with the implementation of various electronic control techniques. The introduction of sophisticated components and systems has required new methods to assess their safety performance.

As a result, major advancements in the standards governing the safety of machines have also been required, and we have seen the release of risk-based, quantitative Standards by both the IEC and ISO global organizations. Guided methods within these standards greatly assist in the implementation of state-of-the-art safety solutions, and now allow a simplified selection of safety components and systems to achieve the appropriate risk reduction.

At the same time, the advantages of remotely controlling a machine have become so universally recognized that the latest generation of safety standards could no longer omit specifications for these types of communication and control systems. With these new standards in widespread use, many regulators are now giving some additional scrutiny to safety-related wireless control systems.

This paper aims to be an objective and comprehensive reference for persons involved in the selection of wireless remote control systems in safety critical applications.

We hope this document aids you in that task, and continue to appreciate your comments and suggestions that allow us to keep improving it.

To all our valued contributors to this second edition – both from within Autec, and from our partners and peers – thanks for your passionate involvement!

Antonio Silvestri
autecsafety.com

Radio remote controls for lifting applications: functional safety

Introduction to safety radio remote controls

In past years, radio remote control systems have become commonplace on lifting machines of all sizes. With such universal acceptance, users and purchasers of radio controls have come to regard them as convenient, safe and reliable. But in the global village of today's marketplace it's not always as simple as that. The most fundamental responsibility of an employer is to provide a safe workplace, and regulatory bodies around the world are increasing the requirement for employers to be able to show how this is achieved. When selecting safety-related equipment, such as remote controls for lifting machines, the criteria and processes used for making that decision should be demonstrable.

Compliance of radio remote controls with the relevant Standards

The first step is therefore to demonstrate that a radio remote control is in conformity with all of the standards in force in the market in which the equipment will be used. Depending on the jurisdiction, regulations relevant to radio controls fall under several categories:

➜ Radio emissions and immunity: these requirements address the risk of interference of the device with other radio devices, and the health risks associated with electromagnetic radiation. For example, the R&TTE directive and its harmonised standards (EN 300220, EN 61000, EN 301489), FCC part 15/90, AS4268.

➜ Functional safety: these requirements are the most complex, and address the risk that the device may malfunction causing dangerous machine behavior. For example, EN ISO 13849-1, IEC 62061, AS4024.

➜ Requirements specific to the lifting machine: these standards may impose special requirements on the system in a wide variety of ways, including safety performance, physical parameters, labelling, etc. For example, EN IEC 60204 1/32, EN 13557, AS 1418, ANSI ECMA 15:2010.

➜ Electrical safety: these requirements aim to control the risk of electrical shock and fire, and are common to a wide range of electrical equipment. For example, the Low Voltage Directive (EU) or AS/NZS 3000 (Australia and New Zealand).

These regulations can be complicated, and can interact with each other. It is also important to recognise that they also call for *minimum* requirements. Simply meeting these requirements may not be enough to satisfy the over-riding requirement that a radio control is 'safe' or, in other terms, that it reduces risk to a tolerable level.

A second step is to make sure that the radio remote control also complies with

the suitable protection level resulting from the evaluation of the risks ("Risk Analysis" is the correct procedure to be used for this task).

How to tell if a radio control is suitable

Appearance is a very poor guide to the safety of a remote control, as some types that are fundamentally flawed look very similar to other radio control systems. There are, however, two things that can be examined with the naked eye:

➜ Is the Stop button a mechanically latching type? As with all Stop buttons, those on radio controls should use positive-breaking normally closed contacts. Once activated, the Stop button should need to be manually reset before the radio control system can be used again. If the Stop button on a radio control system appears to be a standard pushbutton, then additional enquires are warranted.

➜ Does the radio control system use rechargeable batteries? Most 'safe' remote controls use rechargeable batteries for a simple reason - they are transmitting constantly once turned on, even if no command is active. This is necessary so that the radio control system fails safe in the event that communication between the transmitter and receiver is lost. Some radio control systems that use standard, non rechargeable batteries can employ them because they only transmit when a command is being given. While this results in a much lower power consumption and longer battery life, it drastically reduces safety.

Beyond these simple observations, purchasers should first look for compliance with the mandatory standards. The protection of the radio control system against faults should also be determined, normally considering both the Stop function and the motion controls separately. While manufacturers' self-assessments of the safety performance are useful, independent assessments from qualified laboratories (for example, notified bodies competent in functional safety) are clearly more valuable.

But the best defence that a purchaser can have against selecting an inappropriate radio control is to build up some knowledge of the technology so that the choice is not based on price, appearance, or manufacturers' unsupported claims, but on sound principles.

Reliability versus safety

Many "unsafe" radio controls find their way onto lifting machines because purchasers are unaware of the requirements, or lack the knowledge to apply them correctly. In some cases, the lack of attention by the manufacturer of the radio control system to safety issues is reflected in the overall build quality, and the user becomes aware of the poor performance. But in other cases, the user may be quite satisfied with the day-to-day use of an unsafe radio control. This is not surprising, because performance under fault conditions is a very different thing to basic functionality. As with most safety issues, inattention to the safety needs can go unpunished for much of the time - the shortcomings are only exposed when something goes wrong, sometimes with tragic consequences.

What next?

As outlined in these first paragraphs, safety in radio remote controls involves different aspects, which are thoroughly explained in the next sections of this paper. The first section "Safety in digital Communication" explores concepts related to radio transmission. This is of high importance since a safety related message must be properly protected from the interferences of an open and congested radio spectrum. The Safety Functions typical of control systems in machinery applications are considered in the section "Failsafe radio remote controls". Here some techniques used to ensure that these functions are properly protected against dangerous faults are also described. The final part, "Functional Safety", deals with the fundamental principles of safety in control systems. This knowledge sets the basis of system classification regarding safety performances, with an eye on the present standards and on the value of product certification for Functional Safety.

Safety in digital communication

Safety is the principal requirement of any machine, and must be properly assessed and verified for each component. This is particularly important for machines such as cranes and hoists that typically operate above and around personnel, where uncontrolled motion could present many hazards. Of course, it is even more critical in the protection of people who work on platforms. The control system of these machines is required to behave in a safe manner, even in the presence of faults. When wireless control is used, analyzing the safety performance becomes more complex, and some knowledge of the terminology and techniques used can aid in understanding the requirements.

The following section introduces this topic, explaining the basic principles for those involved in choosing and using radio remote controls for cranes and other machines. We will, in particular, analyze some safety-related concepts in digital communication.

A remote control system typically comprises two main components - the transmitter and the receiver. The transmitter accepts operator commands from pushbuttons, joysticks, and other devices and encodes these commands into a message that is sent to the receiver. The receiver detects this message, decodes it to retrieve the commands, and then performs the commands that it was given. In most cases, these messages are sent over a radio link, but other media such as infrared or fibre-optics are sometimes used - most of the design principles discussed here are common to them all.

A wireless control system must protect the link between the transmitter and receiver against several potential hazards. For example:

➜ External EMI noise or other interference must not cause unwanted motion of the machine.

➜ Each transmitter/receiver pair must be uniquely coded to prevent control of the wrong machine.

➜ There must be a suitable response time for commands to be executed - in particular a maximum guaranteed time for recognition of a Stop command.

Furthermore, this protection of the communication link and its response time must be maintained, even in the event of a fault. Below, we explore some of these techniques that can be used to protect a wireless system against these risks.

Managing interference: communication errors

The past few decades have seen the rapid proliferation of wireless communication systems, with large increases in both the number of applications, and in the number of units in use. With an

increasingly congested radio spectrum, the resolution of interference problems is becoming fundamental to both safety and reliability.

In a wireless control system, the messages sent from the transmitter to the receiver (often referred to as telegrams) contain the commands that the operator is giving to the machine. Obviously it is vital that these commands are understood correctly at the receiver, and any damage or corruption of the telegram does not result in erroneous machine motion. To that end, each telegram must include some additional information to function as an error-check so that the receiver can ensure that the telegram was received correctly. Error-detection methods are heavily founded in mathematics, and vary in complexity and efficiency.

