controldesign.com
control design
FOR MACHINE BUILDERS

Engineer's Guide to Machine Safety

SPONSORED BY
BECKHOFF

PutmanMedia®

TABLE OF CONTENTS

AD INDEX

Integrate automation and safety on one platform: TwinSAFE

www.beckhoff.us/twinsafe

TwinSAFE from Beckhoff: the universal safety system for everything from I/Os to drives.
The TwinSAFE I/Os for the EtherCAT Terminal system fully leverage the high performance offered by EtherCAT:

- Compact: Safety Logic in a 12 mm terminal block
- Powerful: up to 128 safety devices per Safety Logic
- Versatile: integrated function blocks for emergency stop, protective door, two-hand control
- Modular: standard and safety I/Os integrated in a single system
- Flexible: fieldbus-neutral communication, eliminates dedicated safety networks
- Certified: solution up to SIL 3 according to IEC 61508 and DIN EN ISO 13849 PL e


Integrated in all TwinSAFE components: Safety Logic

New Automation Technology **BECKHOFF**

A case for integrated safety systems

By Sree Swarna Gutta, I/O Product Manager, Beckhoff Automation

Machine safety technology has come a long way from the basic safety relays of the past. Today, machine designers have more advanced safety tools at their disposal, including highly integrated programmable safety solutions. The best offerings in this category include safety solutions that can leverage standard hardware, software and networking infrastructure to implement high levels of safety up to SIL 3 according to IEC 61508 and ISO 13849.

In practice, this means that users can install I/O with built-in safety logic right alongside standard I/O in the same segment, whether that's on a DIN rail or mounted on a machine. Other automation hardware comes with integrated safety functionality, such as servo drives and distributed drive systems. In terms of networking, the safety data can be transmitted over a standard industrial Ethernet or fieldbus using a "black channel" approach. With the proliferation of safety functionality to many more hardware types, machine builders can distribute more safety in more places while increasing performance and reducing overall equipment and cabling costs.

Q: How has the ever-expanding availability and use of programmable I/O impacted the spread of integrated safety and programmable safety logic?

SAFETY, INCORPORATED
Integrated safety systems, such as TwinSAFE, incorporate safety program engineering into the universal TwinCAT 3 automation platform used for PLC, motion control and more.

A: More people are using programmable safety I/O because of its many advantages, such as the wide range of form factors. These include standard DIN-rail-mountable terminals in the same segment as standard I/O and machine-mountable I/O modules, which reduce cabling to the control panel. Integrated safety devices have really made it easy for machine builders to offer more safety in more places.

Because of integrated safety's programmability in standard automation software, you can configure complicated logic inside a simple input device to make it safer for the people who are operating the machine. This enables machine builders to use safety as a competitive advantage and deliver many different safety features rather than just hardwiring an e-stop to certify the machine according to minimal safety requirements.

Programmable safety with safety I/O is easier to implement and less expensive – during commissioning and in the long term. It reduces the number of components and, as a result, the control cabinet footprint. Machines are safer, and they have less downtime because of easier restarts from a safe stop to a running state. These are major reasons why more machine builders are implementing integrated programmable safety, rather than the traditional approach.

Q: What are the benefits of programmable safety over older ways of implementing machine safety, such as safety relays?

A: Traditional safety relays are still the most common method, but they just cut the power to stop machines. Integrated programmable safety does much more. First, the safety is totally integrated into the machine control system, so you have a wealth of diagnostic information available. That's really important. When a machine stops, it's crucial to understand why. With simple safety relays, you have to open the control cabinet just to know which relay tripped and, usually, trace the wiring back to the field device.

With integrated safety logic, you have access to much more diagnostic data. EtherCAT and TwinSAFE, especially, provide information down to the terminal level to localize where a signal tripped and why.

Another challenge with safety relays is that specific relays only offer specific functionalities. There are separate devices for e-stops, door switches, safety mats and other devices. Adding another e-stop using traditional safety relays involves significant wiring effort. Therefore, the component list gets bigger and bigger when commissioning a safety system.

When using integrated safety, this functionality is mostly handled in software, so the hardware side is simpler. The safety I/O is either an input or an output, and what it does is up to the program. Changes require little to no rewiring, since safety logic updates take place in software. But the system retains the necessary redundancy using the TÜV-certified Safety over EtherCAT (FSoE) protocol.

Having access to the safety program in code benefits serial machine production. Transferring code from one machine to another machine is easy. All you need to do is wire the I/O as you normally would.

In addition, analog safety is available in programmable systems. Purely digital safety relays can only be on or off. Analog safety allows machines to constantly check the pressure or the temperature on a module, for example, and safely turn it off before it fails. That reduces machine downtime and helps with maintenance.

Q: What opportunities exist for technology convergence in safety systems?

A: When we speak about integrated safety, we're talking about one system. On the hardware side, standard I/O and certified safety I/O integrate easily into the same segment. On the software and programming side, Beckhoff provides TwinCAT 3 software as a universal engineering and runtime platform for all machine automation needs. It's all one system.

What advantages does it give? All the information is immediately accessible, including the diagnostic data. Because it's all in one system, you can put that diagnostic infor-

mation on an HMI alongside other machine performance stats. If something happens, operators or maintenance can easily troubleshoot it, for example. Also, machine builders talk a lot about IoT and remote monitoring. Uploading the safety data to the cloud, a database or HMI is possible and easier to accomplish in one system. For many years, TwinCAT has been driving the convergence of all of these industrial automation technologies.

