For more information:
Leanne Hanson
Padilla Speer Beardsley
612-455-1776
lhanson@psbpr.com

Title: Design Your Safety Control System for Quick Recovery

Rockwell Automation

Not long ago one of our application engineers was sitting in a Rockwell Automation customer's maintenance and engineering offices discussing the pros and cons of a safety system improvement, when a red light started blinking. In mid-sentence, the two engineers got up and ran to the production floor. He scrambled to find his safety glasses and followed them to the "necker" line. The necker line, which forms the top neck on aluminum cans, had jammed. Other workers advanced toward the line from different directions and in a matter of seconds, multiple protective gates unlock and open. Workers reached in to remove the jammed material. In a few minutes, workers re-closed all the gates and restarted production.

When you are forming hundreds of cans a minute, having the machine down for even a few minutes adds up. You need to keep those cans moving – every second is precious.

subhead: Focusing on Machine Safety

A more aggressive focus on machine safety is one of the most significant trends in automation today. Although everyone supports a safer working environment, the implementation of safety systems can hinder production, if not designed or deployed properly. But this need not be the case; improved safety and productivity can go hand in hand. To accomplish this dual strategy, we must design our machines and their control systems for recovery.

So what is Design-for-Recovery (DFR)? It takes into consideration concepts that return a machine to a running state as quickly as possible after an interruption requiring maintenance or a demand on the safety system. Design-For-Recovery has a wide range of implications in machine design, including machine layout, process flow, labeling, training and spares, as well as providing easier access to the machine. Taking this range into account, designers must consider a number of factors during the design stage to improve the ability to recover and restore the machine to a productive state.

During the machine design process, machine designers must consider safety standards and regulations. The prevention of unexpected machine start-up while a task is in process is one common theme. Tasks fall into one of two categories: 1) routine, repetitive and integral (RR&I) to the production process and 2) those that are not routine, repetitive or integral. For more information on RR&I, see OSHA 1910.417 (USA), ANSI Z244.1 (USA), and Z460-05 (Canada) and ISO11418 (International). For those tasks that do not qualify as RR&I tasks, all energy sources must be removed and locked off before tasks can be performed. For those tasks that are routine, repetitive and integral to the production process, safeguarding principles may be implemented when properly specified through formal risk assessment. This article addresses Design-For-Recovery for those tasks that safeguarding principles can protect.

This article focuses on three basic concepts that apply to the safety-related-parts of the machine control system: 1) the machine access strategy, 2) the safety system diagnostic strategy and 3) the zoning strategy, as they relate to recovery time.

Access Strategy

Designing access points to a machine must be commensurate with the expected frequency of the tasks and machine rundown times. When frequent access is required, opening and closing barriers and gates proves time consuming and thus hinders recovery. Safeguarding devices – such as light curtains, safety mats and laser scanners – would serve these applications well. When rundown times are lengthy, light curtains may not be acceptable as the operator may be able to reach the hazard before it achieves a safe state. In addition, machine designers can use safety-rated speed-monitoring devices to allow access to the machine as soon as it achieves a safe speed rather than wait for a ”fixed” time, which allows for the maximum possible time required for a machine to stop.

The machine designer must understand the different types of access in order to better understand access strategy and its effects on recovery time. In general, three primary types of access are available to machine designers for recurring tasks: 1) partial body access, 2) full body access with trip detection, and 3) full body access with constant detection.

Partial body access occurs when a person maintains a portion of his or her body in the protective zone of a safeguard while accessing a machine. This also is commonly called a “reach-through” application. An example would be reaching through a light curtain field or interlocked gate, as shown in Figure 1. This approach provides direct access to the hazard area and a quicker recovery, and it incurs a larger

upfront cost for multi-stage machines as safeguards must be provided for each access point. However, reduced recovery times offer long-term cost savings because operators have direct access to where a stop occurred. Light curtains should be used where access is frequent (every few minutes or less). Interlocked gates should be used for medium cycle times, or where the potential for ejected parts may be a hazard. Gate interlock switches and speed monitoring should be used for long rundown times.