Typically, though, special coding systems are used such that a small change in the input data (i.e. the commands for the RRC system) causes a large change in the telegram. This minimizes the chance that two (or more) errors could cancel each other out, and make a damaged telegram appear valid.

In fact, the number of simultaneous errors that would need to occur in order to defeat an error-detection system is a measure of its effectiveness, and is called Hamming Distance (referred to here as HD)– a higher number indicates a better system.

Managing interference: co-existence with other wireless control systems

Control systems that communicate over wires (or optical fibres) are relatively simple to manage, because there are a limited number of devices connected on the network which use standard communication protocols - for example, Modbus, Profibus, DeviceNet, Canbus, etc.

In a radio remote control application, however, the communication medium is open. This means that we can never guarantee that the receiver will not be exposed to messages being transmitted by other remote control systems, even those located far away. In this case, the use of standard protocols increases the similarity between telegrams on different devices, thus increasing the risk that an overheard telegram from another system may be inadvertently decoded and accepted.

Such an occurrence cannot be considered a random event (such as noise damaging a telegram) – on the contrary, it is a systematic risk.

Use of proven proprietary telegram protocols helps protect against interference from other types of systems. But in order to avoid problems with similar systems from the same manufacturer, it is also vital that there is rigorous management of unique (non repeatable) identity codes for each safety radio control system.

Managing interference: sharing the radio spectrum

Like many of the world's natural resources, the radio spectrum is finite, and some means must be provided to share it amongst the increasing number of people and devices seeking to use it. This is usually obtained by partitioning the available spectrum into as many "frequency channels" as possible, whilst maintaining sufficient spacing between them to avoid interference. The more channels that are available, the larger the number of systems that can successfully co-exist on the same site. The maximum number of channels is set by regulatory as well as technical constraints.

focus on... measures of error-detection

The Hamming Distance (HD) between two strings of equal length is the number of positions at which the corresponding symbols are different. Put another way, it measures the minimum number of substitutions required to change one string into the other, or the number of errors that could transform one string into the other (e.g.: the Hamming Distance between "bored" and "robed" is 2, and between 1001100 and 1011001 is 3).

Some existing standards specify a required HD of 4 – this is easily achievable with modern techniques, but may still be insufficient for systems having long telegrams (e.g. a radio remote control with many commands) and/or telegrams that are sent very frequently (as is normal for radio control systems in order to have fast reaction times).

The ultimate measure of error-detection performance is that of Residual Error Probability - i.e. the probability that an error is not detected. Under given conditions, increasing the Hamming Distance will result in a reduction of the Residual Error Probability. The latest generation of state-of-the-art radio remote controls use coding systems with Hamming Distances in the range 8 to 15 - which reduces Residual Error Probability below 10^{-9} (one in a billion) or even below 10^{-15} (one in a million billion!)

focus on...
ensuring unique identity codes

To ensure that only the correct machine is controlled, different radio systems must be distinguished from each other by each having a different ID number, common for each receiver/transmitter pair, but different between systems. One common method is to use a number of small switches or links to set the code number in the transmitter and receiver - typically about 16 switches are used. The switches may be set in the factory to a different value for each system, or this may be left for the purchaser to do. In either case, there are serious problems with this approach:

➜ More than one remote control may be set with the same code because the manufacturer re-uses them.

➜ Two or more users may co-incidentally set their codes the same.

➜ One of the switches or links may move, or become contaminated, changing the ID number.

➜ A person may tamper with the ID number of the transmitter or receiver.

➜ This system may not comply with some regulations, for example, that the address system be “failsafe and tamperproof” (EN IEC 60204-32, AS1418.1).

A safer approach is for the manufacturer to assign an ID code to each system that is guaranteed unique in the world. The ID code may be stored in a removable sealed module to prevent tampering, yet enabling simple exchange if service is required.

Another possibility is to memorise a different serial number on each unit, and then provide controlled and safe procedure for pairing a transmitter to a receiver before installation.

For some very low quality systems changing the radio frequency can be performed only by the manufacturer or a service agent, because it may require substitution of internal modules or components. This is a very old-fashioned approach - certainly not one suitable for today’s crowded wireless environments.

A better solution that is also common are radio modules featuring “frequency synthesizers”: here the operating channel can be chosen in various ways - by means of dip switches or rotary selectors, or blindly changed with a special procedure, or even automatically changed at every power-on. Typically, at least 32 non-overlapping channels are usually provided.

This seems to be a simple and practical solution, but unfortunately, with the continuous growth in number of wireless devices, the effective manual management of channels is now not a simple task in a busy working yard or industrial plant. New systems may come in and out of the site many times during the day - compromising even the most accurate channel plan. It is likely that the devices will be from various manufacturers; so changing the operating frequency may require knowing many different procedures.

That’s why technology improvements that automate channel management, or even overcome the need for it, have been proposed by some remote control manufacturers.

When a transmitter is equipped with a built-in receiver (together referred to as a *transceiver*), it may provide an *automatic channel selection* capacity. The transceiver can monitor the amount of traffic on each channel, and choose to operate on the least congested among them. The selection may be made when the system is started, or continually while the system is in use. The former is simpler to implement, any will operate satisfactorily in many situations - but the operator may be occasionally forced to restart the system as the interference environment changes.

For a system to actively manage the operating channel while the system is running requires more technical complexity, as a transceiver will also be required on the receiver side. But the improvement that this offers is that the system can maintain a stable link even with varying interference profiles, as long as the operator remains within the operating range.

Thus, the use of transceiver radio modules is needed to implement advanced frequency agility for interference avoidance. With a radio channel then available in both directions, data-feedback from the machine to the operator becomes a simpler task than in the past, allowing for a higher refresh rate and easier installation.

Though not itself a safety function, in some applications, data-feedback may undoubtedly add to the overall safety of the system. For example, critical operating parameters of a crane (such as wind speed and hook load) may be monitored by the operator directly on a display mounted on the portable transmitter, so that he could act before an automated safety reaction of the control system occurs.

focus on...
sharing the radio spectrum: techniques across the world

These techniques for automatically managing the operating frequency are certainly advantageous, and are mandated in regulatory standards all over the world. On the other hand, as different markets are differently regulating the radio spectrum, we are far from reaching a worldwide standard.

For example, Japanese ARIB STD-T67 requires a "Carrier Sensing Device" to test the presence of a radio wave on the selected channel, before initiating any transmission; once a channel is assessed as free, it can be occupied indefinitely; if it is found busy, it simply cannot be used.

European EN 300220 specifies a "Listen Before Talk (LBT)" spectrum-access technique, which asks that the channel is tested periodically before every one second transmission; the standard also encourages "Automatic Frequency Agility (AFA)" to avoid busy channels. The additional technical complexity is rewarded with the permission to use almost all of the 863 - 870 MHz band without the need to observe the very strict duty cycle limits applied to conventional devices.

A totally different approach is used in "Frequency Hopping Spread Spectrum (FHSS)", as specified by the American standard FCC 47 CFR part 15.247 and its Canadian and Australian equivalents.

Here the radio communication must use a frequency that is periodically changing according to an agreed sequence of "hops" known to both the transmitter and receiver, but that appear random. Each channel can be used for a very short time (tens to hundreds of milliseconds), while it is also necessary to wait a much longer period (seconds to tens of seconds) before repeating the hopping sequence.

This way many similar systems operating on the same site are very unlikely to jump with synchronized sequences; in practice they will never or rarely collide, thus removing the need for frequency coordination. The complexity of such a system is quite high, but the relevant standards offer a much higher transmission power limit, because the average power on any channel remains low – this in turn allows for an extended reliable communication range.