Q: Some machines used in discrete manufacturing require intrinsically safe I/O hardware and explosion protection. What advice do you give to these OEMs?

A: When we talk about safety in a standard machine, people think about e-stops and safety switches. When we talk about intrinsic safety, people immediately think of the oil and gas industry. The perception is that intrinsically safe devices only belong in those industries, but that's not true. Intrinsic safety is used in other industries, such as processing sugar and flour, where there's significant dust, or cosmetics, alcohol and many others with vapors that are prone to explosion.

Typically, engineers use intrinsically safe barriers with standard I/Os, rather than intrinsically safe modules. This adds up to more parts, bigger control panels and higher costs. It's better to use an intrinsically safe module that slides right next to standard I/O or safety I/O. Intrinsically safe I/O terminals provide reliable, low-voltage communication directly to sensors and devices in hazardous areas, even in Zone 1 or Zone 0 where dust or other particles could act as an ignition source. They simplify safety architectures and are equally important to machine builder OEMs.

Q: What technologies or best practices are being used to ensure the security of safety data?

A: Many people worry about whether their data is secure and what might happen if it's not. With EtherCAT, the functional principles make data automatically secure. EtherCAT establishes secure networking because it's set up without any IP addresses, and the EtherCAT master knows exactly what kind of data to expect from the slave devices. Through EtherCAT's default mode of operating, your data is already secure.

For safety data, it's actually more protected. FSoE uses a "black channel" approach, so standard devices can't read the safety data when it passes through. Only the safety terminals recognize the data. They read and process that data, then send commands in response. Using TwinSAFE, customers don't have to worry about data security, especially when using EtherCAT.

For more information about Beckhoff Automation integrated safety, please visit www.beckhoff.com/twinsafe.

What is safety in industrial automation?

By Jeremy Pollard, CET

I remember back in the good old days that an e-stop wired into a master control relay (MCR) was the only way to go to take power away from the controlled outputs in an automated process. There were always 200 devices in series—an exaggeration, maybe—so that any one of these device could take the system down.

HAVE FUN TROUBLESHOOTING THAT MESS.

Anti-tiedown pushbuttons on presses were all the rage until someone decided to see if they could tie wrap one of the buttons in the closed position and see if the press would still work. Imagine their surprise when it did. Pushbuttons were replaced by finger sensing, so that the operator had to use both hands for safety.

Therein lies the rub. The safety is for what or whom—the operator or the press? Well, it's the operator.

Modern-day safety systems have morphed into something unrecognizable from the early days of simply protecting the operator. Safety devices, controllers and networks are all part of the puzzle that falls under the safety umbrella. This umbrella suggests that there is protection for all things automation, and it can do it with the same flexibility and software that we have come to take for granted in standard control systems.

Today there are different safety integrity levels (SILs). As per "A Guide to the Automation Body of Knowledge" from ISA, a SIL is not directly a measure of process risk, but rather a measure of the safety system performance of a single safety instrumented function (SIF) required to control the individual hazardous event down to an acceptable level.

Imagine an e-stop button that is required to stop a pallet wrapper in its tracks when hit. The reasons for this need can vary and need to be defined by operations. Remember it is an emergency-stop function.

Let's say it is wrapping tires, and the top course of tires shifts on the first wrap and needs to be repositioned. A normal stop function may be OK for this. However should someone open a gate that has not been identified as part of the safety system performance review, and approaches the wrapper, the wrapper has to stop 100%.

With a normal stop button, the contact block may have fallen off, and pressing the button does nothing. I have seen that happen.

With an e-stop, however, it has to work. Back to the old MCR system, an e-stop button was a mushroom-head button, red in color, with a single NC contact block—no different from a normal stop button, and it can suffer from the same issues.

In today's 100% world, the e-stop now has two contact blocks and is normally wired into a safety relay or controller. This system detects a contact failure and wiring malfunctions. Also, when this e-stop is hit, it stays locked in, and the user has to twist it to release—all positive actions.

Some safety relays cannot tell you which e-stop has been pressed, but I would submit that a safety relay should only be used in a closed system, such as a small machine skid. For larger processes and processes that are distributed, the risk management system has to adjust.

The safety controller is software-driven and can report to the control system when the e-stop has been pressed. A safety network can be employed to connect multiple safety controllers together to create a homogenized system to protect all aspects of the operation.

Safety-device application determines the level of SIL. Level 1 is the old MCR system where the systems employ standard control elements.

Level 2 is entry level for a true safety system. Redundancy is the word of the day here. You could use a standard e-stop with two contact blocks with two MCR relays, and you would create a better safety system. But you would normally want to use fail-safe devices with a safety-rated relay system.

Imagine an e-stop button that is required to stop a pallet wrapper in its tracks when hit.

Level 3 is fully fault-tolerant. This is the level in which true safety-rated devices, relays and controllers would be used, along with the connectivity component where needed.

One application I was involved in was to detect a person who has entered an area in between moving carts. We used a Pilz eye-in-the-sky device, which detected movement within a configurable area.

There were two issues. The first was personnel safety. The company didn't want to have anyone hurt from being in the wrong place. Secondly, a cart could twist and get trapped causing a pileup, which could harm the overall process.