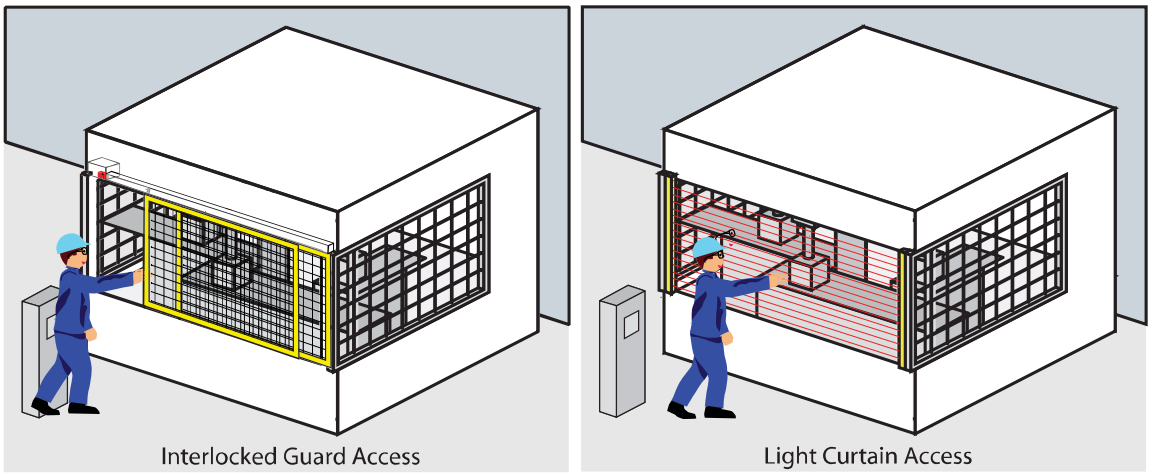
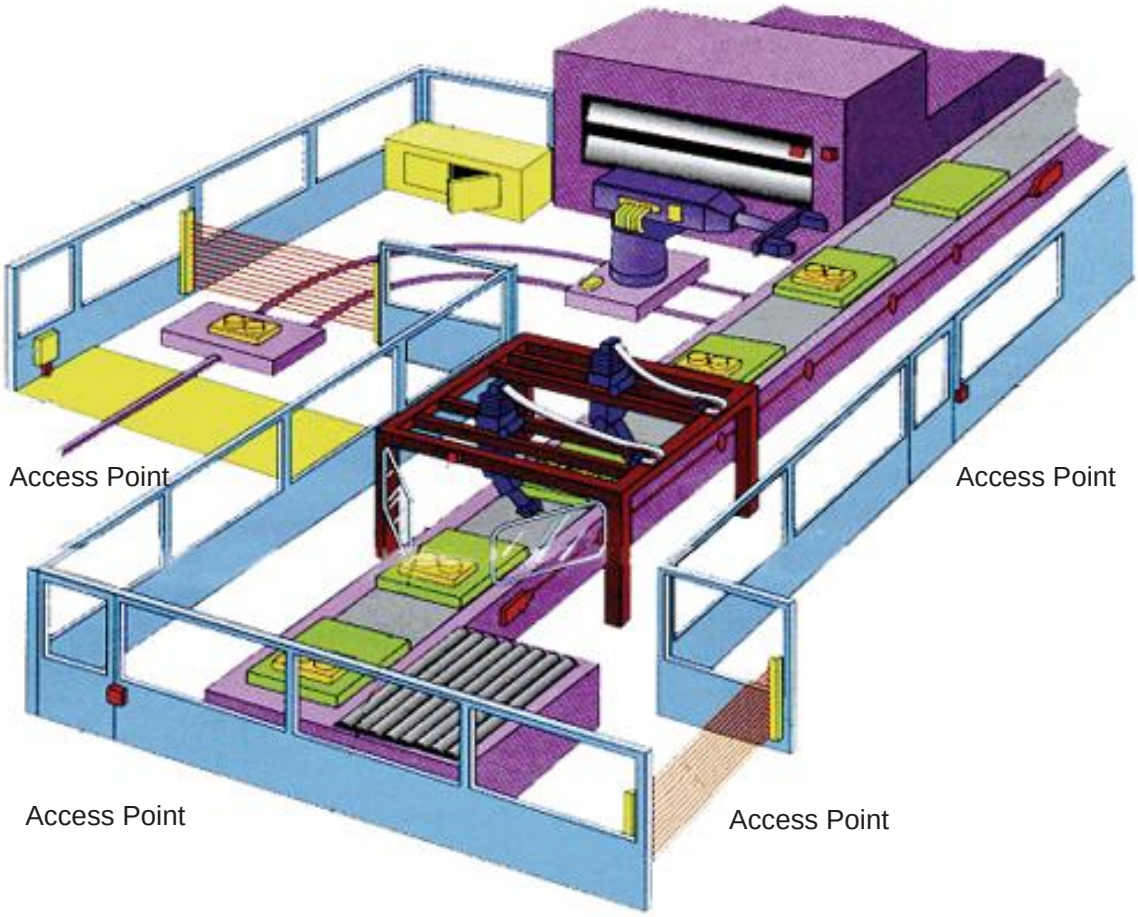


Figure 1. Partial Body Access for Direct Access and Quick Recovery

Full body access with trip detection occurs when a person passes through the protective zone of a safeguard. Full body access often is used with “perimeter guarding”, where a fence or wall surrounds the machine. Entry would be through a safeguard, which might be a presence sensing device or an interlocked gate, as shown in Figure 2. Typically, the operator shuts down the machine and then enters the guarded area. This approach allows multiple persons easier access to the hazard area. The drawback to this approach is the time lost walking into and out of the single entry point and then to the location where the task must be performed. Use multiple entry points to help improve recovery time.