A fixed channel device may operate normally in the presence of a frequency hopping system, because it will usually be able to withstand very short interference bursts. But, as the number of frequency hopping systems in a location grows, the situation for the fixed channel device will sooner or later become unsustainable. For that reason, the European standard EN 300220 also suggests combining together FHSS and LBT in an even more powerful interference avoidance technique to give the best outcome for coexistence amongst all types of spectrum users. This is now offered in the most advanced RRC systems, and is expected to become more widely adopted in the coming years.

Response time

The minimum response time of a radio remote control system is dependant on the data rate, which is itself dependant on the quality of the telegram used, the radio components, the noise level, and the operating distance. Response times in the range of 100 milliseconds are normally perceived by an operator as instantaneous, and are usually much less than the response time of other electromechanical components. From a safety viewpoint, though, the *maximum* response time is more important. The actual response time of the control system may increase above the theoretical minimum due to interference causing some telegrams to be damaged, and thus rejected. This delays the reception of a valid telegram, and during this period operator commands will not be put into action. Clearly this is a potential hazard which must be managed. After a predetermined amount of time has elapsed without a valid message from the transmitter, the receiver must perform a stop and bring the machine to a safe state. The permitted time may vary from application to application, though the most common limits are between 0.5 and 2 seconds, as required by EN IEC 60204-32 and AS1418.1. The mechanism by which the loss of valid signal reception for a period of time causes the machine to revert to the stop state is called a Passive Stop, and is a fundamental requirement of a safety radio control.

Another such requirement is a Stop button or other actuator that the operator can use to quickly bring the machine to a safe state. For this function the maximum response time set in EN IEC 60204-32 is 550 ms; but it is necessary to consider the specific requirements needed in the real application, which may be shorter. The Stop pushbutton must be a normally-closed type

with positive-break contacts – i.e. the operating force of the button must act directly on the contacts to force them apart without reliance on springs or other mechanisms. Standard pushbuttons with normally-open contacts are completely unacceptable for use as Stop actuators in safety systems.
Some radio control types use the Stop button to simply turn off the transmitter, and rely on the loss of signal at the receiver to cause a Passive Stop. The disadvantage of this technique is that of response time - the machine will not revert to the safe state until the Passive Stop time has elapsed. A better solution is to send a dedicated stop-telegram to the receiver when the operator presses the Stop button, a technique known as an Active Stop. This results in a rapid response time if the stop-telegram is received correctly. If it is not, the system will stop anyway after the Passive Stop time due to loss of the normal telegram. The mix of these two techniques can therefore provide the best of both worlds: the rapid response time of the Active Stop and the safety net provided by the Passive Stop.

Frequency Management	Pros	Cons
Fixed frequency with PLL synthesizer	Simpler, cheaper; when proper frequency coordination is possible, it operates very well	Needs frequency coordination of all devices present in the same site; in practice, periodic re-tuning will be needed as the environment changes
Listen Before Transmit + Automatic Frequency Agility	Automatic frequency coordination; allows use of a broader frequency range in Europe	Higher complexity; if many devices are present on the same site, full advantage is obtained only when all devices in the same site use LBT: it only reaches its full potential when regulations mandate its use, and are enforced
Frequency Hopping	No need for frequency coordination; mitigation of fading effects; allows use of a broader frequency range in Europe; allows use of a higher power in North America and Australia	Higher complexity; not permitted in all jurisdictions; it may suffer communication delays in the presence of many fixed-frequency interferers
Frequency Hopping + Listen Before Transmit	Same as Frequency Hopping + seamless avoidance of interference	Highest complexity; not permitted in all jurisdictions; as for LBT-AFA, full advantages are obtained when all devices in the same site use LBT

Failsafe radio remote controls

As stated in the previous parts of this paper, the primary safety function of the radio remote control system must be the ability to bring the machine to a safe state. Protection of the Stop function against faults is therefore clearly critical. It should be noted, though, that protecting the Stop system is not enough to achieve a safe system, as it is reliant on the human operator to take appropriate and timely action in an emergency. The operator may not be present, or not be aware of the hazard, may not react in time, or may even take some action that makes the hazard worse. Some benefit is gained by ensuring that an unused transmitter turns off (initiating a stop condition) when it has been idle for a period of time. But again, this alone is not sufficient - the radio control system must be protected against faults that cause the initiation of unexpected motion, without requiring the operator to activate the Stop. For that reason, we consider here the safety performance of a remote control based on two possible failures:

➜ Failure of the Stop function.

➜ Unintended Movement From Standstill caused by a fault (also called UMFS protection).

Duplicate Stop outputs

One of the most predictable hazardous faults that could occur in a radio remote control system is that the Stop output does not turn off when required. Typically, this problem is addressed by using two Stop outputs, both of which could independently take the machine to a safe state. While this is definitely

focus on... UMFS protection

Unintended Movement From Standstill (UMFS) protection avoids any unwanted movement from any single fault affecting the control system.
This function automatically maintains the machine in the safe state in presence of faults or errors, when actuators are in the neutral position.
In Europe, the Machinery Directive 2006/42/EC requires that reasonably foreseeable misuse must be taken into account. Annex I, section 1.2.2, requires that “When designing and constructing machinery, and when drafting the instructions, the manufacturer must envisage not only the intended use of the machinery but also any reasonably misuse thereof”. Statistics confirm that human behaviour in emergency conditions is difficult to predict, and often could even worsen the situation. This emphasises that UMFS protection is becoming a necessary measure to reduce risks. A correct risk analysis not only calls for the protection of the Stop function, but also requires that the UMFS protection be handled as a safety function.
Also in the USA, the unintentional actuation of a motion must be protected. The ANSI ECMA 15:2010 “Specification for Cable-less Controls for Electric Overhead Travelling Cranes), section 4.14, requires that “Functions controlling motion shall use adequate protection against unintentional actuation”.

standards for radio remote controls

EMC Standards

EN 301 489-3	Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic compatibility (EMC) standard for radio equipment and services; Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz
EN 61000-6-2	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
EN 61000-6-3	Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments
EN 300 220-2	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1000 MHz frequency range with power levels ranging up to 500 mW; Part 2: Harmonized EN covering essential requirement
ISO 7637-2	Road vehicles – Electrical disturbances from conduction and coupling – Part 2: Electrical transient conduction along supply lines only
ISO 7637-3	Road vehicles – Electrical disturbances from conduction and coupling – Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines
ISO 10605	Road vehicles – Test methods for electrical disturbances from electrostatic discharge
EN 50 371	Generic standard to demonstrate the compliance of low power electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (10 MHz - 300 GHz)

Environmental Standards

IEC 60529 IEC 60529-A1	Degrees of protection provided by enclosures (IP Code)
IEC 60068-2-1	Environmental testing – Part 2-1: Tests. Test A: Cold
IEC 60068-2-2	Environmental testing – Part 2-2: Tests. Tests B: Dry heat
IEC 60068-2-6	Environmental testing – Part 2-6: Tests. Test Fc: Vibration (sinusoidal)
IEC 60068-2-27	Environmental testing – Part 2-27: Tests. Test Ea and guidance: Shock
IEC 60068-2-30	Environmental testing – Part 2-30: Tests. Test Db: Damp heat, cyclic (12h+12h cycle)
EN 60068-2-31	Environmental testing – Part 2-31: Tests. Test Ec. Rough handling shocks, primarily for equipment-type specimens
EN 60068-2-64	Environmental testing – Part 2-64: Tests. Test Fh. Vibration, broadband random and guidance

Electrical Safety Standards

IEC 60950-1	Information technology equipment — Safety — Part 1: General requirements
EN 50178	Electronic equipment for use in power installations
IEC 60204-1	Safety of machinery — Electrical equipment of machines — Part 1: General requirements
EN 13557	Cranes - Controls and control stations
IEC 60204-32	Safety of machinery — Electrical equipment of machines — Part 32: Requirements for hoisting machines

Functional Safety Standards

EN ISO 13849-1	Safety of machinery – Safety-related parts of control systems
IEC 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
IEC 61508	Functional safety of electrical, electronic, programmable electronic safety-related systems
IEC 61784-3	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions

pull-out

safety glossary

CCF (Common Cause Failure)
Simultaneous failure of different parts of a system as a result of a single event. This does not consider the case when the failures are a consequence of each other as in a chain of events.