There were times where an operator had to be in that area to perform his duties, which would shut the process down, which could not be disabled. The need to run the process became more important than the safety aspect, so it came down to training. Being safe means different things to different people and to different processes. Be sure you have a proper safety design and that it is fail-safe.

The future depends on it.

Intrinsic safety comes with requirements

How to design a control circuit for use while keeping barriers in mind

By Dave Perkon, technical editor

Once an area is classified as hazardous with a potentially explosive atmosphere, many steps must be taken to eliminate ignition sources. When looking at a fire triangle with oxygen, fuel and source of ignition, two of the three are often present in these areas. It's the designer's responsibility to eliminate all sources of ignition, and that includes limiting both electrical and thermal energy to a level below what could ignite the hazards present. Depending on the area classification, even the tools used for installation must not cause sparks and are therefore made with aluminum or similar material.

Intrinsic safety (IS) barriers are devices designed to limit the current and voltage that can cause sparks in a device's power and signal conductors.

When IS barriers are used in hazardous locations, some of the basics that must be considered beyond area classification are methods to eliminate hazards; certification of device or apparatus; and design and wiring methods.

It is important to point out that installing a control system in a hazardous area is not a one-man show. The facility is required by law to properly classify any area that may contain an explosive atmosphere. The control-system designer must check with plant engineering, operations or safety personnel and determine the area classification. A facility that appears to be nonhazardous may have several hazardous areas, including explosive fumes or powders, so always check.

Take a close look at your standard intrinsic safety system design, and, with a critical eye, check the components to ensure they are suitable for use in the hazardous area.

When specifying IS barriers or any hazardous area control system components, work closely with the vendors and manufacturers. They are great sources of information and should be leveraged, along with training, if you are new to designing control systems for use in hazardous areas. Even if you are an expert, the standards and requirements change. Take a close look at your standard intrinsic safety system design, and, with a critical eye, check the components to ensure they are suitable for use in the hazardous area.

There are many applications where a spark, heat or small explosion ignites an explosive, such as a gas grill spark igniter, a hot bridge wire setting off an exothermic chemical reaction (gas generation) in an airbag initiator and a primer in a cartridge initiating propellant combustion.

On the other hand, IS devices do just the opposite. An IS barrier limits the sparks and heat in electrical devices that can cause explosions, under normal or abnormal conditions, to a level incapable of causing ignition of a hazardous atmosphere. They work well protecting low-power devices such as instruments, sensors, LEDs and solenoids.

Other protection from explosion methods includes explosion-proof equipment or enclosures and purging or pressurization of the device or enclosure. These methods are often used in combination with IS barriers as the barriers are not suitable for all applications. For example, an IS barrier typically limits voltage and current, but safe energy levels vary depending on the area classification. In some areas, such as with hydrogen gas, a circuit with about 24 V and 150 mA may provide enough energy to create a spark large enough to ignite the mixture of gas and oxygen.

The National Electric Code Article 504 discusses intrinsic safety. Not only must the IS barrier be certified for use per the hazardous location class and division, it must be certified by a local, third-party agency such as UL and the Canadian Standards Association (CSA Group). The IS barrier must meet requirements and standards based on the geographical location of the plant. Equip-

Installing a control system in a hazardous area is not a one-man show.

ment installed in Europe often must have certifications for the specific country.

Zener diode barriers are one way to implement intrinsic safety. This barrier type is connected to a safety earth ground which can cause electrical noise that may cause problems, especially with analog circuits. Isolated IS barriers are also available and provide galvanic isolation, which eliminates the dedicated safety ground. These galvanic barriers typically require a separate power supply, but only one is needed to power all barriers.

Zener barriers are a simple cost-effective method to connect discrete sensors and solenoids. The isolation provided by galvanic barriers work well with transmitters, thermocouples and other analog circuits.

The field devices connected to intrinsic safety barriers must be FM approved for that use along with the class, division or zone, group and temperature ratings of the area or must be a simple device or apparatus that does not store or generate more than 1.5 V, 0.1 A or 25 mW such as simple switches, sensors, LEDs or thermocouples.

The installation and wiring of IS barriers must carefully match the design drawings. A standard industrial enclosure can be used with intrinsic safety devices and apparatuses, and it does not need to be sealed. However, a conduit seal must be used between hazardous and nonhazardous enclosures to isolate the hazardous atmosphere from the safe area.

The same wiring methods can be used for intrinsically safe and non-intrinsically safe conductors, but they must be kept physically separate using 2-inch air space, conduit or partition. The IS wiring must also be clearly labeled to not confuse it with safe area wiring, and light-blue wire is often used for IS circuits to highlight its purpose.

There are many requirements for application of intrinsic safety barriers. Be sure to understand the hazards and how to eliminate along with certifications, design and wiring requirements. There are many beyond the few basics noted here.

Crashing and smoking automation

A simple mistake is all it takes to remove machine tooling and control hardware from a system in spectacular fashion

By Dave Perkon, technical editor

As I read a news story on how India lost and found its Vikram Lander on the moon, I couldn't help thinking about some of the spectacular automation crashes and failures I've witnessed. Fortunately for India, it was not a total loss; its Chandrayaan-2 orbiter and its eight scientific instruments will likely be orbiting the moon and providing valuable information for years.

Over my career and like India's moon program, I have definitely lost a lander craft or two, but the main ship still functioned—after the bent parts were repaired. However, complete system failures do occur during machine startup or maintenance activities. Fortunately, I was just a spectator to some loud, flaming and truly destructive failure events.

