Be Not Afraid -- the Time has come to Trust Safety rated PLCs

By Tim Parmer, Siemens Energy and Automation

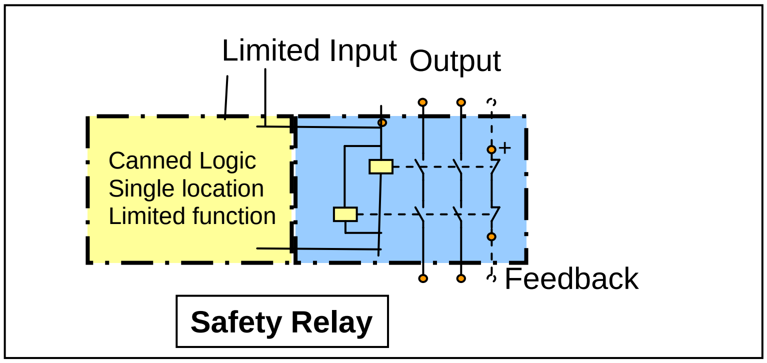
Safety PLCs combine the functionality of a control system with a safety system in one controller platform, allowing manufacturers to greatly reduce machine life cycle costs. An advantage of combining automation and safety is the ability to use one programming language for both control and safety circuits logic which reduce the training required and simplifies the coordination of automation reaction to the safety stops. Safety PLCs help reduce wiring time by enabling safety networks to monitor and/or control all of the devices on a single safety network. Troubleshooting is often cut by 60-80% since the status of each networked safety device is easily displayed the same HMI as the automation statuses.

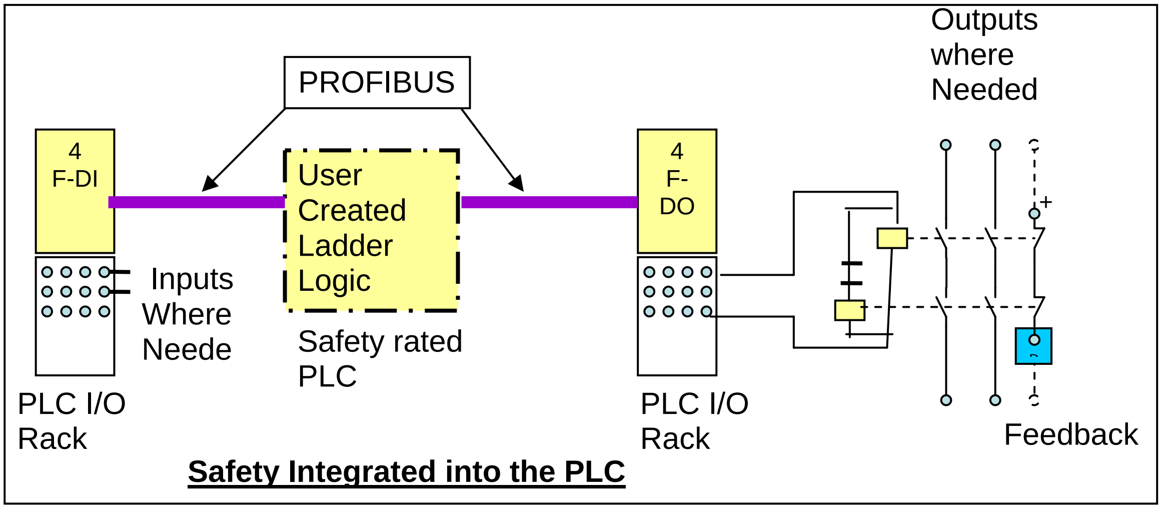
Safety system designs utilizing safety PLCs deliver multiple layers of protection that work together to provide a safe control system. When unexpected events arise, each layer can mitigate the effect of the fault. Safety PLCs from Siemens have led the way creating this "Layers of Protection" concept, achieving the level of protection required for the controller to earn a SIL 3 safety rating. These layers consist of the traditional parts of the PLC, each doing their increased functional safety task to ensure each can act independently, and as a team, to ensure that faults are captured and pacified before they can cause harm. The layers of protection in a Siemens safety PLC consist of four specific parts: a failsafe input module, a safety rated network, a diverse tested logic processor, and a failsafe output module. These layers work together in the safety PLC to provide protection previously available only with safety relays. Delivering this protection in a control architecture that is fully integrated in the automation PLC simplifies delivering safety information to the operator. It also provides the power and flexibility to meet machine control and safety requirements.

The idea of connecting machine safety control directly to the PLC still may cause concern for some people. When you consider the history of the PLC in industry this is a very understandable emotion. However, today's safety PLC is quite different than the PLC used for automation control. Standard duty PLCs have evolved to a highly reliable tool in industry today; however, they are still based on single linier processing of single monitored inputs. This means that any point of failure can cause an unknown failure mode and that is intolerable for protecting personnel from injuries caused by machines in motion. Any system will someday fail it is understandable that the standard duty PLC can not be relied upon when it comes to the safety of employees working around the machine. Therefore, the standard duty PLC must have addition system components to be able to protect the operator and machine even when there are hardware or software faults present. Now this layer of special safety components that was once only allowed in the Hardwired Safety Relays has been successfully integrated into the PLC to create a true hybrid that bring safety protection layers and automation control together. Safety PLCs now use Control reliable design and layers of protection to meet the high levels of reliability required by the current standards.

