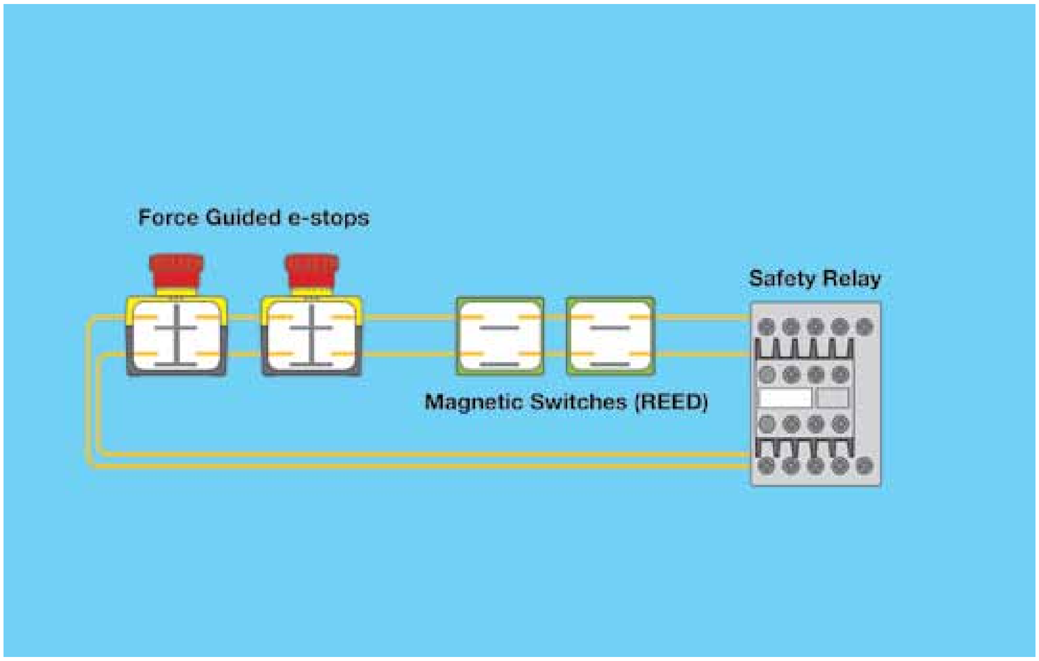
Redundancy in technological systems

Redundancy is a concept frequently applied in technological systems. Investigating in detail why redundancy is used, one will find that there are many reasons for doing this. Looking at several redundant implementations should make this clear. Still, all aspects of redundancy have one idea in common: increased ability to control a system even when problems occur.

Safety

Functional safety systems are probably the most common automation solutions based on redundancy. Here the rationale is to provide a control system that is able to safely shut down a machine in case of emergency. Depending on a detailed safety evaluation, safety solutions of varying complexity can be used to address the particular needs of the application.   Safety systems are still designed to comply with EN954 which divides applications into five classes between B at the low end, and CAT 4 at the upper end. To show that not all redundant systems are equal let's focus on two scenarios. **Figure 1** shows a safety system where a number of redundant-safe input devices (e-stops and magnetic interlock switches) are connected redundantly in series. These safety strings are then connected to a safety relay which is ultimately responsible to shut down motors, drives, or other potentially harmful devices.

Figure 1: Multiple safety devices are commonly wired as shown in this illustration. If a contact fails on a device, this can lead to situations where even safe inputs that are faulty will allow the system to be restated.