A couple decades ago, NASA's Mars Climate Orbiter crashed into Mars because the engineers were talking to the craft in English engineering units when it should have been speaking metric engineering units. Feet-per-second of thrust is quite different than Newtons-per-second of thrust, causing the adjustment to be off by a factor of 4.45. NASA repeatedly sent the wrong information to correct the craft's motion and maybe didn't check for a proper response. Unfortunately, it often only takes one incorrect variable, closed contact or misplaced wire to crash an automated machine.

It is important to predict and find those single-point failures before your automation makes the problem catastrophically obvious.

It's hard to believe that engineers cannot check that the engineering units are correct in a $124 million spacecraft, but it happens. It is also hard to believe that a programmer does not include contacts (interlocks) in a drive-enable circuit that ensures the tooling is clear, but it's not that simple.

Some will say it is hard to test something flying through space 100 million miles away, but sending a command to test its response is about as basic as it gets, especially if it's off by a factor of 4.45. And it has to be done in the correct order. Here's an example of how not to do it.

Years ago, I was working at a machine builder as an integrator programming and starting up a machine, and my competition comes in to work on the large dial table next to me. The first thing he does is dry-cycle the eight stations on the dial table. Shortly after starting that, within an hour of arriving, the dial table unexpectedly indexes and damages every station on the machine—massive damage, everything was bent.

From my spectator position, I thought it was great, and the programmer's failure was obvious. He didn't check the critical machine safety interlocks. In this case, the interlock all station tooling is clear of the dial. He should also have programmed an interlock that while the dial is indexing the station tooling must stay clear or the dial must stop.

While the PLC program checks many sensors to ensure the tooling is clear of a potentially damaging motion, often only one "clear" interlock contact is used in series with an output coil to inhibit a dangerous and powerful machine motion.

Just one wrong program bit and a machine motion can literally peel the tooling off a machine, which is much more common than crashing a spacecraft into a planet or moon. The same is true for a single relay contact or a misplaced wire.

The loudest and most destructive machine automation crash I've ever seen was at an appliance manufacturing plant. An integrator was starting up a multi-station, 100-foot-long walking-beam transfer that moved refrigerators through a final assembly and test system. The technician manu-

ally actuated a relay, and well over a million dollars of automated equipment was ripped from the mounts, including 10 large free-standing control panels.

The technician barely escaped with his life, but the resulting damage to the equipment was similar to a multi-car pileup on the freeway; and it certainly sounded like it.

I saw a similar thing happen in an automotive body shop. The walking-beam transfer cycled when about 30 robots were working on several vehicles. While not as catastrophic as the appliance line, blow torches were needed to cut up several vehicle frames to clear the resulting crash.

So, how do you keep that from happening? It's easy; carefully perform a well-thought-out test procedure, and use a safety relay in a Category 3, or similar, control reliable circuit. Just as a safety circuit can be used to safely stop machine motion, it can be used to check that tooling is clear before motion is started. While they are two physically separate functions and circuits, the technology is the same.

It is important to predict and find those single-point failures before your automation makes the problem catastrophically obvious. Good design practices and a bit of failure analysis will help. For example, is it a problem to have 120 Vac and 24 Vdc directly adjacent to each other?

Some will say no; electrical noise could be a problem. That's true, but another problem is incorrect wiring. Did I tell you about the integrator who accidentally connected 120 Vac to a 24 Vdc circuit and burned up 40 reed switches on a piece of test equipment? It started to burn as I was turning breakers on and testing voltages, and then a fire extinguisher became involved. As a reminder of this smoking automation, the shop smelled like an electrical fire for the better part of a week.

As NASA and others know, you cannot always get it right 100% of the time, but that is the goal. Be careful with those units or measure, bits and wiring.

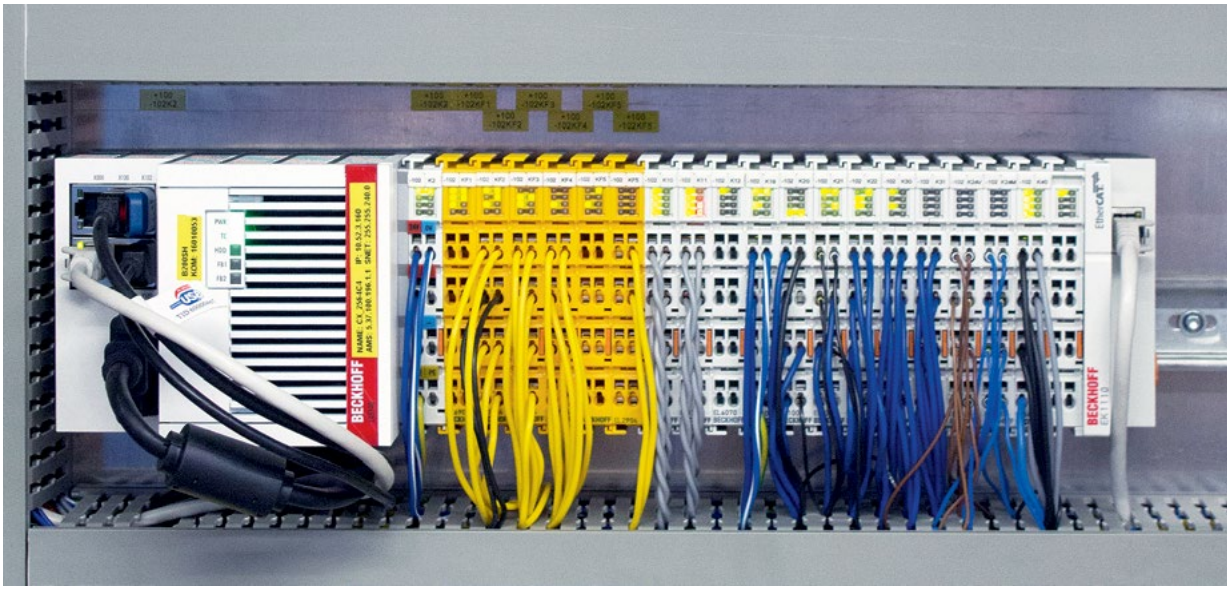
The Convergence of Safety and Non-Safety Increases Scalability, Flexibility