Full body access with constant detection occurs when a person has unobstructed access to the hazard and is detected at all times during the access. Techniques to accomplish this include laser scanners, safety mats, and horizontally mounted light curtains. The ease of direct access to the machine makes this approach ideal for recovery, even though it has higher upfront costs and takes up more floor space due to requirements of stop time distances. An example of this strategy is shown in Figure 3, where a scanner detects the operator at all times during the task.

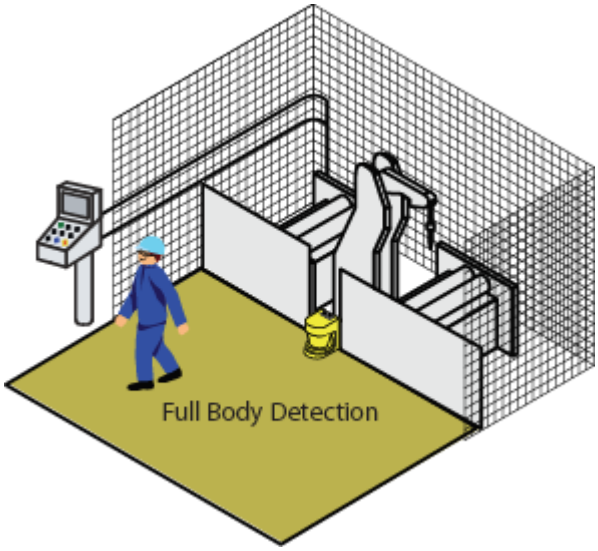


Figure 3. Full Body Access with Constant Detection

Going back to the incident described earlier, the aluminum can manufacturer was using partial body access on its necker line. Several customized interlocked guards were retrofitted to the machine. Therefore, when a jam occurred, operators could go directly to the jammed area, open the guards, remove the jammed material, close the guards and return the machine to a production state. Alternatively, the manufacturer could have used a perimeter guard. In this case, operators would have entered the guarded area through strategically located interlocked gates or light curtains, remove the jammed material, leave the hazard area and then restart the machine.

Diagnostic Strategy

Diagnostics play a huge role in Design-For-Recovery of safety-related control systems. Diagnostics are critical for quickly identifying the reason for the demand on the safety system as well as guiding the workers through a quick and effective restart routine. After executing a task or set of tasks, the safety system must be returned to a protective state before returning the machine to a running state. Each safeguarding device must be returned to an “ON” state – a state that allows the machine to restart.

Sensor Diagnostics

A popular arrangement for integrating safety systems is to connect the interlocked guards in series, as shown in Figure 4. The internal impedance of the safety logic device limits the number of gates that can be connected in series. Some logic devices can accommodate tens of gates and even higher. A pair of wires is run from the safety logic device (for example, a monitoring safety relay) to the first interlock. The wire pair continues through each of the interlocks. Finally, the pair of wires returning to the logic device closes the circuit. Although this approach is less expensive to install than other approaches, it has two major weaknesses. First, if one of the gates is not closed, the machine operator has no way of knowing which gate is open, so time is wasted as the operator walks to each gate to confirm it is closed. Second, if a problem (like an open circuit) occurs within one of the interlocks, finding the problem is challenging. As a result, this design potentially results in a major loss of production time.