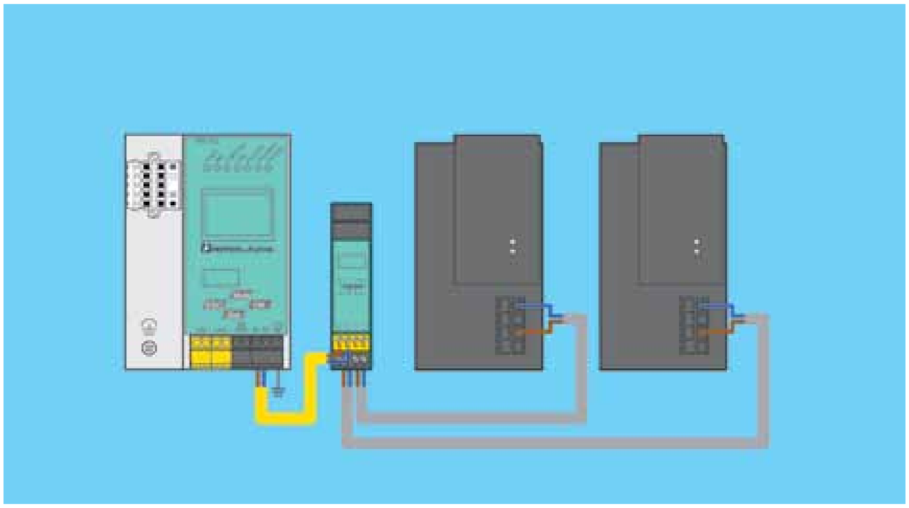


Consider a situation where one of the safe contacts on a magnetic safety switch is welded or simply sticky. Due to the redundant nature of the safety string the machine will still come to a safe shutdown as soon as the door, evaluated by a magnet, is opened. Even better, the safety relay will not even allow a restart of the system after the door has been closed. The reason for this is that the safety relay "demands" that "as soon as one of its safe inputs shows an open contact, the second input MUST also go open," clearly a condition not satisfied due to the welded contact. Unfortunately, it is rather trivial to trick the safety relay. All one has to do is open and close another door. As soon as this happens, the safety relay detects its two inputs as open, making this a resettable condition.

As soon as this happens, the redundant nature of the system is compromised. All it takes is a second fault at the magnetic door switch, and it will not be able to result in safe system shutdown.

Contrast this with **Figure 2** where each of the safe input devices is not daisy chained into a safety relay but connected to a safe input module. Those safety input modules are then connected to a network that supports safety functions. Going into the details of the implementation is not necessary to discuss the effect this type of solution has. The information from the redundant contacts of the safety devices are processed by the safety input module and then transmitted via the network. Because each module has a unique address, the "safety controller" (replacing the safety relay) can easily evaluate each input device independently. In a situation where the magnetic interlock switch has a welded contact and is then activated, the safety controller will–just as the safety relay did previously–deactivate the machine. Closing the door again will not restart because only one safe contact was ever seen open. In contrast to the system in **Figure 1**, this setup cannot be tricked by cycling another door or e-stop. A higher level of safety has been achieved.

Figure 2: By associating each safe input with a safety-rated input module, the safety controller in this network can be configured to safely inhibit restarts as long as a safe input has not been replaced.

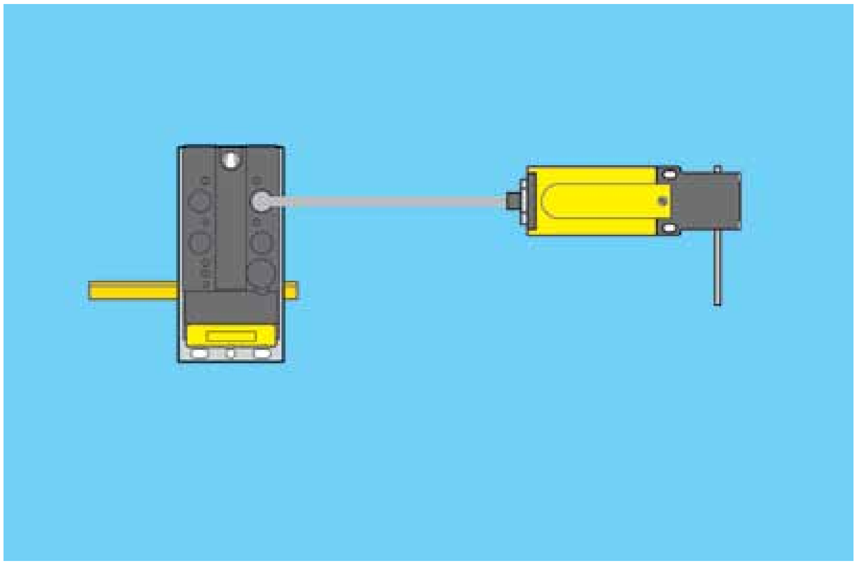


Besides offering this higher level of safety, the system in **Figure 2** also provides significantly enhanced diagnostics. In the past, safety was often seen as a necessary evil to keep operators from making grave mistakes and getting hurt in the process. The solution in **Figure 2** shows that this is not the only reason. Because each safety device can be uniquely identified, PLC programmers can easily write logic to clearly indicate the location of a fault. Furthermore, using the right network to transport the safety data, it is even possible to automatically identify if a safety device has a fault (for instance a welded or sticky contact), if machine vibration results in nuisance shutdowns (significant vibration causing intermittent contact opening) or perhaps, willful interference with the system.