Integrating safety systems into a machine's standard control platform simplifies operation, increases diagnostic capabilities and creates safer work environments

By Sree Swarna Gutta, Beckhoff Automation

Whether combining AT and IT or IT and OT, the convergence of previously disparate technologies continues to be an important topic because of the benefits to engineers, OEMs and end users. However, the integration of safety with non-safety technology is another convergence that deserves serious consideration. As with IT and OT, the combination of safety and non-safety into one system enables increased flexibility and scalability, better data acquisition across systems and more opportunities for customization. Most importantly, it creates a safer work environment for operators and plant personnel by accommodating more safety technology in more places.

Programmable safety devices in an I/O form factor that are also integrated into the main machine control architecture make this convergence possible. These I/O terminals feature integrated safety logic and communicate with the PC-based machine controller, whether they connect through a shared backplane or Ethernet cable. EtherCAT industrial Ethernet technology creates other opportunities for technology convergence in safety systems, such as built-in diagnostics and support for multiple fieldbuses. This approach is certainly a departure from previous architectures, in which safety and non-safety systems purposely remained separate in silos. The converging technologies enable machines to maintain safety integrity level (SIL) standards while offering further customization benefits.



Unlike traditional safety systems that remained separate from non-safety components, integrated options can be located on the same DIN rail and communicate with the PC-based controller and other I/O via a shared backplane.

To understand how this convergence works and why it is advantageous, it is important to first carefully consider the different levels of safety technology. These range from basic safety with simple relays to stand-alone safety controllers and up to distributed I/O terminals with programmable safety logic.

1. BASIC SAFETY DEVICES

The traditional basic safety approach keeps safety systems entirely separate from the machine control platform. These safety devices include relays and switches that simply cut power to machines or modules if triggered. Although they are relatively low cost and require no programming effort, they must be hardwired directly to each module and every other safety device to ensure the entire machine or line stops operation when one device is tripped. Installation and wiring of safety relays is time- and labor-intensive, especially on larger machines.

Safety relays and other basic devices are usually not configurable. Because they possess no network connectivity, they cannot communicate back to the PLC or provide performance data or diagnostics beyond what their LED lights show. This was the only industrial safety solution for many years and met the minimum requirements for protecting operators and equipment. However, in the age of the Smart Factory and Industrie 4.0, basic safety has not kept pace with industry advances. It is inefficient to implement because it requires greater commissioning efforts and ultimately provides low-tech safeguards for workers.

Integrated-safety-2: Some safe I/O terminals, including all new TwinSAFE modules, incorporate safety logic at the device level rather than requiring a separate safety PLC.

2. STAND-ALONE SAFETY CONTROLLERS

Stand-alone safety controllers are expandable and offer some programmable logic, but as a result, these systems require additional engineering efforts. This method supports the ability to network safety devices and provides greater diagnostics for troubleshooting, but it does not truly enable the convergence of safety and non-safety systems.

Like basic safety technology, safety controllers remain physically separate from the machine controller. Although both contain logic, the safety controller and PLC only support asynchronous communication, which means crucial data from the safety system are not available for analysis. In addition, the safety device uses different software than the machine control logic, and the required training and maintenance for multiple software packages slows commissioning and troubleshooting.

3. INTEGRATED SAFETY WITH PROGRAMMABLE I/OS

Greater technology convergence is happening through integrated safety systems with programmable safe I/O terminals. The safety terminals are differentiated on the outside by their solid yellow exteriors, and on the inside, they possess redundant circuits and microcontrollers to maximize reliability and meet IEC 61508 and DIN EN ISO 13849-1 safety standards. These devices are installed directly into a standard

I/O segment alongside non-safe terminals and can communicate over modern industrial Ethernet systems like EtherCAT. Integrated safety can extend beyond I/O terminals to implement safety logic in components in the field, such as Servo Drives and servomotors with built-in Safe Torque Off (STO) and Safe Stop 1 (SS1) functionality. In any case, this method uses the same engineering environment as the machine control and provides maximum flexibility for distributed safety networks.

Programmable I/O modules can also support single-channel safety. With the necessary firmware for safe communication protocols, these modules allow engineers to set acceptable condition parameters for many different applications, such as temperature monitoring, level sensing, speed testing and pressure monitoring. This capability provides advantages for engineers in process industries, among other fields.

Integrated safety can extend beyond I/O terminals and implement safety logic directly in Servo Drives and other components in the field.

These safety terminals possess a single yellow stripe on their exteriors to differentiate the single-channel analog technology from standard digital safety terminals in an I/O segment. Most importantly, the specialized single-channel terminals enable the use of standard I/O for safety tasks.