Failsafe
Capability of a device or system to reach a safe state in case of fault.

Failure
An event in time where an item fails to perform a required function. After that, the item has a “fault”.

Fault
A state of an item that is no longer able to perform a required function.

Functional safety
Part of the overall safety that depends on the proper working of the process or of the equipment in response to relevant inputs.
Example: a cage surrounding a machine that prevents the user from touching moving parts is not an example of functional safety. An interlocked gate with limit switches and safety contactor where opening the gate stops the movements of the machine is an example of functional safety.

Harm
Physical injury or damage to health. Its severity is considered during the risk assessment, and may be minor or even fatal.

Hazard
Potential source of harm. Hazard must not be mistaken for its consequences (such as burn, cut, crush injuries). Example of hazards are a motor, a piston, a pump, a knife. Different phases of machine’s lifecycle pose different hazards.

Hazardous situation
Circumstance in which one or more persons are exposed to an hazard. This exposure might result in harm either immediately or over a long period of time.

Manufacturer
Any natural or legal person who designs and/or manufactures something (e.g. machinery, radio remote control) and is responsible for its conformity with a view to its being placed on the market, under his own name or trade mark or for his own use.
In the absence of a manufacturer as defined above, any natural or legal person who places it on the market or puts it into service.

Reasonably foreseeable misuse
the use of machinery in a way not intended in the instructions for use, but which may result from readily predictable human behavior.

Risk
Combination of the probability that harm occurs and the severity of the harm.
Risk = Probability x Severity.

Safety
Absence of unacceptable risks - risk reduction to tolerable levels.

Safety function
A function of the machine, the failure of which may result in an immediate increase of the risk. Failure of the safety function does not itself lead to harm, but this might occur if the failure happens in a hazardous situation.

Systematic failure
A failure having a deterministic relationship with its cause. This type of failure may only be eliminated by modifying the development / production processes or the operational procedures. Systematic failure may arise at the specification stage, during design, manufacturing, or installation as well as during design and implementation of any incorporated software.

wireless communication glossary

AFA Automatic Frequency Agility
Capability of a device to change the operating frequency channel if it is unsuitable for use, e.g. if found busy after an LBT check. Some commercial equivalents: Automatic Channel Selection, Automatic Frequency Tuning,

(Frequency) Channel
The available radio spectrum may be sub-divided into smaller, non-overlapping, slices of frequencies. Ideally, if any system is able to keep its emissions inside that slice, and separate the signals sent on different slices, then many different communications may be held on the same time, each one on a different “channel”, without interference from the others.

Duty Cycle
The proportion of time during which a transmitter is actively transmitting messages to the receiver, averaged over a one-hour period, and normally expressed as a percentage.

EMI noise
Electro-Magnetic interference, that is radio waves unwantedly emitted by electric-electronic equipment, which appear as “polluting” the environment where the RRC is operating. EMI from any device has to be reduced below specified emission limits; any device shall show a minimum immunity to EMI coming from others.

FHSS
Frequency Hopping Spread Spectrum, a technique of accessing the radio spectrum which involves jumping (hopping) continuously on different channels on a broad radio spectrum. The purpose is to minimize the effect of a fixed frequency interferer, as well as to cause the “shortest” interference to other systems.

Interference/Interferer
Often used with the same meaning as EMI noise, more appropriately refers to intentional radio-wave emitters that are using the same radio spectrum as the RRC, potentially causing imposition and disturbance to operation. An example interference source is a second RRC system.

LBT
Listen Before Transmit (or Talk), a technique of accessing the radio spectrum which involves checking periodically that a frequency channel is free, before using it.

Radio Spectrum/Frequency Band
A defined range of radio frequencies containing a number of channels available for use.

Response time
The time needed for triggering a corresponding action on the machine, after a command has been activated on a remote control transmitter.

Telegram
Coded message sent periodically from a transmitter to a receiver.

Transceiver
(Radio) Device capable of operating as a transmitter, as well as a receiver, enabling bidirectional communication.

Wireless control system/radio remote control (RRC) system
Different wordings to indicate the same meaning: a system with at least a transmitter and a receiver device, or two transceiver devices, capable of exchanging commands or data with a machine from a remote position.

abstract

The use of electronic and programmable control systems in machinery for the manufacturing, logistics and construction sectors has proven in recent years that performance and safety can go hand in hand improving the quality of a workplace. The growing awareness of the benefits brought by “safety systems” also helped make these solutions more and more used and widespread, so that they are also becoming universally accepted and more economical than in the past. Furthermore, new worldwide standards are focusing on risk reduction as the most important objective to be achieved in the whole products’ lifecycle.

When it comes to wireless control systems, they offer several advantages over cabled control systems, involving not only increased productivity, but also safer working conditions. As a result, even in the industrial machinery sector, safety today comes together with the highest technology, so that not only have we excellent performance, but we have excellent and safe performance.

When choosing the right radio remote control, manufacturers or installers must obviously take into account the overall safety of the system, which involves electrical and radio aspects, requirements relevant to the specific application and, most importantly, Functional Safety. Each control system that processes a certain input and returns an output aimed at reducing the risk beneath the tolerated level performs what is defined as a “Safety Function”. These functions aim at reducing risks even in fault conditions, and their behavior and structure are described in detail in this paper. Radio communication aspects, as well as an explanation of safety-related international standards, are also dealt with in the document. Particular focus is dedicated to the new international standards that have come into force lately (EN ISO 13849-1 and EN IEC 62061), which introduced both probabilistic and quantitative aspects for the definition of safety functions, involving the entire products’ lifecycle.

The ultimate aim of this document is to offer sound knowledge to identify control systems providing valid safety functions. There are several motivations for pursuing safety in the industrial sector. First of all an ethical reason: each human being deserves the best possible protection from hazards. On the other hand, reducing or eliminating risks will result, in the long run, in a reduction of costs related to workplace injuries (compensation, insurance premiums, downtime costs,…)

It is also true that laws require safety in the working environment, and so international regulations and standards are more and more committed to ensuring a safe workplace and to define measures to prevent accidents. Furthermore, given that the present state-of-the-art technology grants high safety levels and allows the reduction or avoidance of risks, we are now in a better position to select the right safety components to achieve effective protection.

Ways to check products’ compliance with the standards are fully available, and independent organizations can certify the safety performance of components and machinery. Choosing those products that ensure the best possible protection also becomes a winning strategy as proliferation of these systems will result in cheaper safety technologies for all.

an improvement over a single output, it is not a complete solution. If one of the outputs fails to switch off, then we are relying on the second output to stop the machine. But if there is no indication that the first output has failed, the radio control is now operating without the protection of a second Stop output. A manual inspection of the outputs may reveal a problem, but it is often impractical to schedule manual inspections at a close enough interval to ensure that a fault is detected before a second fault occurs. It is necessary for the control system to itself detect that a failure has occurred, and to prevent the machine from operating while only one output is operational. This duplication with fault-detection may also be called “redundancy with self-monitoring”, and should be present in safety remote controls used on lifting machines. The Stop outputs from a radio control receiver may utilise a special class of relay known as a “safety relay”. Despite their name, their design is little “safer” than a regular relay - they are still vulnerable to welding, coil burnout, or other mechanical failure. What makes them different is the feature known as “forcibly guided contacts”, and this name is more indicative of their real function. If one set of contacts jams in the ON position, the other set cannot return to the normally-closed position (as can happen in standard relays, particularly those with small contact spacing). This means that the control system can know with some certainty what one set of relay contacts is doing, by monitoring the other set. This simplifies the design of a rugged safety control circuit, where one contact set is used for power switching, and the other set is used for monitoring. Another solution may use solid state outputs that are continuously monitored by the electronics and deactivated if a failure is detected.

focus on... Stop inputs

Some guidelines for actuators carrying out the Stop function can be found in ISO 13850:2006 (Safety of machinery – Emergency Stop – Principles of design). It specifies functional requirements and design principles for the emergency Stop function on machinery, independent of the type of energy used to control the function. It is applicable to all machinery except for machines in which the provision of emergency Stop would not lessen the risk, hand-held portable machines, and hand-guided machines.
According to this standard the Stop button used in a radio remote control should use normally-closed and positive-break contacts – i.e. the activation force of the button acts directly on the contacts to force them apart, and is not reliant on spring pressure or similar to open. Another requirement is that the Stop button should also be latching, and require manual reset. Some safety remote controls use Stop buttons with two separate channels – unless both channels are in the normal position (closed), the system cannot be operated.