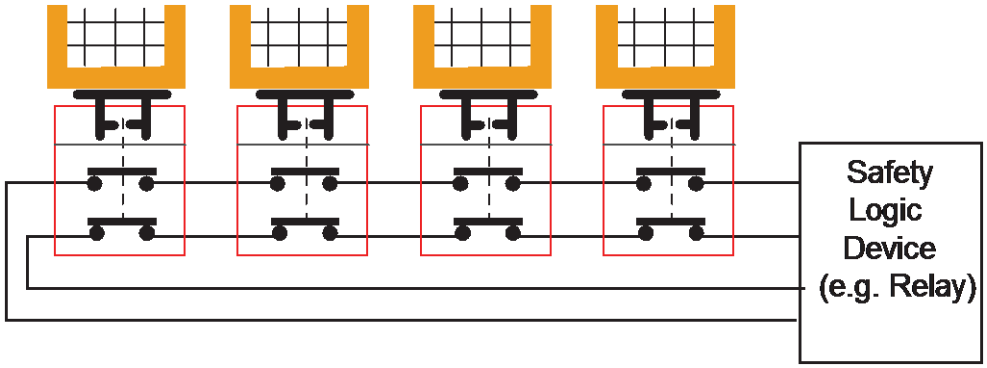


Figure 4. Series Connection of Interlocked Gates with No Diagnostics

To improve the first design, machine designers should use a third contact in each interlock to signal the machine control system (typically a Programmable Logic Controller), which is shown in Figure 5. This is more expensive due to the additional wiring, the programmable controller input points and software code needed to display the gate status. If one or more gates are not fully closed, a machine operator is informed of exactly which gates are open. Thus the machine operator does not waste time checking all the gates. This approach, however, still suffers from the long series of safety wiring. Troubleshooting the safety circuit can be time-consuming and potentially costly.

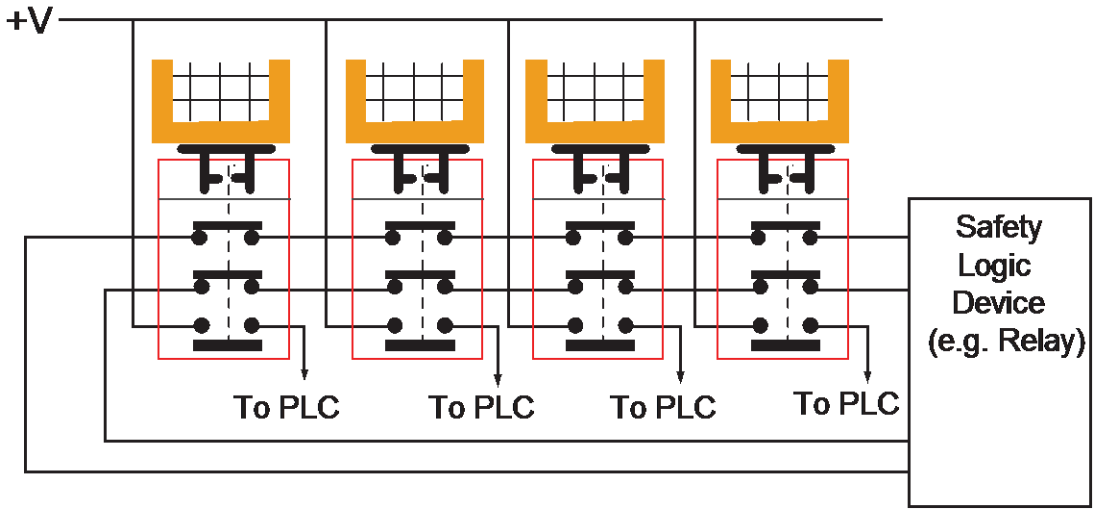


Figure 5. Series Connection with Additional Diagnostic

A third approach is to connect the individual gate interlocks directly to the safety logic device, as shown in Figure 6. This approach performs best when recovery is strategically important. Typically, safety logic devices of this type can communicate with or can be integral to the machine control system informing the operator of the gate status (open or closed), or whether a fault condition exists in the safety circuit. This helps minimize the troubleshooting process as the location of the specific fault is quickly identified and resolved.