Integrated safety is essential in today's manufacturing environments with greater use of robotics, complex motion control equipment and autonomous vehicles. Modern plants require both simple safety devices, such as e-stop buttons, and more sophisticated light curtains, safety switching mats and two-handed controllers, among others. PC-based automation software with standard safety function blocks allows engineers to create the necessary programs to protect workers and equipment in these work environments. During operation, the PC-based machine controller and safety controllers are able to monitor each other.

Increased performance data and diagnostics capabilities are available as a result of this convergence, and unlike with standalone safety controllers, the information can be easily displayed on the HMI because the safety system is connected to the PLC. More programming is necessary than with basic safety, but integrated systems simplify commissioning. They eliminate the complications caused by multiple programming environments, additional networks and the necessity to hardwire each device to all others. For EtherCAT-based devices, communication takes place using the TÜV-certified Safety over EtherCAT (FSoE) protocol.

SECURE COMMUNICATION OF SAFETY DATA

FSoE – sometimes called Fail Safe over EtherCAT – transmits safety data over a plant's existing network via a "black channel." This secure channel within the network increments a Cyclic Redundancy Check (CRC) for every two bytes of safety data to ensure they are secure and error-free. The functional principles of EtherCAT enable the transmission of safety and non-safety data without limitations on transfer speed and cycle time. Designed for high-speed communications, EtherCAT checks the safety devices in real-time and immediately halts operation when tripped. In addition, built-in diagnostics help engineers troubleshoot physical issues, such as faults with cables, connectors or I/O terminals.

Supported by the EtherCAT Technology Group, FSoE is fieldbus-neutral and works over 100 Mbit/s EtherCAT, but it can also integrate with many other industrial Ethernet networks or fieldbuses. If plants use DeviceNet, PROFIBUS, CANopen, EtherNet/IP and PROFINET networks, implementing integrated safety systems with FSoE simply

requires the addition of appropriate EtherCAT I/Os and gateway devices.

FSoE is not only certified by TÜV; it also meets all requirements for IEC 61508 and DIN EN ISO 13849-1. These safety designations remain unchanged whether communication occurs via legacy fieldbus, industrial Ethernet or over wireless networks. In addition, FSoE and integrated safety I/O unlock possibilities for increased customization.

CONVERGING TECHNOLOGIES ENABLE CUSTOMIZATION

A key benefit of integrated safety is the ability to customize and test how safety systems function through software. If a customer has a modular machine, the OEM or integrator can disable a certain module in software, rather than the traditional route of redesigning and reprogramming the machine's safety system. The previous method involved changing I/O, re-engineering components or creating crude workarounds, such as "jogging" wires to bypass unnecessary parts of the safety system. With PC-based automation software, these adjustments can be made quickly by adding or removing modules or groups.

Despite these advantages, some companies have been slow to adopt integrated safety technology due to concerns about combining safety and non-safety on one platform. However, integrated safety is reliable and preferable to basic safety devices and stand-alone safety controllers. If the safety PLC and machine controller are in the same environment, then they know what the other is doing at all times and can communicate more effectively. With greater flexibility and faster installation, it is possible to design machines and plants to have more safety technology than ever before. As a result, implementing integrated safety with programmable I/O modules is by far the safest choice.

Sree Swarna Gutta, I/O product manager,

Beckhoff Automation.

For more information:

www.beckhoff.com/twinsafe

Are purged enclosures and intrinsically safe barriers necessary?

How do I reduce wiring between hazardous and nonhazardous areas?

By Mike Bacidore

A Control Design reader writes: Our facility processes propellants and explosives with many areas classified as hazardous—Class II, Div. 1. Normally, we install the controller and I/O in a suitably purged enclosure and use intrinsically safe barriers for most field device connections. I'm not sure this is the best solution on a large canister-filling project, where there are nearly 500 I/O points on the hazardous-area automation. Because of the large installation and space limitations in the hazardous area, the main control panel will need to be located outside the hazardous area. How do I keep from running more than 500 wires, about 70 ft each, between hazardous and nonhazardous areas? What are my options?

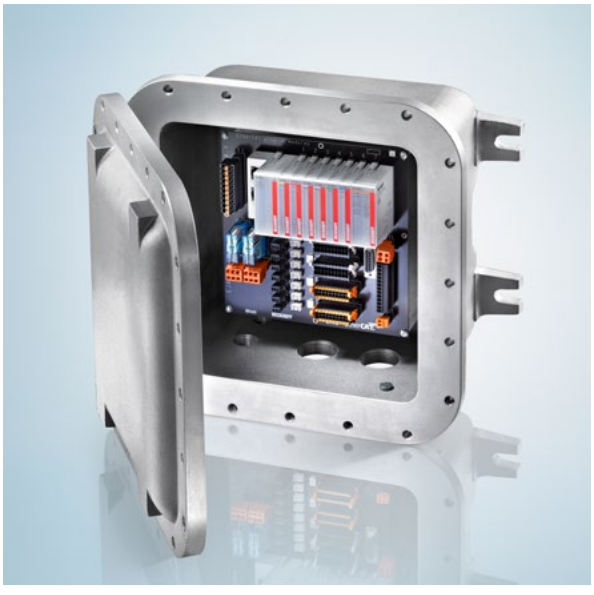
ANSWERS

REDUCE WIRE RUNS

This method—running a cable from each I/O point in the control cabinet through intrinsically safe barriers to the sensor or other device in the hazardous area—is certainly the way engineers have dealt with intrinsic safety for years. Fortunately, there are new options to reduce the number of lengthy wire runs, which can be very cost-intensive in terms of expense and installation effort. New methods and technologies could reduce the effort down to one cable rather than 500 in some instances.

