controldesign.com

control design

Sensors, Vision & Machine Safety

PutmanMedia®

TABLE OF CONTENTS

AD INDEX

Balluff provides the tools you need across industries **www.balluff.com**

A FULL RANGE OF SENSORS FOR A FULL RANGE OF TASKS

Intrinsically safe devices vs. systems

Guidelines from OSHA and NEC to keep your people, machines and processes safe

By Rick Rice

One of the most important design criteria, if not the most important, is the safe operation of your machine or process.

Safety can be broken down into two focal points:

1. safe for the humans that interact with the equipment
2. safe for the components of the machine or process.

The primary focus must always be the safety of the individuals who interact with the equipment. Effective physical guarding combined with a reasonable and efficient way of interrupting the function of the equipment and restoring use thereafter are very important considerations in the design of a control system.

Traditionally, a control system would start with a master control relay to, as the name suggests, control the voltage that is supplied to the motive parts of the control system. The basic circuit would involve a normally open start button, a normally closed stop button and a tie-in contact to keep the master control relay engaged unless the stop button is pressed. To make the circuit safer, the stop button would be a maintained-contact button by using a mushroom button that must be pulled back out to re-engage the contacts.

Control systems became safer with the addition of an e-stop button—mushroom-shaped and maintained contacts. These buttons could also be shrouded in such a manner so that a padlock could be applied to the shroud, preventing the e-stop button from being reset, or pulled out. Separate from the cycle stop button, an e-stop button could be strategically located around the machine or process area to provide a quick, easy means of immediately stopping the controls, in case of emergency.

Safety circuits and hardware have evolved greatly since the early control systems. Terms such as “dual-channel” and “dual-redundancy” are commonplace today. These terms present the logical progression that, if one circuit or device is safe, then two circuits or devices is safer.

Safety systems have advanced dramatically over the past few years, in particular, to the point where the driven devices—variable-frequency and servo drives, for example—have safety circuits embedded in the design to prevent power on the input side from getting to the output side of the device.

Protection of the devices in a control circuit is the secondary focus of safety circuits. Early control-system designs incorporated devices such as thermal overloads or thermistors in the master control relay circuit so that a product jam or shorting motor winding would immediately drop the control circuit.

As technology has advanced, many control devices have built-in protection circuits that immediately stop the device and provide a relay contact to the main control system to notify of a device failure. Motor controllers are a good example of devices that incorporate this method of protection.

By protecting the controlled devices, the human element is also protected by reducing the possibility of a broken component challenging the integrity of the physical guarding. Fractions of a second can make all the difference between a belt part and a broken one, so protection in a variable-frequency drive or servo drive instead of a PLC or PAC—milliseconds later—can literally save a life.

Everything we have talked about so far deals with safety of the control circuit or controlled devices, but what if the environment itself is the unsafe part?

In petrochemical and processing, the product or by-product of the process can contain solids, liquids or gases that have low flashpoints. In the food-packaging industry, some of the most common of household baking items, such as corn starch or baking soda, are highly explosive if exposed to a spark.

This might seem like an obvious statement but control systems use electricity. Even if it is 24 Vdc, it is still enough to create a spark sufficient enough to ignite a combustible material. The approach to the design of control devices to be used in a hazardous environment so that the available energy, electrical and thermal, is too low to cause ignition is called intrinsic safety (IS).

The National Electrical Code, Section 500, defines classes of hazardous locations as Class I (gases and vapors), Class II (dust) and Class III (fiber). Each class is further defined as Div. 1 (under normal operating conditions, including maintenance) and Div. 2 (accidental release or exposure due to unexpected rupture or breakdown).

In the industry, one might commonly see Class I, Div. 2, to describe an unexpected exposure of electrical energy to dust, for example.

Let's talk about a few common control devices that would introduce risk in a hazardous environment. Many machines use limit switches or cam switches; a cam switch is a limit switch with a roller on the end that follows a lobed cam.

The construction of these mechanical switches requires a physical lever to pass through the body of the switch. No matter how well made, there is the possibility of a gas or fine powder getting into the inner workings of the switch and providing a catalyst to a source of ignition.

While not as common any more, many electric motors came with exposed windings to aid with cooling. This provided a path for the combustive material to get into the terminal block area of the motor.

Newer motors tend to be totally enclosed and fan-cooled to reduce this risk, but unless the body is completely dust-, liquid- and gas-tight, the combustive material can still get through to the motor.

For these reasons, devices used in a hazardous environment must be intrinsically safe. However, the use of intrinsically safe field devices does not make a control system intrinsically safe.

For this reason, the Occupational Health and Safety Association (OSHA) requires that the whole control system be designed to be intrinsically safe. It is not enough to use IS-rated devices.

The exception to this general rule is devices that use low power or are passive in nature. A good example of this would be thermocouples or resistance temperature detectors (RTDs).

Generally, the design of an IS system requires the use of low voltages and low temperatures, so as to not provide an environment that is conducive to the ignition of combustible materials.

While the common focus is on the field devices, the control cabinet itself might contribute the biggest risk of combustion. Inside that enclosure, one will find lots of miniature switches turning off and on, as well as plenty of devices that release energy—heat—as a result of normal function.