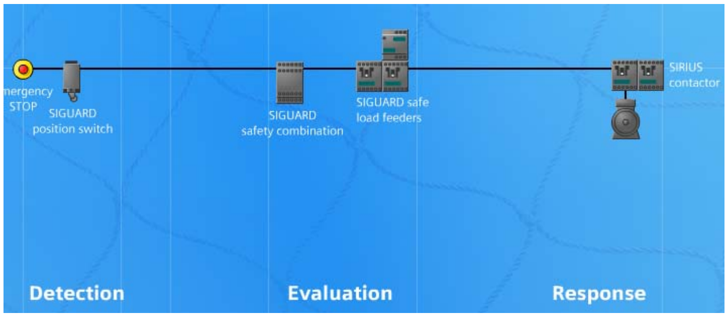
<u>Changes in the PLC</u>

Safety system designs over the years have evolved to rely on multiple areas (layers) of protection around the production facility so that when unexpected events arise each layer can mitigate the effect of the fault in turn. Today's Safety PLCs from Siemens have embraced this "Layers of Protection" concept internally to achieve the level of protection required for the controller to reach a SIL3 safety rating. These layers consist of the traditional parts of the PLC each doing their increased functional safety task to insure that each can act independently and as a team to insure that faults are captured and pacified before they can cause harm. If we look at traditional PLCs and the accompanying safety relays in general terms they each function in basically the same way manner by Detection, Evaluation, and Response to the real world stimulus. The primary difference in these two systems has been the reliability requirements and use of control reliable design concepts to insure that critical control functions will be detected when they are required if not before.

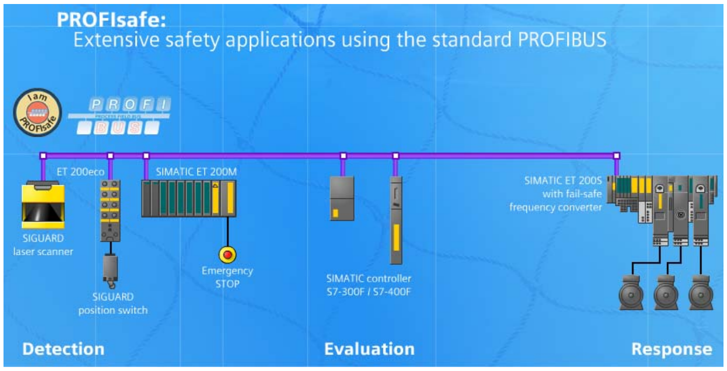




In simple terms Control Reliable is the use of redundant monitoring and control systems to insure that a single failure does not create a dangerous condition. In the control reliable Safety Relay these functions are compressed into one isolated location which creates a gap between their function and the communication to the machine operator. When we look at the Safety PLC we can clearly identify the control reliable functions of the safety relay in the various layers of the Safety PLC and see clearly the advantages from distributing communication to these functions around the machine. In addition we can see the added flexibility provided by being able to program the system reactions required while relying on the control reliable functions in each system layer to provide the functional safety requirements.



Traditional Safety Relay Function



Safety PLC integrates Simplified Safety via Yellow modules

The layers of protection in a Siemens safety PLC consist of the four parts, a failsafe input module, a safety rated network, a diverse logic processor and a failsafe output module.   These diverse layers work together in the safety PLC to provide protection previously available only in the Safety relays. By delivering this protection in a control architecture that is fully integrated in the automation PLC it simplifies the process of delivering the statuses of the safety system directly to the operator panel and provides the power and flexibility of the automation controller to solve the safety related control requirements.

The Layers of Protection function beyond the Application Program

The first layer of protection is in, the **failsafe Input module** that has taken the task of control reliable monitoring and protection. Typically all error handling was done inside the PLC, but in the safety PLC we have moved the error handling out to the input module for greater protection at the closes point to the safety input device. These modules divert to a safe shutdown mode (pacified) upon any detected failure independent of the PLC and do not rely on the PLC or the network for local error handling. These I/O modules performs functions previously only found in safety relays and seamless connect these functions into the automation controller. As listed below each Failsafe input module is relied upon to perform several tasks that insure safe inputs are correctly monitored:

- Monitored signal wire -- The input module has built in self testing. It generates test pulse signals that are used to insure valid monitoring of the input devices
- Intelligent modules provide local protection actions (lockout & reset)
- Discrepancy analysis and time out to insure reactions to faulty inputs
- Communication watchdog time out
- Error detection of communication telegrams to the safety PLC
- Category 3 & 4 requires redundant monitoring signals, so two inputs per device can be easily software configured to function together