BRIDGE THE GAP
Figure 1: Terminals rated for Zone 2/22 bridge the gap between intrinsically safe sensors and actuators in Zone 0/20 and cloud-connected controllers.

First, consider reducing the number of cables and the size of the control cabinet by locating intrinsically safe components in the production area. Intrinsically safe I/O terminals can be installed in Zone 2/22 and connect with intrinsically safe sensors and actuators in Zone 0/20 (Figure 1). In process environments, IP20-rated I/O terminals can be mounted on DIN rail in separate enclosures. A single cable can connect each segment of intrinsically safe I/O terminals to the controller, reducing the required cables and intrinsically safe barriers.



SAVE THE SPACE
Figure 2: Space-saving, pluggable terminals can be used in Zone 1/21 when located inside explosion-proof Ex d enclosures.

Second, explore the benefits of pluggable, circuit board-mounted I/O modules (Figure 2). These can be placed in Zone 1/21 when located inside an explosion-proof Ex d housing. As a result, only one Ethernet cable would need to run from the control panel to the I/O enclosure, allowing much shorter cable runs from the I/O to the sensors without requiring multiple barriers. Because this requires the design of a custom circuit board to plug the I/O terminals into, it might not be the best solution for a one-off project. However, it is an excellent option when complet-

ing multiple machine/equipment builds or installations in this facility or others.

The EtherCAT industrial Ethernet protocol provides benefits for both of these solutions. Because EtherCAT can support more than 65,000 devices on one network with real-time performance, the relatively small number of sensors in this instance will not cause problems. In addition, EtherCAT is an inherently open solution, easily integrating with multiple fieldbus and network protocols, such as HART, Profibus, DeviceNet, CANopen or EtherNet/IP. Once data from all these protocols are gathered from all connected sources, they can be transmitted over a single Ethernet cable once it reaches an EtherCAT I/O segment. This should eliminate the bulk of long cable runs into the Class II, Div. 1 environment without requiring changes in the existing machine controller or network architecture.

SREE SWARNA GUTTA

I/O product manager / Beckhoff Automation / www.beckhoff.com

TWO OPTIONS

Because the reader believes he or she is unable to install any remote I/O, due to space constraints in the hazardous area, the best solution at this point is using junction boxes to consolidate the intrinsically safe (IS) wiring in the hazardous area back to the PLC in the unclassified area. Two options are described below.

Option 1: I/O possibilities

If there is some space to install remote I/O, then Type X pressurization enclosure—although generally done with Class I rather than Class II, it makes Div. 1 areas essentially non-hazardous—is certainly an option (Figure 3). The reader could put the PLC with IS barriers in the Type X pressurized enclosure, or I/O in the Type X pressurized enclosure and run Profibus DP back to the PLC. Then put IS process wiring receptacles, or IS glands, on the Type X pressurized enclosure because they carry FM approval for intrinsically safe, and by definition IS wiring only requires Div. 2 seals.

Under NFPA 496 Standard for Purged and Pressurized Enclosures for Electrical Equipment, 2008 Ed., Section 4.2.3, all Div. 1 seals not part of the pressurized sys-

ELBOW ROOM

Figure 3: If there is some space to install remote I/O, then Type X pressurization enclosure—although generally done with Class I rather than Class II, it makes Div. 1 areas essentially non-hazardous—is certainly an option.

It’s possible to consolidate the 500 cables down to two, approximately a 99% reduction in cabling from the PLC in the unclassified area to the hazardous area.

tem need to be explosion-proof, although I would make the case for IS wiring since by definition it is energy limited and our EX receptacles do not allow the mitigation of gas, and, as dust particles are larger than gas, they would never pass dust either.

Our largest backplane I/O system from allows for 192 intrinsically safe I/O discrete connections or 96 analog connections, which would mean, for 500 I/O, the reader would need at a minimum three racks. In addition to the racks, the reader would need to purchase all the I/O cards but would not have to buy IS barriers and install them in the pressurized enclosure, so is saving money and space.

Again, three or more racks may or may not be possible depending on the space constraints of the hazardous area. Our I/O system comes with a redundant Profibus DP communication card that will allow for both a smaller footprint in the hazardous area by not requiring IS barriers, and it’s possible to consolidate the 500 cables down to two, approximately a 99% reduction in cabling from the PLC in the unclassified area to the hazardous area.

Option 2: Junction boxes with homerun cables

If there is no space in the hazardous area for multiple I/O system racks, then, to reduce the amount of cables from the hazardous to unclassified area, the reader would simply install the PLC with IS barriers in the nonhazardous area, then install process wiring junction boxes in the hazardous area and then run homerun cables back to the unclassified area.

With eight-port junction boxes, it’s possible to consolidate the 500 cables down to 63 cables, approximately an 87% reduction in cabling. The only drawback is the reader would have to purchase field wireables or overmolded cables for all the junction boxes and/or field devices.