While not as obvious as combustible gases or liquids, dust is likely the most common source of combustible material. We are talking of particles as small as 500 microns in size.

OSHA 1910.399 states, "Combustible dusts that are electrically nonconductive include dusts produced in the handling and processing of grain and grain products, pulverized sugar and cocoa, dried egg and milk powders, pulverized spices, starch and pastes, potato and wood flour, oil meal from beans and seed, dried hay, and other organic materials which may produce combustible dusts when processed or handled. Dusts containing magnesium or aluminum are particularly hazardous."

To avoid ignition, we generally talk about voltages under 29 V and current consumption under 300 mA. While PLCs and associated I/O modules can be selected to operate at 24 V or less, the presence of a VFD, for example, would imply voltages at well above the 29 V target.

As one can imagine, it would be pretty much impossible to make all of the components inside a control cabinet to be intrinsically safe, so what can we do to protect our control system from the risk of ignition? Well, the somewhat obvious answer would be to keep the microscopic dust particles out of the enclosure in the first place.

The conventional design methodology involves introducing elements to reduce the normal operating temperature inside a control cabinet or enclosure.

The easiest way to do this would be to provide a filtered inlet to draw in outside air and a fan to circulate that air throughout the enclosure before exhausting it back out of the enclosure.

This approach doesn't work for a hazardous location because we would be drawing all those microscopic particles into the enclosure and exposing them to an environment that is highly conducive to the ignition of combustible particles. An air exchanger would have the same issue, and an air conditioner would be the best choice if it wasn't for the fact that we are talking about particles that are 500 microns or less.

No matter how tight we make the seal on an enclosure, particles that small are bound to get into the enclosure. Just air convection alone would cause this to happen, as we would have cooler air outside the enclosure and warmer air inside.

The ultimate solution is to create an environment where there is greater air pressure inside the enclosure than outside. The introduction of clean, dry air to the inside and a means to exhaust air from inside the enclosure to outside ensures that airflow will always favor leaving the enclosure. This addresses the normal conditions of Div. 1, but what about if/when we have to open the enclosure to perform maintenance or troubleshooting? For this purpose, most positively charged cooling systems also include a purge system so that all the air can be exhausted from the enclosure before restoring operation.

A pressure sensor monitors the pressure differential between inside and outside of the enclosure and will not permit operation of the control system until the air has been sufficiently purged and a temperature sensor ensures that the temperature inside the enclosure is also kept to a minimum.

One last subject, the difference between explosion-proof and intrinsically safe, should be mentioned. A device that is explosion-proof is contained, so that it is capable of withstanding a gas or vapor explosion. An intrinsically safe device is designed so that it is not capable of causing an explosion in the first place.

It can be easy to overlook the presence of minute particles or vapors in the ambient conditions where our machine or process is intended to operate, but the consequences can be deadly. Please take precautions and ask the right questions to make sure that, where necessary, we are not only safe, but intrinsically safe.

Create a vision-design specification

Use best practices to design and build an effective machine-vision system

By Dave Perkon, contributing editor

There are many industrial applications where machine vision can provide a more robust and capable automated process than simple position and presence sensors, such as photo eyes. Unfortunately, these same machine-vision systems, smart sensors, for example, can affect machine performance and quality by not outputting accurate or repeatable data.

Fortunately, the technology available in off-the-shelf machine-vision sensors is well developed; it just must be properly implemented. To accomplish that, the machine-vision system must be professionally designed from the start, understood by engineers, technicians and operators, especially those not involved with its initial installation, and supportable well into the future. To do this, industry best practice requires creation of a vision-system design specification (VDS).

You cannot make a machine-vision system perform inspections it is not capable of performing, so quickly assembling a vision system, lens and light and mounting it to the machine and programming it isn't best practice. Machine-vision hardware must be carefully specified, designed and tested—not only the camera itself, but the lens and lighting, as well, and how it is mounted to the machine. Resolutions, field of views and mounting positions of camera and light also play a big role.

The purpose of the vision-design specification is to specify how the vision-system hardware will be connected, configured and assembled to meet the inspection requirements. The VDS has several major sections that define a vision system from general to application-specific details.

General VDS sections include detail drawings of the parts being inspected and system interface to upper level systems, such as the PLC. A table of drawings and critical dimensions, features and requirements should be included.

The physical interface of the PLC to the cameras should also be detailed in a diagram with additional sections defining the data structure and communication interface, such as Ethernet. Timing diagrams are also helpful for understanding and system control and monitoring techniques, such as triggering, camera communication active and camera run mode.

Another general VDS section is the HMI, such as camera controls, images and graphical displays. The inspection-results data display should also be defined, including real-time and historical and data-trending. Include definition of how the inspection-results data and inspection images are saved. Future engineering analysis of the camera inspections will benefit from having clearly defined data and at least all reject images and a few good, "golden" part images for reference, saved.

With the general VDS sections complete, the next focus is application-specific—how each camera is configured and installed to complete the documented, required inspections. This includes a definition of the inspections, mechanical-layout diagrams, sample images, camera specifications, lens and lighting specifications and definition of the field of view (FOV)—each a section of the VDS.