Duplicate inputs

To protect the transmitter against failures of its electronic circuits causing unexpected motion, remote controls may use duplicated inputs. Some types use one physical actuator (e.g. button) that drives two separate channels for confirmation of the command. Some models use two electrically and mechanically separated actuators driving the two control channels to confirm each command, thus achieving a higher safety level, because protection is also provided against mechanical failures (such as broken springs, failed contacts, or shorted wires).

Duplicate decoders

As discussed previously, a safety radio remote control has a passive Stop function - i.e. the receiver must receive a valid message from the transmitter within a certain time period or a stop condition will result. The device in the receiver that listens to the incoming messages and decides whether they are valid or not is known as the decoder. If the Stop system is to be protected against faults, it follows that the decoder must be similarly protected. This necessitates the duplication of the decoder (dual channel architecture, using the EN ISO 13849 terminology), and putting a mechanism in place so that unless both decoders agree that a valid message has been received, a stop will result.
Some radio control systems that are claimed to be failsafe do not meet this criteria – they are single-decoder designs. If there is only a single decoder, and the decoder fails, the Stop circuit may not operate correctly. A system of this type is vulnerable to program or data corruption, random hardware breakdown and systematic faults due to software and/or data errors. The situation is similar if we consider the protection

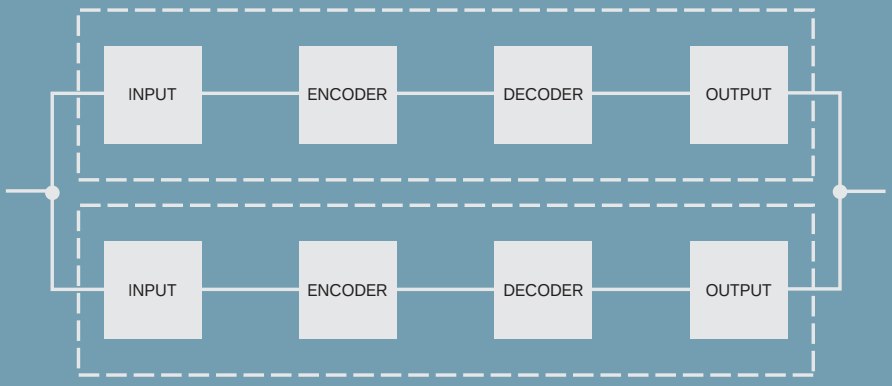
against unexpected motion. Again, in a single decoder system, there is nothing to prevent the failure of the decoder from initiating unexpected motion. To protect against this requires duplication of not only the Stop functionality of the decoder, but of all safety functions it implements. Dual decoders with a voting system are essential to protect against hardware failures: both must agree on a command, or it is not acted on. Still, this can do nothing against common cause failures or systematic faults, such as software errors. If both decoders have an undocumented problem at a specific temperature, both will fail at that temperature. Again, if the same faulty program runs on both decoders they will always agree - but they could be both wrong! Watchdog timers, program checksums and other techniques can partially reduce this risk, but it is unlikely that they can do so to the required level. For higher levels of integrity the decoders should be “diverse”, meaning that both hardware and the software running on them must be different. This is one of the principal techniques used to achieve safety in a remote control system.

Duplicate encoders

We have seen the importance of ensuring that a message is received and decoded correctly, and the way that this can be achieved by the use of dual

focus on...
redundancy

Logical circuit for redundancy:



A single channel system will fail if one of its subsystems fails. A two channel (also called redundant) system would need to have two failures, one in each channel before the system fails.

Basic safety protection for radio remote control systems

Stop outputs	➜ two Stop outputs ➜ use of “safety relays” ➜ fault-detection or self-monitoring
Stop pushbutton	➜ with normally closed contacts, of positive-break type ➜ latching, with manual reset ➜ with two separate channels
Commands	➜ two electrically and mechanically separated actuators driving the two control channels to confirm each command
Transmitter encoder	➜ duplicate encoders to protect the system against initiating unexpected motion ➜ separated inputs
Receiver decoder	➜ dual decoders must both agree on a command before a safety output is activated
Auto turn-off	➜ automatic system shutdown after an idle time to initiate a Stop condition

decoders. It may seem that this is sufficient protection, and that it is not necessary to duplicate the encoder in the transmitter. There is some justification for this argument – if we turn off power to the transmitter using a positive-break switch then it will stop transmitting. With duplicate decoders in the receiver, we know that at least one of them will detect the loss of communication and cause a Stop condition. So we can achieve a basic level of fault protection for the Passive Stop system using dual decoders with a single-encoder transmitter. The situation changes if we also want to ensure the UMFS protection and the Active Stop protection. Let's assume that the received message was correctly structured and sent, but contained the wrong commands because there was a fault in the encoding electronics of the transmitter: in such a situation duplicate decoders will be of no help. So there is also need for some redundancy in the encoders in the transmitter to protect the system against initiating unexpected motion due to a fault. The same consideration on common cause failures and systematic faults described in the previous section holds here. For high safety integrity systems, duplication should be backed by diversity.

focus on... fieldbus outputs

Use of field bus communication has become widespread in the recent years among industrial machinery, mobile machines and lifting equipment due to the obvious advantages in terms of installation and maintenance costs. Examples are CAN, Profibus, Ethernet with their corresponding protocols CANOpen, Profibus, EtherCAT to name a few.

However, the use of these protocols for safety related functions is prevented by some drawbacks – such as insufficient error detection or message latency. The basic safety principles for transferring safety-related messages are specified in the international IEC 61784-3 standard.

To fulfil these requirements, different technology groups have adopted different measures – all relying on some additional protocols "embedded" in the original ones. This has given rise to safety relevant protocols as CANOpen Safety, SafetyBus P, ProfiSafe, Safety over EtherCAT.

No standard or *de facto* standard has yet emerged for safety-relevant communication over the various field buses, so the adoption of one solution may tie the manufacturer to specific suppliers of systems and tools.

Anyway, the compliance alone of a system to a specific safety bus protocol does not imply any safety integrity of the system itself, for the same reasons illustrated before - any output device that "speaks" a safety bus protocol but with a single channel architecture may fail to act properly as a consequence of a single fault. Compliance with a safety bus protocol simply assures to a predictable level that the messages will be delivered in a timely manner and uncorrupted to their recipients, but offers little protection if the message wasn't the intended one, or if a failure in the recipient causes a hazard.

Duplicate outputs

As we have discussed, the Stop outputs in the receiver must be duplicated to ensure that at least one opens to stop the machine in the presence of a fault. If we are to provide protection against unexpected motion (UMFS), then output duplication is also required for the motion commands of the machine. This may take the form of duplicating each command individually, but there is a balance to reach between reliability and safety. If we duplicate each output, we also double the complexity. And unless we monitor the duplicate outputs for possible failure, there is little advantage gained. A compromise that achieves high safety with little added complexity, is to provide additional outputs that remove power from all movements if no motion commands are active. In this way, the system is protected against some output failures such as short circuits with a relatively simple system. If the confirmation output is duplicated and monitored, a high level of protection against unexpected motion may be achieved.