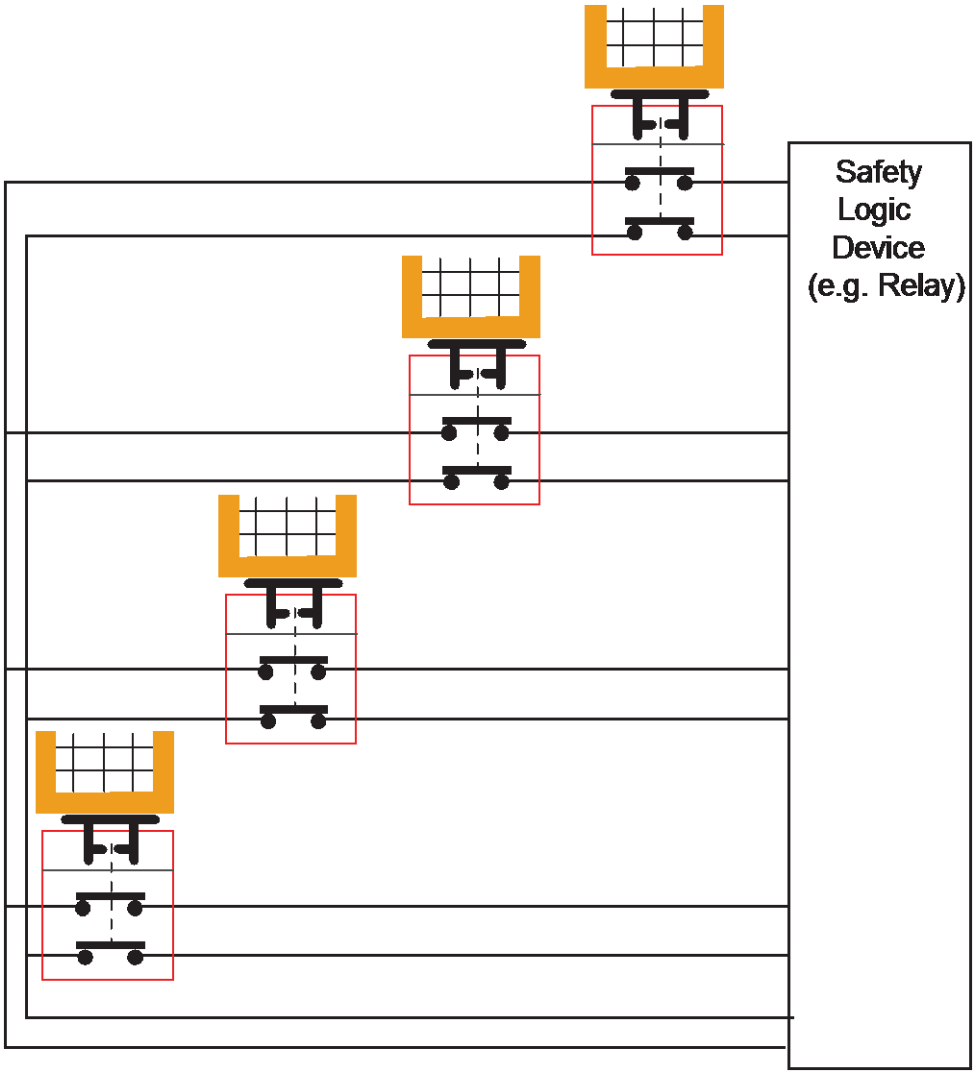


Figure 6. Detection with Diagnostics, individual open gates and safety device faults can be detected

Actuator Diagnostics

Diagnostics of the actuator (e.g., contactors and drives) side of the safety system also is important for Design-For-Recovery. Contactors often are cited as having the highest failure rate due to the high current switching they perform. Many safety relays monitor the actuators by connecting normally closed contacts in series. When only one or two actuators are monitored, diagnostics are relatively straight-forward. As the number of actuators increases, the ability to recover from a fault becomes increasingly longer due to the difficulty in troubleshooting.

In the example shown in Figure 7, one monitoring safety relay controls six contactors (K1 – K6). The monitoring circuit (MC-MC) verifies that all the contactors are off before the safety relay energizes them. This design's weakness is the troubleshooting time required when the machine cannot start because of a contactor fault. Which contactor has the fault?

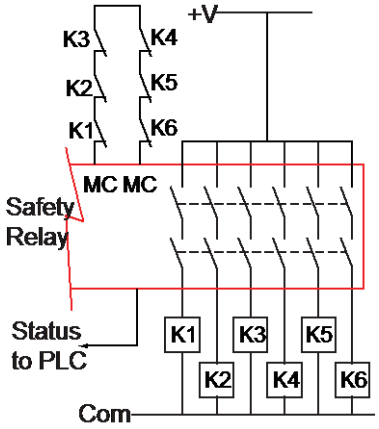


Figure 7. Series Monitoring of Actuators

The Safety Input/Output block achieves a better approach. Each contactor can be monitored individually. This approach utilizes individual wiring from each contactor back to individual inputs on the I/O block. This approach's strength lies in the recovery time because each contactor is monitored individually. If a contactor faults, the safety PLC knows exactly which one. Troubleshooting time is minimized as the faulted device can be quickly identified on a display terminal.

Zoning

Zoning also can be helpful in reducing or even eliminating recovery time. Longer production processes run more efficiently if the process is broken down into semi-independent zones. Zoning allows a portion of the process to be stopped while the other portions continue to run. In an ideal world, material goes in

at multiple points of a process and a product comes out at the end. But the real world must accommodate momentary slowdowns and shutdowns to replenish materials, clear jams, make adjustments and other similar tasks. Allowing small amounts of inventory to accumulate between zones or using parallel zones allows selected zones to shut down for quick tasks.

The key is to accommodate zoning with a sophisticated safety control system. The safety system must be able to provide protection within the zone, as well as at the interface between zones. Otherwise the whole machine must be stopped, resulting in the loss of valuable production time.

How do you implement zoning? The ISO11161 and ANSI B11.20 standards offer guidance on safety aspects of zoning and related issues. A few examples will help highlight the benefits of zoning for reducing recovery times.