The inspections should be detailed so all can understand what dimensions, features and orientations are checked with expected results and reject definitions. Then a mechanical-layout diagram or two is required to show the camera, lens configuration, including spacers and adapters, and light. The layout diagram should also detail the position of the inspected part relative to the face of the camera lens and light. Include dimensions and part numbers. Sample images of the inspection acquired using the defined layout must also be included for reference.

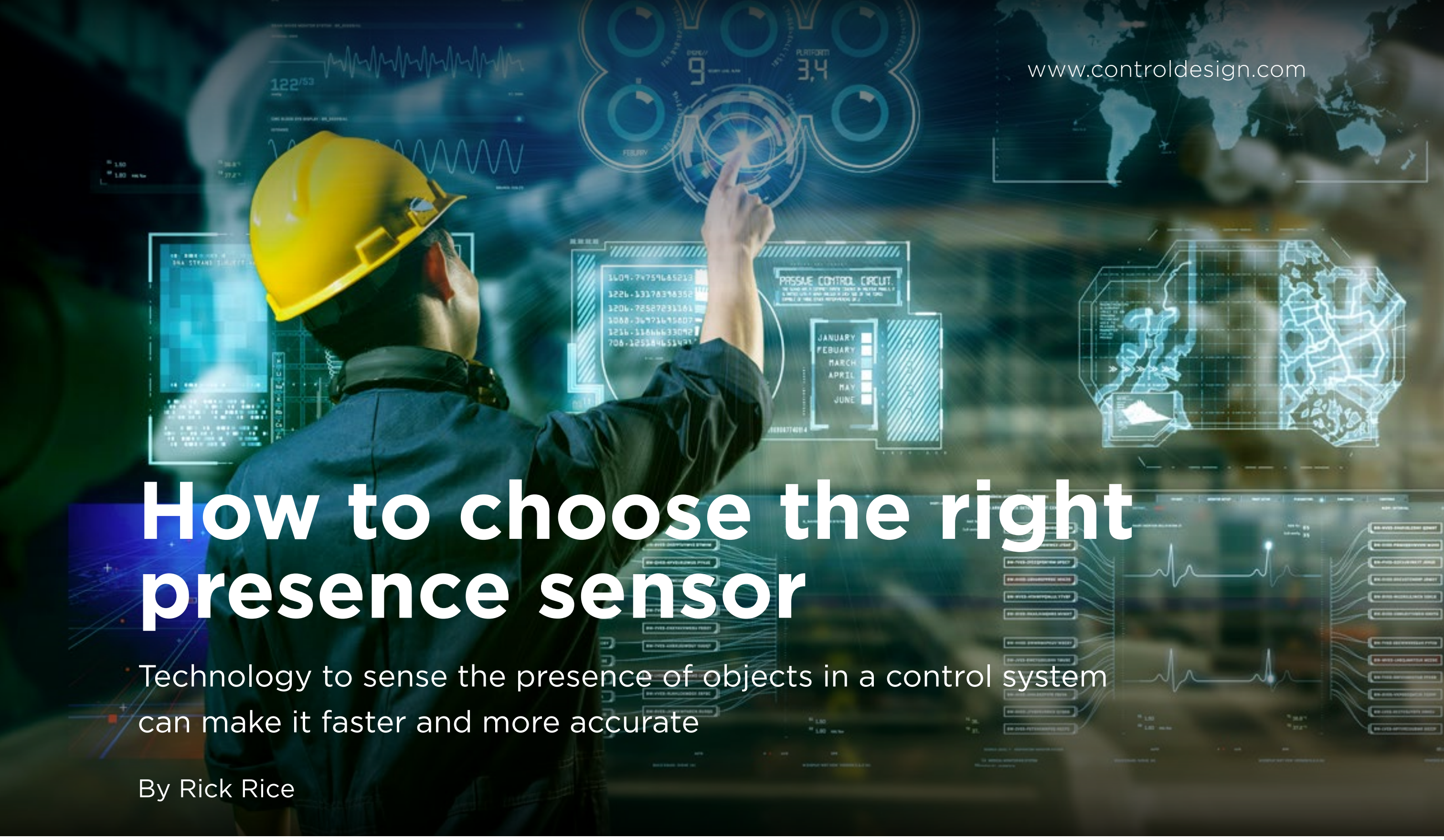
Additional application detail sections include specification tables for the camera, lens and light. Include camera part number, type of image, such as area or line scan, resolution, orientation and cabling. Lens part number plus spacers and adapters must be listed along with the FOV, working distance and depth of field. Fixed-focus or adjustable-focus details should also be listed, as well as focal and f-stop settings. Images of the lens settings are helpful and should be documented for future reference. Finally, include a lighting specification table including part number, color, location and distance to part, as well as power supply and triggering such as strobe or constant on.

A field-of-view diagram section must document the height and width of the acquired image relative to the inspected part. Include both pixel and engineering unit dimensions. This diagram can be an actual image or a graphical representation of the FOV.

Some final sections of the VDS, often for each, include calibration, camera checks and reject characteristics. Calibration may need to be carefully detailed for measurement applications. However, telecentric lenses often do not need calibration after their initial setup, so it is important to carefully detail these requirements.