Functional safety: principles and references

Safety electronics

Two main global trends have become evident in recent years, and they are still influencing technical and technological decisions.

On one hand, more and more electrical, electronic and programmable systems are integrated in all types of machinery, including lifting machines. This trend began some decades ago in the automotive sector, where systems like airbags, anti-lock brakes, traction control and stability control finally ensured that performance, reliability and safety coexisted. Since then, electronic systems have been included in the design of many other manufacturing fields. Their effectiveness and proven value are indisputable, and they are now so widespread that they are also highly economical.

The second trend is the increasing importance devoted to safety. Accordingly, international standards have enforced stricter and more precise requirements and restrictions, with the aim of focusing on safety as the most important objective to be achieved in the product lifecycle. As a result, technology has developed with the intention of applying and obtaining safety, which can be described in general as “the reduction of risk to a tolerable level”.

The two trends also affected the machinery sector, including lifting and material handling machines, as well as manufacturing machines - fields where the mechanical aspects traditionally prevailed over others. When designing and producing machines, electrical, electronic and programmable systems offering increased safety levels are now being designed and integrated.

Radio remote controls have followed this same path, integrating more and more electronics and improving the *Functional Safety* of these systems, with Functional Safety being defined as “the safety resulting from the correct functioning of a control system in response to input signals thus reducing external risks to a tolerable level”.

We will therefore focus on functional safety and highlight current standards and their application in the safety functions of radio remote controls.

Functional safety according to EN ISO 13849-1

The reference standard for control systems installed on all kind of machinery for professional and non-professional use is EN ISO 13849-1:2006 (Safety of Machinery – Safety-related parts of control systems) which derives from the previous EN ISO 954-1 and concepts introduced from IEC 61508. This standard describes safety requirements and provides guidance on principles for the design of safety-related parts of control systems.

The main points of the standard are:

➜ It applies to all safety related parts of control systems, regardless of their

nature, e.g. electrical, electronic, programmable, hydraulic, pneumatic, mechanical etc.

➜ It defines different levels of fault resistance by Performance Levels. These indicate the ability of the machine's safety-related control system to ensure the safety function operates under predetermined working conditions. PLs are classified according to the average probability of dangerous failure per hour. There are five PLs, from PL a (the lowest level of risk reduction) to PL e (the highest).

PL is defined as a function of some important parameters:

1) the control system's architecture which is defined by categories, which directly refer to the earlier standard EN 954-1;

2) the reliability of its components which is defined by $MTTF_d$ (Mean Time to Dangerous Failure). Its value can be given in three levels (Low, Medium and High);

3) the ability to detect in a timely manner possible faults, which is defined by DC (Diagnostic Coverage). Its value can be given in four levels (None, Low, Medium and High).

There is also another important parameter for the calculation of PL: CCF (Common Cause Failure). CCF is defined as "failures of different items, resulting from a single event, where such failures are not consequences of one another". EN ISO 13849-1 provides a list of measures known to be effective in avoiding CCF and requires that a system guarantees at least 65% of these measures. This way, the designer can analyze the possibilities for CCF and implements appropriate avoidance measures (such as separation, diversity…) to reach a high level of resistance to these types of failures. In fact, without CCF calculation, a single event may render a 2-channel ar-

TABLE 1

Performance Levels (PL)

PL	Average probability of dangerous failure per hour 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

Note: besides the average probability of dangerous failure per hour other measures are also necessary to achieve the PL.

GRAPHIC 1

Logical representation of different designated architecture for Categories of EN ISO 13849-1

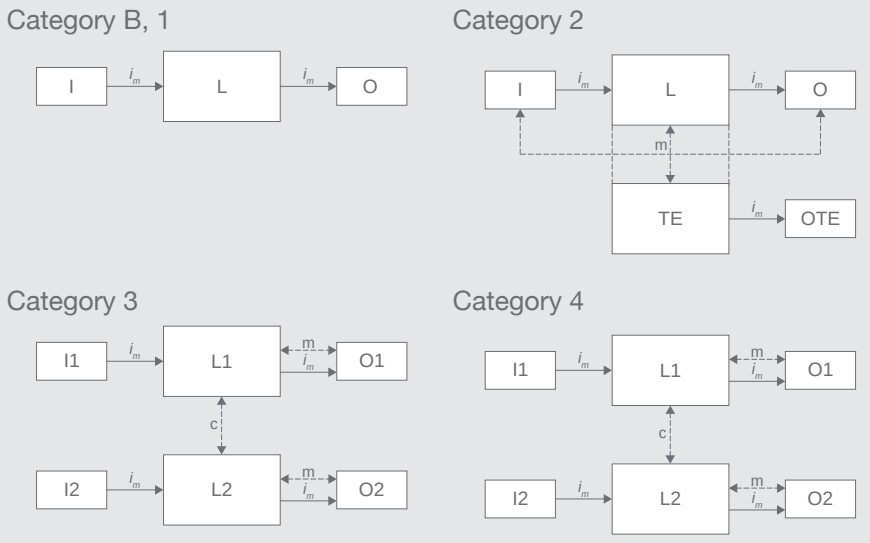


TABLE 2

DC

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

The functional blocks in each architecture represent:

I, I1, I2	input device, e.g. sensor
L, L1, L2	logic
O, O1, O2	output device, e.g. main contactor
i_m	interconnecting means
m	monitoring
TE	test equipment
OTE	output of TE
C	cross monitoring

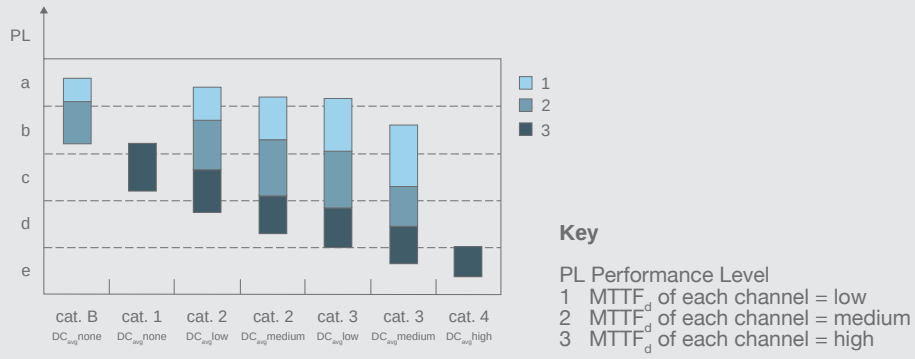
TABLE 3

$MTTF_d$

Denotation of each channel	Range of each channel
Low	3 years ≤ $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ ≤ 100 years

chitecture unable to perform safely.
At the end, if and only if the system architecture complies with one of the designated categories of EN ISO 13849-1, PL may be estimated with the simplified method by taking into account all these parameters and by using Graphic 2.
It is important to note that even if the combination of different architectures, different $MTTF_d$s and different DCs can result in the same PL, a “fail-safe” behavior requires a “reliable”, redundant and monitored structure, that is to say, it requires category 3 or 4.