In the first example, as shown in Figure 8, four machines are connected in series. The slowest machine limits the overall production rate: 40 units/minute. Two obvious safety solutions are to place perimeter guarding around the whole process or create safety zones, one around each process. With the single perimeter guard, the whole machine must be shut down for a routine task. Let's say the task takes 10 minutes to complete, then the production loss is 40 units/min x 10 minutes = 400 units.

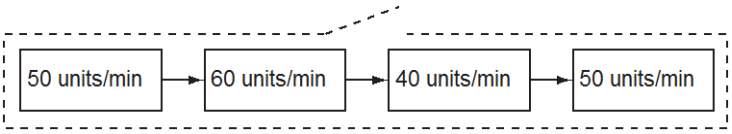


Figure 8. One Zone - Good

If we create four zones, as shown in Figure 9, and Zone 2 needs a 10-minute routine task, then the loss may be avoided if a buffer of 400 units can be added to Zone 3. Zones 1 and 2 must stop during the task, but Zones 3 and 4 continue to run. After 10 minutes, Zones 1 and 2 come back on line just as the

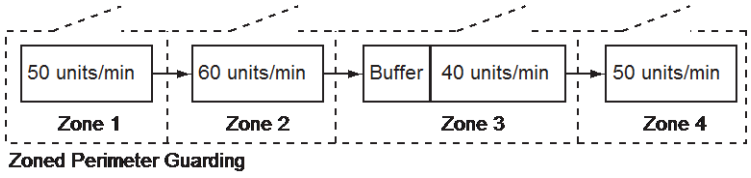


Figure 9. Multiple Zones - Better

Zone 3 buffer is dwindling to zero units. If the process is designed in this manner, then a zoned safety-related control system is required to take advantage of the added buffer.

As machines increase in complexity, zoning becomes more challenging as well as beneficial. In the example below, Figure 10, the machine (Zone 1) operates at 50 units/hour, with material coming in at the beginning as well as in the middle of the process. Unfortunately, one of the feeders can hold only 60 units. The solution? Use two feeders to keep the machine running. While one operates, the second is reloaded. The optimal approach is to create two safety zones; one for each feeder. Another feeder ("D") operates at over twice the machine rate. Use a buffer to keep the machine running, while Feeder D is replenished. Zoning the safety system around Feeder D, excluding the buffer, provides the best Design for Recovery (no down time) for these material feeders.

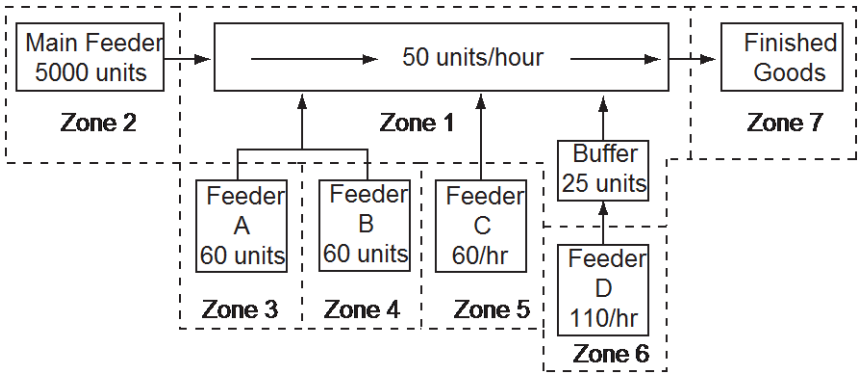


Figure 10. Complex Multiple Zoning

In the example shown in Figure 11, Zone 1 provides product at a capacity of 300 units/hour. The subsequent process only can be performed at a rate of 100 units/hour. To help meet production requirements, use two machines in parallel. The final zone can handle the output of both units. Create four zones for the ideal zoning arrangement. If Zone 2 must be shut down, then Zone 3 can continue to operate, albeit at a reduced rate.

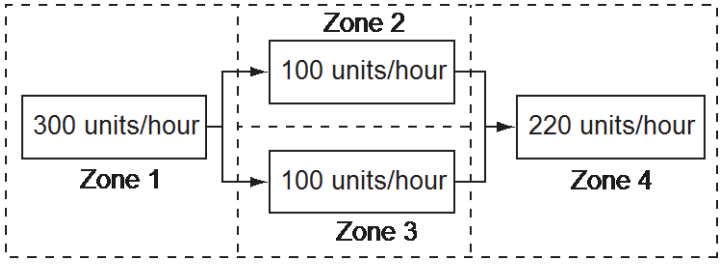


Figure 11. Split Zones - Best

In each of these zoning examples, the safety system must complement the production system, creating an integrated safety/production machine control system. What methods are available for zoning safety systems? To accomplish zoning, use simple safety relay architectures or more sophisticated safety-rated PLCs. The more complex a system becomes, the more favorable the safety PLC becomes for implementation as well as recovery. Examples of some simple architectures help to show how zoning might be accomplished.