Camera checks, such as exposure and focus, should also be defined. This is important information to know over the lifetime of the application and can show if inspections are changing. Test gauges, golden parts and/or challenge parts should also be defined and detailed to prove the vision system is working as expected over time and enable recalibration and adjustments if not. And be sure to include example reject images and details of the inspection tools used to find them.

Clearly defining vision system hardware, mechanical configuration and the application-specific requirements in a vision-design specification is industry best practice. Be sure to create one, implement the vision system as designed and then clean up the VDS after final testing to ensure accurate, usable information now and in the future.



How to choose the right presence sensor

Technology to sense the presence of objects in a control system can make it faster and more accurate

By Rick Rice

The field of automation is based on a simple concept. Take something that can be done manually, and make a machine or process to do the function automatically. Keeping with that simple theme, automation depends on input signals to determine when an event happens and output signals to create a desired action. All the rest is just filler. Some of you may get a chuckle out of this crude analogy, as you can probably picture yourself using similar terminology to justify your existence to a boss or upper management.

Input devices come in all sorts of shapes and sizes but, at their base function, they come in two forms—digital and analog.

A digital sensor is, by its very description, either off (a 0) or on (a 1). A simple form of a digital sensor is a limit switch. A limit switch is a physical switch that uses a pivot point upon which a rod is mounted. One end of the rod will make contact with an object in motion and the other end activates a switch. When the rod is deflected far enough, it will make the opposite end change state on a pair of contacts. In the non-deflected state, the switch is open (or off), and in the deflected state, the switch is closed (or on).

An analog sensor translates displacement into a variable signal, reflecting the zero (off) position and points in between up to the fully deflected position. The most common form of analog signals are current (4-20 mA) or voltage (+/-10 V). Analog signals usually employ a concept called live zero. This approach makes it easy to identify when a wire is broken or no signal is present by making the physical zero equal to a value other than 0. Take, for example, the 4-20 mA current signal. Fully off is 4mA and fully on is 20 mA.

Sensors today still use these concepts, but the variety of sensors grows with each passing year. This article will focus on presence sensors and the technology employed to sense the presence of objects in a control system. Let's review some of these.

A limit switch uses physical contact to deflect an operator. The position of the operator is translated into either a digital or analog signal. An example of the use of a limit (also called a finger) switch would be positioning the actuator in the path of an object travelling down a conveyor or a walking beam. The switch will remain in the zero (off) position until the object makes physical contact with the actuator as the object moves down the conveyor. The switch will return to the "off" position after the object moves out of the path of the actuator on the limit switch.

A cam switch is a variation of a limit switch where the operator rides on a rotary cam. The operator is opposed by a spring that keeps the switch in the off position unless the lobe on the cam deflects the operator enough to cause a change in state. Like a limit switch, the cam switch can be either digital or analog in nature. An example of the use of a cam switch would be in an electro-cam, where cams with different lobe shapes are mounted on a common rotary shaft, each with an associated cam switch. The shape of the lobes are machined to cause the cam switch to turn off and on at different times during the rotation of the shaft. The result is a means by which to provide timing signals to a control system.

The first two switches are examples of physical switches. The following are examples of non-contact presence sensors. In these examples, the sensors must be relatively close to the object but do not to come in physical contact.

A proximity switch is a transducer that takes advantage of the properties of the object to be sensed. They come in five forms: magnetic, capacitive, inductive, optical and ultrasonic.

A magnetic (reed) switch uses the properties of a magnet to sense the presence of an object. The original was invented by Bell Laboratories in 1938. A pair of flexible, ferro-magnetic contacts are contained in a casing. The close proximity of a magnet will cause the contacts to shift position (using the principles of like poles repelling) and either make or break contact. An example of the use of a reed switch can be found in a pneumatic actuator. A magnet is attached to the rod that travels inside the cylinder of the actuator. A reed switch (or more than one switch) is attached to the outside of the cylinder in such a position so as to come in alignment with the magnet that moves inside the cylinder in time with the extending and retracting of the cylinder rod.

A capacitive proximity sensor uses the change in capacitance between the sensor and the object to detect the presence of an object. In order for an object to be sensed by a capacitive sensor, the object must act as a dielectric. An application example of a capacitive sensor would be presence of a foil pouch inside a carton.

An inductive proximity sensor uses a fluctuating current to induce a magnetic field in the object to be sensed. The object to be sensed must be metallic in order to emit an electromagnetic force (EMF) when exposed to a fluctuating current from the sensor. An example of the application of an inductive sensor would be to sense the presence of the end of travel of the rod on a cylinder.

An optical proximity sensor uses the properties of light to sense an object. Optical sensors (also called photo eyes) use the travel of light in a variety of methods to sense an object, regardless of the method deployed. Examples of photo eye sensors include opposed (also called through-beam), retro-reflective and diffuse. In all three types, the object to be sensed impedes the travel of light from the sender (transmitter) to the receiver.