GRAPHIC 2

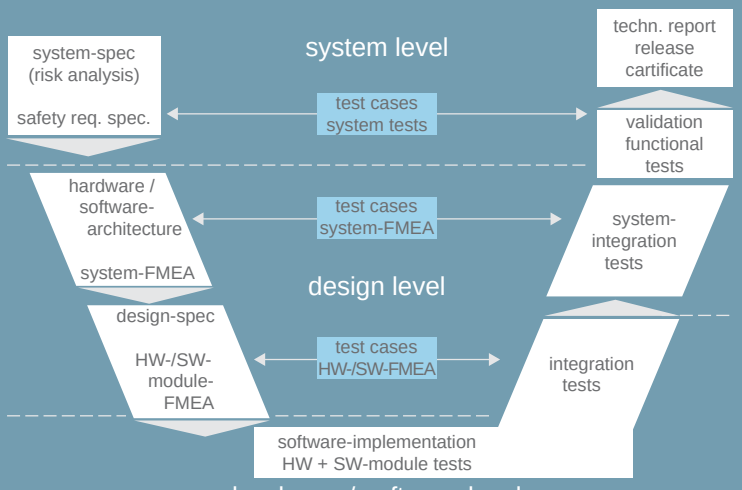


focus on...

certification of functional safety for radio remote controls

Clearly, the standards governing the functional safety of radio remote controls are complex. The analysis of the electronic and programmable systems that comprise them is exceptionally so – in fact, there are very few organizations in the world competent in the assessment and certification of safety electronics (TÜV SÜD and TÜV Rheinland being the most widely recognized). With such complexity involved, manufacturer’s self-declarations of a product’s conformity with functional safety standards should be examined with a very critical eye. It is highly unlikely that a manufacturer working in isolation from independent certification laboratories would even be competent to assess its own products!
For meaningful results, a manufacturer of safety remote controls must work very closely with these laboratories from the earliest stages of a product design through to the production and maintenance processes. As well as independent certification, such a relationship brings major technical and organizational advantages – it proves the manufacturer has the ability to design, test, and maintain this level of safety in its products, and in a way that is transparent and accessible to independent experts. Of course, this requires a commitment of the entire company culture, and would be a process more likely to span decades than months.
Also, a company capable of producing independently certifiable remote controls will bring with it the highly refined design and quality systems that result in a better user experience.
To the purchaser or end-user of remote controls, the use of independently certified systems brings many advantages:
➜ Certainty that they know what they are buying;
➜ Increased safety and reliability, resulting in savings thanks to decreased downtime, reduction of injuries and equipment damage, reduced insurance costs, etc;
➜ Reduced administrative burden in documenting the selection and risk-assessment procedures;
➜ Reduction of exposure to litigation.

CERTIFICATION PROCESS



Process for the design of safety-related parts of control systems

Designing the safety functions of control systems in compliance with the EN ISO 13849-1 is part of the evaluation of a machine's safety, and in the risk reduction process.

The first step to take is identifying which functions of the control system are safety-related - or stated more correctly, the safety functions that a control system must perform.

The second step is to define the required Performance Level (PLr) for each safety function. Identifying this PLr defines to what extent the risk reduction shall be reliant on the safety-related parts of the control system. The more reliant on the control system for risk reduction, the higher the PLr will be.

The risk tree in Figure 1 can be used to define the PLr. It takes into account three parameters:

➜ severity of the possible consequences of a failure;

➜ the frequency and time of exposure to the hazard;

➜ the possibility of avoiding the hazard.

An example

We use here the example of a radio remote controlled overhead travelling crane moving heavy loads in a typical factory environment.

Let's calculate at first the PLr for the radio remote control's Stop function, by taking into account the risk caused if it does not activate when required.

Starting from point "1" in Figure 2:

➜ The possible severity of injury is serious if (for example) a heavy load is dropped or is otherwise not controllable - hence select S2.

➜ The frequency and/or exposure time to the hazard is high if one considers that many persons are working nearby while the crane is in operation - hence select F2.

➜ Finally the possibility of avoiding the hazard needs to be evaluated depending on the specific conditions on that site but, in general, should be possible - hence select P1.

So the minimum PL required for the Stop function is PLr d.

Secondly, consider the risk that a fault may initiate unwanted crane motion. In this case, the consequences of failure without correct and timely operator intervention (via the Stop function) is essentially the same. As previously discussed, we must anticipate that the operator may not be perceive the hazard, or take the correct action in time to prevent it, so we must again select the path S2-F2-P1, and the resulting required level for protection for Unintended Movement from Standstill (UMFS) is also PLr d.

The Performance Level required for the two safety functions of an industrial radio remote control is therefore at least PLr d according to the EN ISO 13849-1.

FIGURE 1

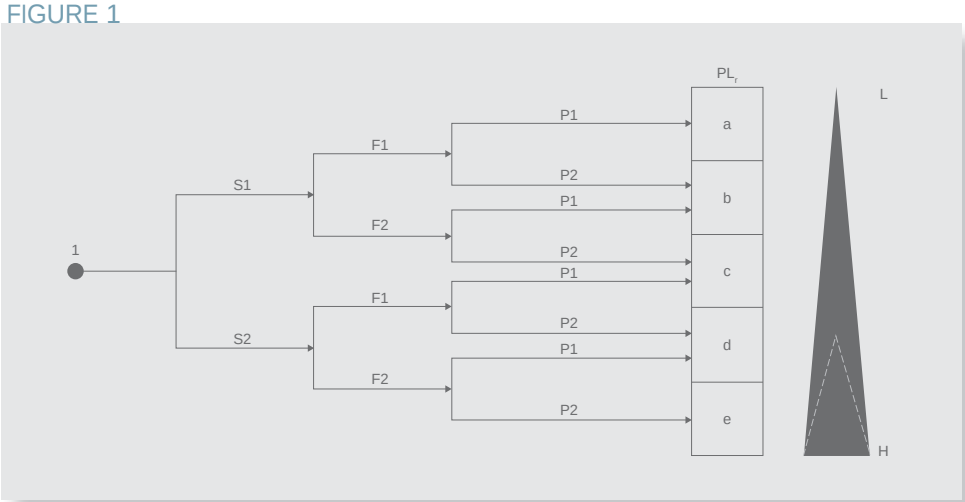
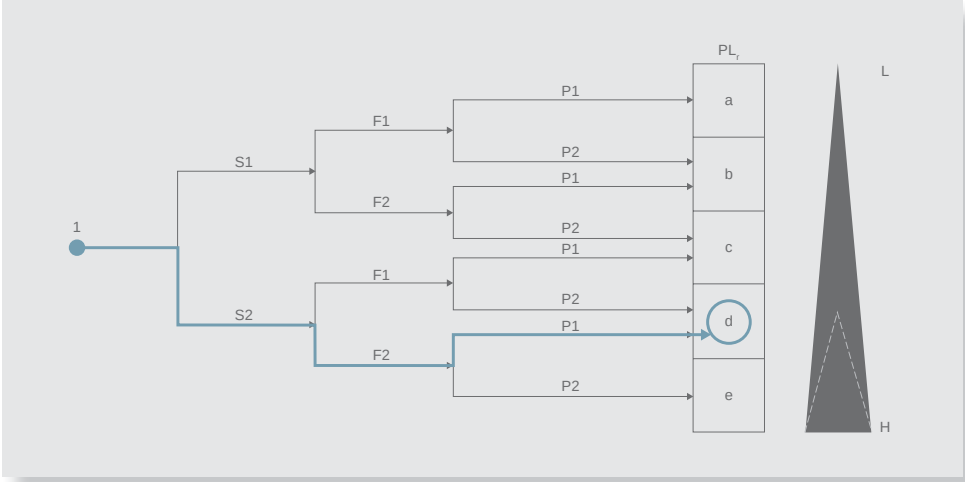


FIGURE 2



Key

1 starting point for evaluation of safety function's contribution to risk reduction
L low contribution to risk reduction
H high contribution to risk reduction
PL required performance level

Risk parameters

S severity of injury
S1 slight (normally reversible injury)
S2 serious (normally irreversible injury or death)
F frequency and/or exposure to hazard
F1 seldom-to-less-often and/or exposure time is short
F2 frequent-to-continuous and/or exposure time is long
P possibility of avoiding hazard or limiting harm
P1 possible under specific conditions
P2 scarcely possible

focus on...
EN IEC 62061

During the last years the IEC (International Electrotechnical Commission) has been committed to define a regulatory framework for functional safety.
The first standard addressing the modern concepts of functional safety is IEC 61508 (Functional safety of safety-related electrical, electronic, and programmable electronic systems). The standard focuses on risk-based, safety related system design, with the goal of implementing only the "correct" level of protection measures, which should result in far more cost-effective safe solutions.
This standard is based on two fundamental concepts:
➜ The Safety Life Cycle is defined as an engineering process that includes all of the steps necessary to achieve the required functional safety. The basic philosophy behind the safety life cycle is to develop and document a safety plan, execute that plan, document its execution (to show that the plan has been met) and continue to follow that safety plan through to decommissioning with further appropriate documentation throughout the life of the system. Changes along the way must similarly follow the pattern of planning, execution, validation, and documentation.
➜ Safety Integrity Levels (SILs) are order of magnitude levels of risk reduction. There are four SILs defined in IEC 61508. SIL1 is the lowest level of risk reduction, SIL4 is the highest.
IEC 61508 also spawned different specific standards for the different engineering sectors affected by the functional safety of electrical, electronic and programmable electronic systems (e.g. the petrochemical and nuclear industries). The machinery industry is one such sector, and the relevant reference standard is EN IEC 62061 (Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems), where only the first 3 Safety Integrity Levels are considered (i.e. up to SIL 3).