The safety PLC approach works best in larger, more sophisticated machines, or where the process requires tight coordination between the safety and standard control systems. Figure 12 shows three zones. Safety devices are connected directly to safety-rated blocks for individual diagnostics. Safety information is communicated over a safety-rated network (CIP Safety over DeviceNet in this case). Status notification to neighboring zones is accomplished easier with this architecture. Zone 2 employs speed monitoring to allow access to the machine as soon as a safe speed is achieved. In addition, the GuardLogix processors integrate closely with the non-safety portion of the machine control system. Interlocked gate and actuator status are communicated easier to the display terminal. A further benefit

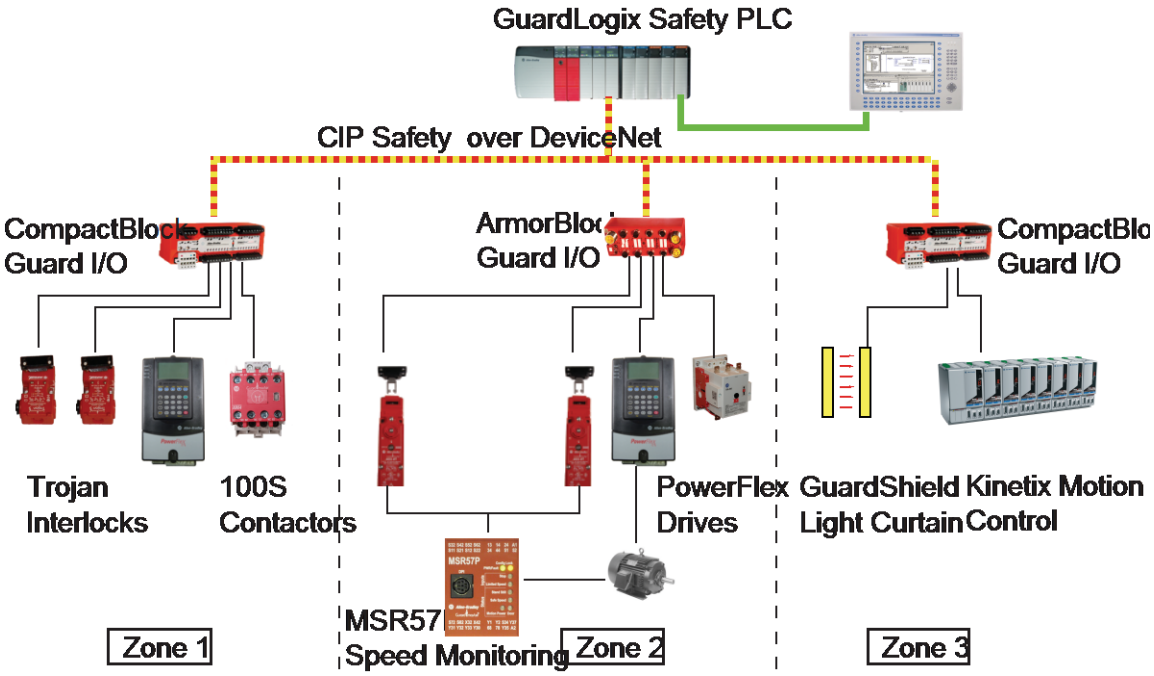


Figure 12. Integrated Safety and Production System

is this approach can be readily expanded to numerous zones.

An intermediate level of sophistication is shown in Figure 13. Logic devices, like the SmartGuard safety PLC, locally control the safety at the individual zones. The SmartGuard can be programmed to turn off the hazards under predetermined conditions and communicate its status to the other zones over DeviceNet. The SmartGuard also communicates status information to the ControlLogix machine control system.