In a through-beam photo eye, the transmitter sends a beam of light to a receiver mounted directly opposite the transmitter. When an object blocks the path of the light, the receiver no longer receives the light and the resultant signal is turned “off.” These sensors are normally “on” and turn “off” when an object blocks the path of light from the transmitter, to the reflector and back to the receiver. This is the most accurate type of photo sensor but is the most difficult to install, as one must align the transmitter and receiver to a close degree of accuracy.

In a retro-reflective photo eye, light is transmitted by the sensor, bounces the light off a fixed, reflective surface and receives it back at the sensor. For this sensor, the sender and receiver are in the same sensor package. In higher ambient light situations, the use of a polarized reflector filters out light that doesn’t come at the reflector directly from the sensor, improving the intensity of the light at the receiver. Again, these sensors are normally “on” and turn “off” when an object blocks the path of light from the transmitter, to the reflector and back to the receiver. This sensor is slightly less accurate than a through-beam but is easier to install because the reflector is more forgiving, as far as placement relative to the sensor head.

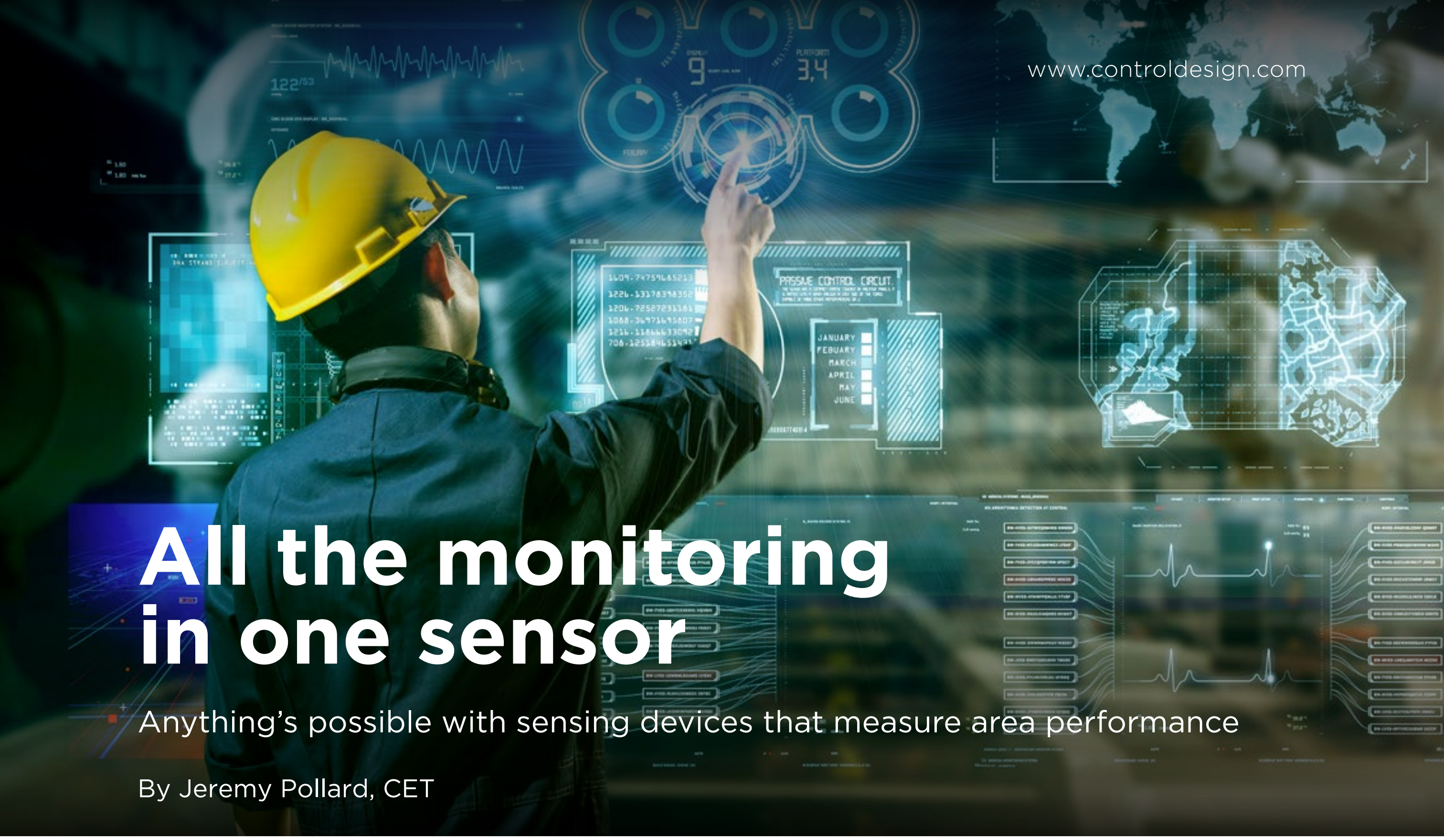
For a diffuse photo eye, the transmitter and receiver are, again, in the same sensor housing. The difference here is the object itself is the mirror to reflect the light back at the sensor. These sensors are normally off (the receiver does not see the light sent out by the transmitter) and rely on the reflective properties of the object to deflect sufficient light back to the receiver. Due to the limited reflective qualities of the object, diffuse sensors are normally used to sense objects that are relatively close to the sensor. These sensors are the least accurate of the three types, as they must rely on the reflective properties of the object being sensed. The color and texture of the object can adversely affect the ability of the sensor to detect the reflected beam back at the receiver.