Redundant power

Power supplies see a lot of abuse. In many cases the AC input voltage is not clean and occasional spikes have the ability to damage critical components. This is the reason why the Process Industry frequently uses redundant power supplies that can switch so fast, the secondary system does not even detect the difference. Due to their high cost these supplies are not as common in discrete manufacturing, but that does not mean it is not possible to add a certain level of redundancy. The two examples I am about to give pertain to AS-Interface. AS-Interface networks are powered by a power supply that does two things differently. The secondary voltage is slightly higher (~30 VDC instead of 24 VDC) and since data and power is transmitted via the same network, the power supply contains additional circuitry for "decoupling." A simple way to add redundancy is as follows. Take two, 30 VDC non-ASi power supplies (i.e. power supplies without decoupling). Use an external power conditioner (effectively the decoupling circuit in a separate housing). Now redundantly power the power conditioner from the two, non-ASi power supplies. As long as one of the supplies works, the network is operational. **Figure 3** shows how this redundant setup is wired.

Figure 3: By separating the power supply from decoupling an AS-Interface segment can be powered redundantly.



Another redundancy approach is based on using a dual-network, AS-Interface gateway that can receive power either through the first network or the second network. In this case, failure of one power supply would still result in the loss of one network, but because the gateway is still powered though the other network, it remains operational. This means the PLC can still talk to the gateway and the information "no power on one network" can be sent to the PLC.

Redundant sensor output

Most PLC logic is based on positive sensor logic. This means that a sensor is in the OFF state when the object to be detected is not present, and in the ON state when it arrives at the sensing location. Intuitively, this is certainly correct, but it may not be the best solution for critical applications. The issue is that the PLC log has no way to determine the difference between a missing or faulty sensor (failed in the OFF state) and the object not-present state. Quite obviously, basing logic on just one bit (the output of the sensor) cannot yield more than two pieces of information. A very simple and cost-effective way to address this inherent shortcoming is based on employing sensors with complementary outputs, a fairly common feature today. On a sensor with complementary outputs, in addition to the output–let's call it Q_1 that behaves like described above–a second output Q_2 is present. Its output state is always the inverse of Q_1. All the functional logic can still be based on Q_1 making the overall logic, still simple and just as easy to read as the logic using sensors with just one output. Q_2 is strictly used for diagnostic purpose. Because of their inverse relation a few extra rungs of ladder logic code can be used to verify the operation of the sensor. The suggested process is as follows:

- At the top of the ladder logic all inputs are copied from the input image table into a secondary data table
- A few lines of additional logic are then used to test that the input pairs satisfy the relation $Q_{1\,=}$ not Q_2
- If this relationship is true for all inputs we conclude that the sensors are functioning properly and are, in fact, connected to the PLC. Now the normal program logic executes using the signals from Q_1 as before.
- If the relationship is violated for one input pair, warning messages can be placed on HMI screens, instructing Maintenance to determine the cause of the issue.

But why is this not done more often if it is this simple? The additional logic is certainly not the reason, but cost is. Adding the redundant input requires twice as many input connections, twice as many wire terminations, twice as many leads in the sensor cable to the PLC input cards, twice as many terminal connections, plus a thicker conduit/cable tray.

The good news is that there are ways to limit the negative impact through the use of a low-level sensor network. Since I am most familiar with AS-Interface I will talk about AS-Interface I/O, but I am fairly certain that similar hardware is available for other solutions. The concept is as follows. The input module is constructed in such a way that a single M12 connection automatically makes two connections to the sensor. Clearly, an input module with four inputs can now only accommodate two sensors. A module with eight inputs accommodates four sensors and so forth. Once the sensor connection to the input module has been made, virtually all of the negative factors mentioned previously go away. Once the data is on the network the size of the cable tray does not change–one AS-Interface cable run supports up to 248 inputs resulting in 124 sensors with complementary outputs. The number of terminal connections also does not change.

If this level of redundancy and resulting diagnostics is not sufficient one can employ intelligent sensors. I do not want to go into this topic as it is not really related to redundancy, but the following could be of interest.

- Intelligent sensors have their own network address. In the case of AS-Interface, 62 such sensors can be connected to a single cable
- Depending on manufacturer, various levels of diagnostics can be implemented. For instance, we offer AS-Interface intelligent sensors where, in addition to the switch state, the following information is transmitted:
    - Functional availability–this is a bit that indicates that the sensor is working properly and includes testing of the sensing coils
    - Target out of range–this bit indicates that the sensor detected a target, but the target never made it into the nominal sensing range. Based on this bit, it is possible to call for maintenance to verify that the sensor is still mounted correctly or that the object to be detected still follows the correct path
    - Target too close–this bit indicates that the target is dangerously close to the sensor and a collision may occur soon. Again Maintenance can be called to fix the issue before the sensor is damaged.
    - On photoelectric sensors, similar bits are available that indicate a dirty lens condition.

Generally speaking intelligent sensors allow an even higher level of diagnostics and–perhaps more importantly–allow preventive maintenance.

Helge Hornis, PhD, Manager, Intelligent Systems
Pepperl+Fuchs
www.pepperl-fuchs.us
fa-info@us.pepperl-fuchs.com
330-486-0001