SIL	Probability of a dangerous failure per hour (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

So the integration of electronic and programmable systems in machinery cannot be planned and designed without taking into account the requirements established by both the EN IEC 62061 and EN ISO 13849-1 standards.
As both standards relate (for safety classification) to PFH_D, the Performance Level and the Safety Integrity Level can clearly be put in relation with one another.

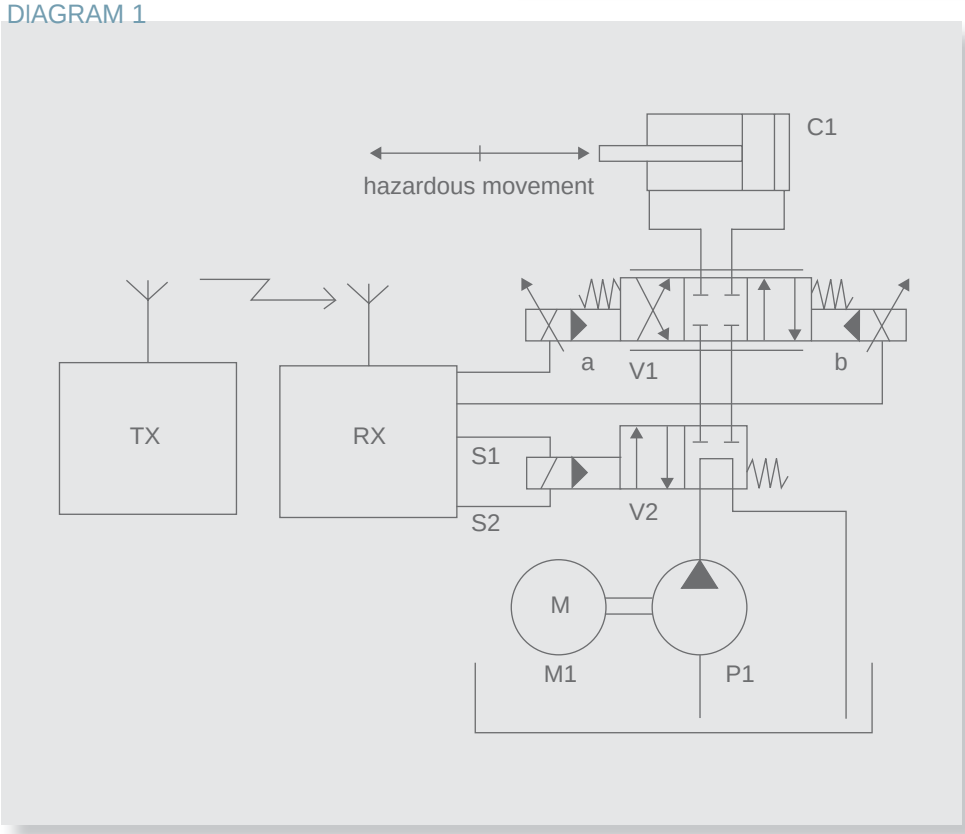
SIL (EN IEC 62061)	Probability of a dangerous failure per hour (PFH_D)	Performance level (EN ISO 13849-1)
-	$\geq 10^{-5}$ to $< 10^{-4}$	a
SIL1	3×10^{-6} to $< 10^{-5}$	b
SIL1	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	c
SIL2	$\geq 10^{-7}$ to $< 10^{-6}$	d
SIL3	$\geq 10^{-8}$ to $< 10^{-7}$	e

Example of remote control use

Let's assume that a safety remote control is to be used to control the movements of a hydraulic machine. The risk analysis of the machine identified the necessity of a safety function to prevent a hazardous movement when the operator did not intend it – i.e. the UMFS safety function. The required performance level for this function shall be PLd. The remote control is directly connected to the proportional valve V1 and the directional valve V2 as per diagram 1. The hydraulic circuit is powered by pump P1, driven by motor M1. In the idle state, the oil simply flows back to the reservoir. To enable movements, the remote control energises the directional valve V2. The proportional valve V1 then controls the direction and the speed of the movement by means of its two solenoids a and b. When a fault is detected, the remote control releases the safety valve V2 by means of one or both the outputs S1 / S2, stopping the oil flow and thus the hazardous movement. The UMFS function of the remote control can be used in systems up to PL d / SIL 2. It satisfies the requirements of category 3, has an $MTTF_d$ of 100 years and a diagnostic coverage of 91%. V2 is a safety component with a declared PFH_d = 2.5 x 10^{-8}. Provided that basic and well tried safety principles are applied, and all measures are in place against common-cause failures for both the electronic and hydraulic subsystems, we can estimate the overall PL as follows. From Annex K of EN ISO 13849–1 we find that the remote control has an PFH_d of 1.01 x 10^{-7}. The overall PFH_d is 2.5 x 10^{-8} + 1.01 x 10^{-7} = 1.26 x 10^{-7}. Again from Annex K of EN ISO 13849–1, this still corresponds to PL d.

Important note: this is only an explanatory example and should not be used as a reference for the integration of radio remote controls, for the implementation of safety functions in a particular machine, or the inference/calculation of safety related quantities.

DIAGRAM 1



A step forward along the path of safety knowledge

This document has covered many aspects of radio remote control theory, design, standardization, and certification. Armed with this knowledge, the reader should be in a better position to critically analyze various manufacturers' claims, and choose an appropriate radio remote control system for their application.

But let us end with a simple analogy: the safety features of a radio control system should be thought of as similar to those of a car – you may drive your car for years without needing the anti-lock brakes or the airbag. In fact, you may not even know whether the car you bought has such systems or not. They will only truly be appreciated on the day you need them.

Autec has been involved for decades in the subject of safety technology, as it started to voluntarily seek independent safety certifications for its products since the earliest comprehensive classifications were available (e.g. DIN V 19250: the first comprehensive standards related to safety in the machinery sector). Those were the only worldwide standards available at that time for applications relevant to the safety of machinery and Autec systems have been appropriately certified by TÜV since then. Now, after more than 20 years of experience in Functional Safety in wireless control, Autec Safety Remote Control continues to strive for the highest protection for people and plant.

The obvious companion to this product development was a continuous, intensive contribution to the evolution of safety technology - for example through the collaboration on the relevant tasks involved in the development of the pertinent international standards. Such collaboration brings with it the great advantage for a company that its own products can be adapted at a very early stage to changing requirements.

The outcome is that today Autec has incalculable experience with an extensive range of applications, which have been evaluated in accordance with SIL and PL.

List of authors:

Alessandro Bonan
R&D manager

Lorenzo Fraccaro
R&D senior engineer

Stefano Bianchin
Documentation & standards manager

Marc Cosgrove
Director
IndustryIQ, Australia

Antonio Silvestri
Product development and marketing director

Proven protection for your people