With all optical sensors, the type of light emitted by the sensor can greatly impact the efficacy of the sensor. For this reason, most photo eyes tend to use LEDs emitting in the infrared light spectrum. Newer photo sensors use class II laser technology to provide a more precise beam of light. This results in more accurate results over longer distances than infrared sensors. Fiber optics can be used to transmit light in a finer medium. Different light sources (colors) in a single sensor head also add to the functionality of the device. As the technology advances, more and more application control of the sensor is added to the sensor (or amplifier) to provide application-specific fine tuning.

The final type of non-contact proximity sensor is an ultrasonic sensor. The sensor head emits an ultrasonic wave and determines distance by measuring the amount of time it takes for the wave to be reflected back to the receiver. Ultrasonic is a great medium for distance sensing because it isn’t affected by dust. Sonic waves bounce off transparent objects like glass and plastic (light would pass through or get deflected). An example of an application for ultrasonic is the presence or level of grain in a silo or powder in a hopper.

While all proximity sensors can be both digital and analog in nature, only optical and ultrasonic sensors tend to be used in an analog application. The speed of sound, like light, is a constant, and this allows for the time from transmission to reception to be used as a means to measure distance. Due to these properties, most of the continuing development of optical and ultrasonic sensors tends to be based on getting more accuracy and user-configurable features out of the technology.

Control systems will always be called upon to keep up with the speed of life, and presence sensing will follow along with new technology to make it faster, more accurate and easier to use.



All the monitoring in one sensor

Anything's possible with sensing devices that measure area performance

By Jeremy Pollard, CET

I have an Ecobee thermostat for my furnace which is professed to be a smart home device. Well, in fact, it is, and it's part of the IoT domain. It set up easily and allows for email alerts.

My furnace decided to shut down recently, and in order to get it going again I had to cycle power to the circuit boards. So, what if that happened while I was away in the sunny south (post-COVID, of course)?

I would not have known, except for the fact that I can remote into the thermostat to see what the temperature is, as well as set alerts if the temperature drops too low—remote monitoring and diagnostics at its best.

I am going to put the furnace on an IoT wall switch, so if the furnace goes wonky again I can cycle power remotely to fix the problem.

How I wish that the furnace itself was an IoT device; then I could tell if the burners are on and the fan is running and view the heat-exchanger differential temperature indication to let me know it is actually working.

Well, then, how can I accomplish that? IoT sensors—that's how.

I can add a wireless IoT temperature plenum sensor and an air flow sensor, which will give me all the information I need, and I will have access to them through Google Home.

My other option is to use my home PLC to use digital and analog I/O to monitor all the signals and set an alarm which could generate an email based on the logic. Or how about using this thing called the cloud?

Industrial remote monitoring using the Industrial Internet of Things (IIoT) and the cloud can provide so much information from your process or machine with the addition of IIoT-enabled sensors. The diagnostics they can provide are priceless.

I tend to lump remote diagnostics into the alarming bucket of processes. Using IIoT devices along with your legacy alarming system can provide you with myriad data that can be used for all kinds of diagnostics and monitoring.

With the advent of IIoT devices and edge computing, remote anything becomes a total reality. One day, I bet that your cell phone will become a task scheduler, whereby the system detects a fatal alarm. Instead of broadcasting that alarm to everyone, location information from your device will allow the system to direct the alarm to the person either most qualified to address the error and who is the closest to the problem. While that may prove to be a feature, if that person doesn't react, then things will go south in a hurry.

Remote monitoring is not the same as remote access; however, remote-access solutions may need to be employed to address the alarming issue.

Wireless sensors can integrate with systems at the device level easily these days, so there isn't any excuse not to employ the extra alarming coverage. By having an edge-computing device, such as Opto22's

These sensors are general-purpose and can indirectly monitor large plant-floor areas.

EPIC, or an edge HMI that can process data, such as ADISRA, putting data into the cloud directly becomes a reality. Using MQTT brokers can make that data accessible without a huge network impact.

An up-and-coming development is the use of synthetic sensors. In principle, these sensors are general-purpose and can indirectly monitor large plant-floor areas so that direct instrumentation of the individual machine contexts is not necessary.