The next layer encountered is the **safe communication network (PROFISafe)** that provides the reliability to insure that data passed between the layers arrives correctly to the proper partner and is properly interpreted. Amazing as it may seem due to the attention placed on the safety rated communication bus it actually accounts for less that 1% of the risk formula in the safety analysis. Key features of the safety rated bus are fault detection, fault reaction and recovery. A high speed cyclic reading bus like PROFIBUS provided several inherent features that made it a great candidate for the first choice of and open safety rated communication bus. By looking at the large data telegram size and the cyclic reading of all data it is easy to see that with features like sequence numbers and partner IDs that the data integrity is superior to a network design that relies simple on change of state to trigger communication. Total communication loss is easily detected with a time out function but lesser faults are handled by other mechanisms as shown in the diagram below.

Remedy Failure Type	Sequence Number	Time Out with Acknowledge	Identifier for Sender and	Data Consistency
Duplication	X			
Deletion	X	X		
Insertion	X	X	X	
Data out of	X			
Data				X
Delay		X		
Masquerade (standard message mimics failsafe)		X	X	X
FIFO failure in Router		X		

X - Indicates function that protects against this Fault type

The central layer of protection is the **safety rated Controller** which creates redundant evaluation of input and safety commands for outputs. In order to provide the extreme level of reliability required the controller is designed to detect single errors in the program execution and the electronic hardware as it executes the program logic. To achieve this in the safety-oriented program, the S7 Distributed Safety package performs automatic safety checks and links in additional redundant safety blocks for error recognition and handling. These control blocks create a level of time bounded diverse logic that continuously monitors for software errors and hardware faults.   When faults occur the corresponding reactions keep the safety system in a safe state or switch it to a safe state by either bringing the controller to a safe stop or sending shutdown signals to the other layers before allowing invalid program functions to affect the machine.

The final protection layer is the **failsafe Output module** which is an intelligent module and monitors its own redundant functions periodically to insure it will be capable of removing power when it is given a de-energize command. Like the failsafe input module this module provides local protection in case of any internal module fault or wiring fault that is detected. The module is at the end of the command react line and will only receive a command to energize its outputs if all the other layers have executed there functions error free and communicated the energize command to the output channel.

- No additional programming is required to get the category 4 ratings.
- The output module has a built in capability of testing itself. -- It generates test pulse signals internally that must be detected by the feedback monitoring of the channel or the module will shutdown locally and signal the CPU of a fault. This verifies that the card will be able to turn off loads when it is required.
- Category 3 & 4 devices require redundant signals, so two outputs switches are provided for each of these outputs. Both outputs must turn on successfully for the device to energize. If any one of these outputs fails, the remaining switch will be used to de-energize the operating device and the PLC will be notified.
- Each module has a safe state failure mode in case of communication failure. It does not rely on the PLC for error handling. Typically error handling for standard outputs is done at the PLC, but we have moved the error handling out to the card for greater protection. The I/O module performs functions previously done in safety relays therefore putting the safety protection at the closest point to the field device.

So when taken all together you can see that the probability of combination of failures creating an event that prevents a safety related output from being de-energized is extremely low. To put a number on this level of safety protection the probability of failure required to reach SIL 3 level in these high demand applications is approximately one dangerous failure in eleven centuries. These safety Layers described here function without the need for special programming by the application engineer so they can be relied upon to protect the same way each time they are applied as they in the other over one million times they have already been applied on other applications. Safety function no longer isolated from the controller Information allows better automation system reactions

User Benefits make the decision to use a Safety PLC even more Clear

Knowing that the safety functions are taken care of by the operating system on the Safety PLC the programmer can simply write the safety controls into ladder logic. Now you can simply take advantage of the many operational benefits available from the Siemens safety PLC system. A few of these benefits are listed below:

- Safety-related systems can be quickly configured with the simple addition of safety rated I/O module included in the standard I/O racks and a selection of the single CPU to controller the complete system
- Consistent handling of standard and safety functions allows fast troubleshooting of safety system problems thus significantly reducing downtimes.
- This extremely flexible topology provides the ability to place the Safety rated inputs and outputs wherever needed along the PROFIBUS networks

- Thanks to the integration of operational information and location data from all the safety related I/O the problems can be located quickly by the operator keeping service downtimes to a minimum.
- Safety and non-safety data on one bus, in one controller, and programmed with one engineering tool allows the optimum in seamless, integrated automation and safety solutions.
- Simple drag and drop graphical configuration provides easily configured safety related I/O and PLC programming in one straightforward software package. (Step7)
- The complete program including the safety and automation program in the S7 controller is easily moved to a replacement CPU in the case of faults without the need for

Integrated safety and standard control into the same PLC increases the friendliness of the system due to the common understanding of the maintenance personnel.

- Now the safety logic can be simply modified by making program changes in ladder logic the same as we are accustom to in the automation control program logic.