JOHN VU

product engineer for interfaces, fieldbus technology division / Turck / www.turck.com

MAKE THE CONNECTION

One thing to consider before you abandon the idea of 500 I/O points worth of intrinsically safe (IS) wiring is the advantages of running IS connections into the hazardous area. It greatly eases the wiring since there are several wiring and cabling methods permitted for IS connections into a Class II, Div. 1 area. Without IS, any wiring you take into the hazardous area will be limited. As you likely know, this usually means threaded metal conduit, metal-clad cable or similar types of approved wiring methods for non-IS signals in Class II, Div. 1.

In keeping with the all-IS approach, you may be able to reduce the number of wires that need to be run for your installation and still maintain IS for all of your signals. There are IS barriers that support connecting to two-contact switch type or NAMUR type sensors over a single pair of wires, cutting the needed wire run back to the safe area in half. This method does come with some switching-speed limitations but can be an option to reduce wire count.

A second method that could be considered to maintain all IS signals but reduce the number of wires is to power several 4-20 mA devices with a single IS barrier and run them in complete digital mode via HART signals. There would be some obvious limitations on the number of devices and what could be done with this method, but it is an option to consider.

Another option to reduce the wire count from the safe area to the hazardous area would be to use a bus system like fieldbus or Profibus to communicate to a number of hubs, each hub having a number of spurs or I/O connection points. Each hub used to distribute I/O around the hazardous area could have IS connections out to IS devices for the I/O point data, easing this part of the wiring install. So the advantage is a reduced number of wires that would need to be run a long distance, and the connections to each I/O point would be IS. The disadvantage is that it introduces the Class II, Div. 1 installation and wiring methods for hubs and for the bus cabling.

Depending on the nature of the I/O data, a wireless network for some number of the data points could be deployed, and direct IS wiring for the rest of the points could be done. WirelessHART or other wireless protocols can be used in hazardous areas to allow for communication back to a control system. This could eliminate some the IS wiring that would be needed and also limit the amount of Class II, Div. 1 wiring that would be needed. There may still be a need to deal with power to the devices, so some sort of power bus installation may still be needed to Class II, Div. 1 requirements, or batteries to power the device and the radio attached, but the overall number of wires would be reduced.

A few smaller control cabinets could be in the hazardous area with protection by pressurization.

Finally, you could also consider breaking up the single large control cabinet. If there is room, a few smaller control cabinets could be in the hazardous area with protection by pressurization, and IS I/O from the pressurized enclosures could be used. This might have been passed over based on the assumption that a pressurization control system would be needed at each enclosure. However, this would not necessarily be required. There are methods to connect a number of enclosures together and treat them as a single enclosure, as far as pressurization monitoring and control is concerned. There are also pressurization control systems that can monitor two separate enclosures at the same time. So, it may be possible to have two or four smaller enclosures placed around the hazardous area controlling your process and have them connected such that a single pressurization control system could monitor them all.

RYAN BROWNLEE

compliance and technology consultant, product management team / Pepperl+Fuchs / www.pepperl-fuchs.us

REMOTE I/O

A wireless approach would seem to be the best possible solution approach, but an additional option could be to use remote I/O. You would collect the data in the XP area into the remote I/O hardware. Transmit it via fiberoptic, if necessary, or cable to the safe area where a PLC can process the data. This would eliminate the 35,000 feet of cabling.

TED COWIE

vice president, sales, safety and industrial products / Motion Industries / www.motionindustries.com

DISTRIBUTE THE I/O

One option is an intrinsically safe distributed I/O platform. One of the benefits of a distributed I/O solution is that it allows mounting of I/O away from the main control panel and nearer to field devices and instruments. The I/O modules should carry a Zone 2/Class I, Div. 2 approval and be suitable for Zone 2/Class I, Div. 2 gas hazardous area mounting in an appropriate enclosure. For dust hazardous area mounting (Zone

22/Class II, Div. 2), do note that additional special cabinet specifications must be met. As intrinsically safe applications vary by the required level of safety and security aspects, I recommend discussing your system layout and architecture with your vendor.

ZIN MAY THANT

senior product specialist / Rockwell Automation / www.rockwellautomation.com

WHAT IS NONHAZARDOUS?

To be a bit clearer on what is meant by nonhazardous area, I'll add in the reference to a Div. 2 area. To me, nonhazardous means safe area, but I've heard people refer to a Div. 2 area as nonhazardous.

I am not aware of any wiring reducing options for runs from the Div. 1 area to the Div. 2 area. If looking to reduce the length of the wiring runs from the Div. 1 area to the safe area, then there are options by ending your wiring runs in the Div 2 area. The two options I can think of are using remote intrinsic safety I/O or using an intrinsic safety fieldbus system. With both of these technologies, there are manufacturers that make Div. 2-approved devices that offer network cabling interfaces to take your data to the safe area. My first choice would be the remote intrinsic safety I/O because it's the most flexible system when it comes to input and output options.

DEREK SACKETT

senior product marketing specialist for interface analog and enterface Ex / Phoenix Contact USA / www.phoenixcontact.com

ONE CABLE

First of all, I myself am not an expert in hazardous locations. With that, I do represent some product that can be placed in Class 1 Div 2 locations. Have you looked into remote I/O options? You will still need to place the remote I/O block in safe areas, but, instead of running the 500 wires 70 ft, you will be able to run a single network cable such as EtherCAT the 70ft and then break out your 500 I/O points from the remote I/O block.

CLARK KROMENAKER,

product manager—HMI, IPC, controllers, I/O, software / Omron / www.omron247.com