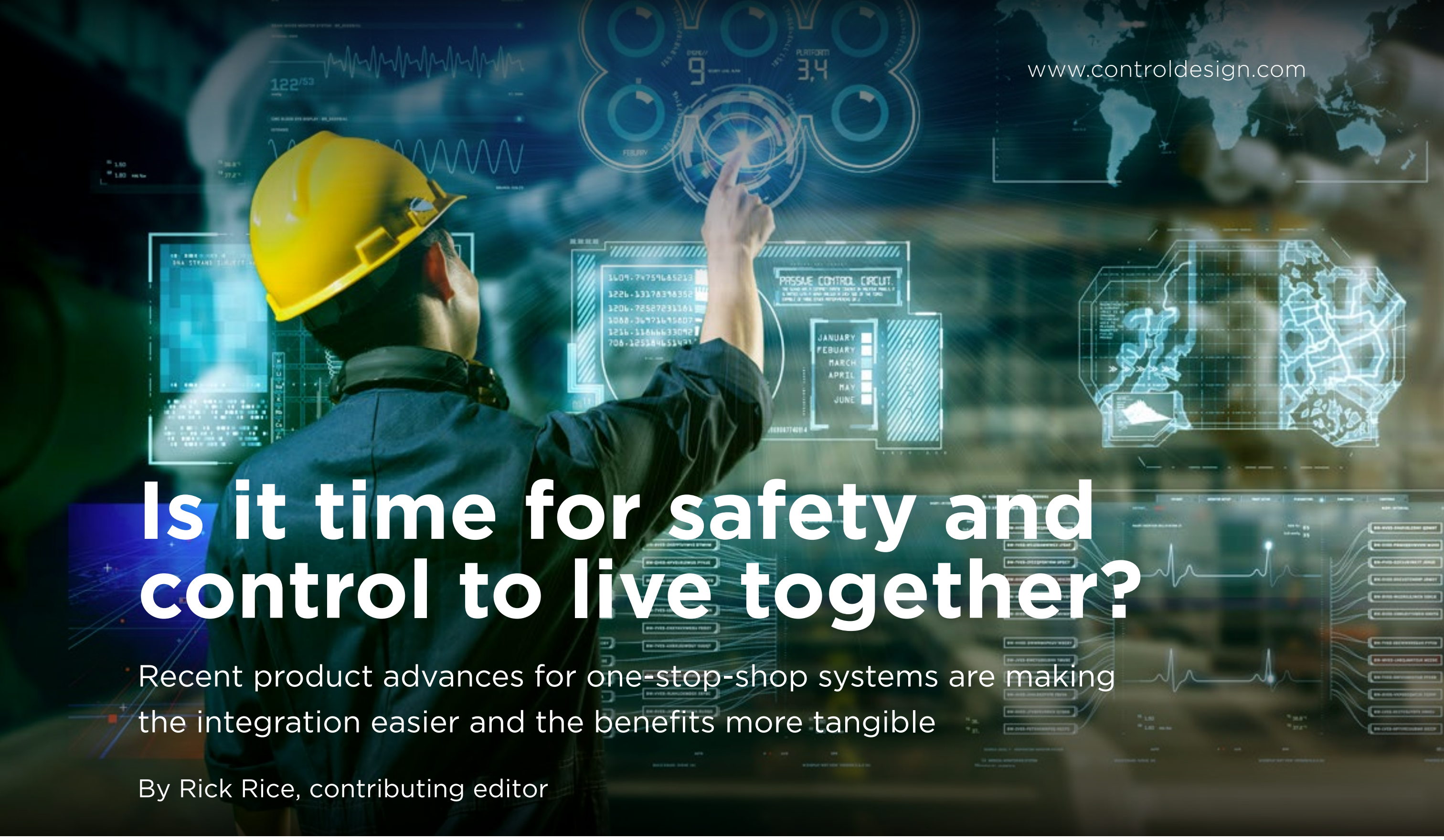
Dr. Gierad Laput wrote a paper which was delivered at the ACM Conference on Human Factors in Computing Systems (CHI, chi2021.acm.org) dealing with these super sensors.

His premise is that these "highly capable sensors" can monitor a large context and virtualize raw sensor data and turn that data into actionable feeds to an application. It has primarily been used and tested in home automation, and the thought is that the premise can be applied to the IIoT space and plant-floor monitoring.

These synthetic sensors would be deployed over a space and monitor various attributes of the environment. Laput's sensor device can monitor 12 different properties, including vibration, audio, EMI and air pressure of the environment.

Part of the holdback of implementing remote monitoring and diagnostics could be cost and the required engineering, depending on the application. Technical expertise may also be an issue since not everyone is familiar with the new technologies, such as interfacing with Microsoft's Azure platform for cloud-based storage of data and remote diagnostics.

I won't be putting my furnace into the cloud, but I could if I wanted. That's the attraction of remote monitoring and diagnostics. It can be done.



Is it time for safety and control to live together?

Recent product advances for one-stop-shop systems are making the integration easier and the benefits more tangible

By Rick Rice, contributing editor

Integrated safety has a lengthy past as determined as its untold future.
Like pretty much everything else in our world of controls and automation, technology is always marching forward. I've found myself on the leading edge of the wave many times in my career when it comes to emerging technologies, and, while I might have enjoyed the rush of diving into a new product, the more mature—slower, older—version of me is a little less thrilled with the prospect.

Moving into a management role many years ago, the consideration of cost is certainly more in view than it was in my younger, let's-give-it-a-go years. For these reasons, the prospect of combining safety and control into a single package was something I wasn't quite ready to jump onboard with. Where does integrated safety stand? And where might it be headed? The concept of safety controllers as a separate entity from a programmable logic or automation controller has been around for a long time. I remember working with early versions of a safety controller as far back as 2005. In those days, the focus was on having supervisory control over the safety devices on a machine or process that was physically and electrically isolated from the programmable controller that operated the equipment, so that a failure of the PLC/PAC would not incapacitate the ability of the machine or process to safely cease operation.