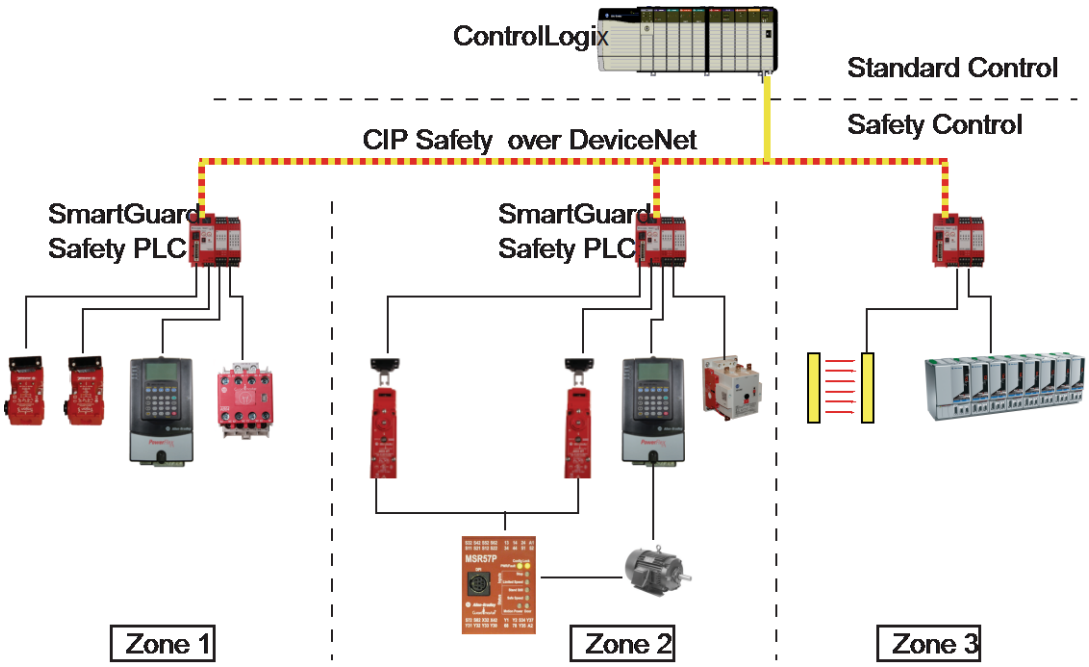


Figure 13. Distributed Safety System with Communications to the Standard Control System

For simpler machines, use safety relays as shown in Figure 14. When the machine is limited to two or three zones, the MSR300 provides a simple configurable, low-cost approach to zoning. Each sensor is connected to an individual input and actuators are monitoried on a zone basis.

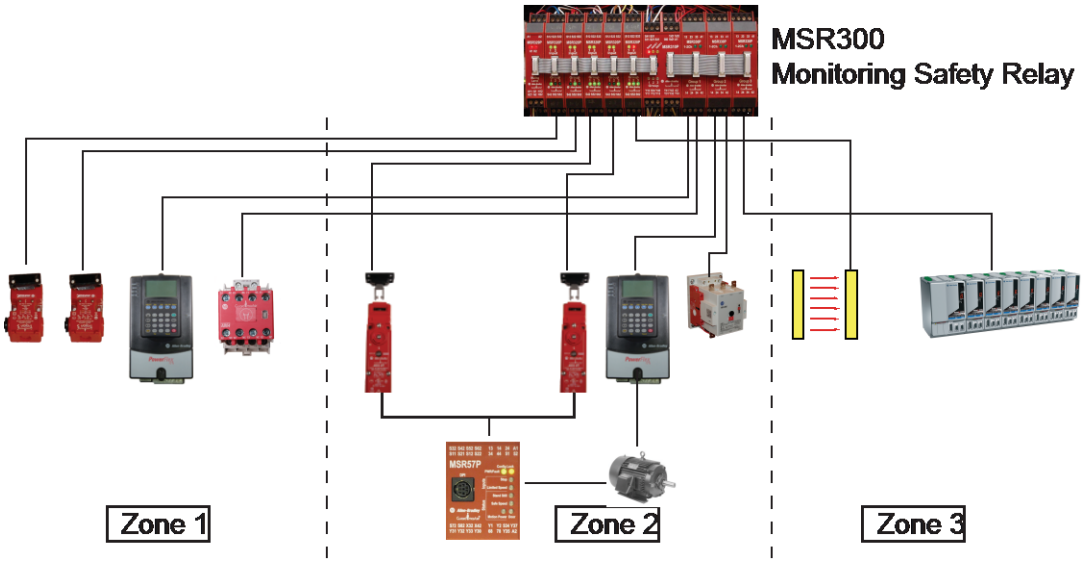


Figure 14. Simple Safety Relay Based Zoning System

Conclusion

Manufacturing continues to be a competitive environment. To help provide a competitive edge, the safety-related parts of the machine control system must be designed to 1) allow safer operation of the machine, and 2) return the machine to a productive state as quickly as possible. Major considerations for Design-For-Recovery include an appropriate access strategy, a robust and accurate diagnostic strategy, a zoning strategy that complements the manufacturing process and a speed-monitoring system that allows access as soon as a safe speed is achieved. Components and architecture systems are available to help manufacturers minimize time to recovery. Implementation of Design-For-Recovery concepts helps improve worker safety while reducing the duration of downtime events. This gives manufacturers the edge they need to remain competitive and compliant – a true “win-win”.

###