When I think of combining control and safety, I immediately think of process systems, rather than automation or machine control. The integration of the two concepts, however, is not new. As early as 2015, Institute of Electrical and Electronics Engineers

(IEEE) had published a report out of its 10th IET System Safety and Cyber-Security Conference, identifying the economics and manageability of an integrated control and safety system (ICSS) over an isolated basic process control system (BPCS) with a safety implemented system (SIS), particularly in the oil and gas industry. Individual vendors had been promoting the use of ICSS for years prior. In fact, I've seen references as far back as 2011.

So, some of you are now wondering, what has taken me so long to get onboard? I would admit that it's probably more about the philosophy of "don't fix it if it's not broken." Though I hate to admit it, I have become complacent in my march through time. I submit that I'm probably not the only road warrior to get caught up in this comfortable position. Let's lay out some pros and cons of separate vs. integrated systems.

In keeping safety and control separate, we encounter the following:

- The PLC/PAC is interested only in the control of the process or machine.
- Code is smaller, easier to navigate.
- Hardware is simple and familiar.
- Safety controller provides a signal (usually dual-redundant) to the PLC to not only drop out the power to the outputs, but also to bring the control system to a software stop.
- Negatively, there is more physical space required in a control panel to contain the separate components for control and safety.

The features listed above were part of the early advantages of a separate SIS. The programming structure of a safety controller has always been pictorial and resembling bit logic.

Most vendors provided an interface that was drag-and-drop in nature. One can quickly build up the structure of the safety circuit by identifying the zones of the machine or process and then declaring the interaction between the zones. Finally, the individual safety devices within each zone are defined and the desired functions are programmed.

In an ICSS, the control and safety controllers are in one package. The features of this unified system are as follows:

- The panel footprint is smaller.
- A common software platform means only one programming package is required to configure control and safety.
- A common package also means intrinsic interlocks between the two systems.
- Vendors offer hardware packages now that include both traditional and safety-

rated I/O on the same base platform.
- A negative aspect is that the unified platform tends to be much more expensive than the separate systems. If there is a failure of the base control/safety processor, then the cost of repair/replacement is a significant consideration.

One-stop shopping for safety and control certainly has merit. A challenge of separate systems is bringing together functions into a unified, safe, dependable control solution.

Product offerings continue to evolve. One supplier representative has been gently poking at me for a couple of years to look at this technology, and, again, the old man in me has resisted the urge to look at the new candy on the shelf.

Moving into this hardware platform isn't nearly as uncomfortable as I thought it might be. The conventional PAC is still there and functions as it always has. To that system, hardware is added for safety, and a separate safety task is added to the base architecture. PACs are after all multi-tasking processors. My particular hardware vendor has both a SIL-2 (Category 3) and a SIL-3 version, based on one-out-of-two (1oo2) architecture.

For clarification, there is a 1oo1, or single-channel, architecture and a 1oo2, or dual-channel, architecture.

A 1oo1 architecture is the simplest safety circuit, commonly referred to as a SIL-1, SIL-2, PL/a, PL/b, PL/c, PL/d or Category 2 system. It has limited ability to detect faults in bits or values, memory faults or problems introduced by electrical noise. Diagnostics usually run on a single processor, using the same paths and connections as the main controller and I/O and, for that reason, are not as reliable. For this reason, 1oo1 architecture may not be desired for processes where safety is a primary concern.

A 1oo2 architecture has dual paths through the safety system (sensors, logic, outputs and field devices) with either path capable of interacting with and controlling the safety function independent of each other to bring the system to a safe state. This system is considered fail-to-safe and gains a SIL-3, PL/d, PL/e, Cat 3 or Cat 4 rating.

Another advantage of the integrated control and safety system is the ability of the control processor to read the status of the safety memory but not write to it. In this regard, there is shared information with no possibility of a programming error causing the safety function to be impacted by the control function. One can even limit the ability of some users from gaining access to the area of the safety functions on the combined control/safety controller, further protecting the possibility of accidental compromise of the safety functions.

A challenge of separate systems is the bringing together of the functions into a unified, safe, dependable control solution.

These combination controllers are able to host both conventional and safety I/O on the same backplane. Presence of the two types of I/O is automatically detected by the processor, and separate communication channels are used to interact with the modules, based on base function or safety function. These controllers also interact with integrated motion controllers and tie the safety functions into the control architecture. Safety I/O can be located on the host controller but can also be remotely located via dual-IP, linear or device-level-ring (DLR) topology.

Ultimately, the choice to continue using separate control and safety systems or unify them into an ICSS architecture is up to the designer, but any decision in this regard should involve some sort of dialog with the stakeholders in the project.

Safety, especially when the machine or process is in close physical proximity to people, must be the primary consideration when designing a control system. There might still be some hesitation to employ this rather sophisticated solution to a small machine where the safety is all in one zone and opening a door shuts down the whole machine, but this technology has advanced to a point where integrating it into a design is no longer a burden and should be a serious consideration in your next automation project.