Chapter 20 Safety Programming in the PLC

Introduction

In engineering, redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe, or to improve actual system performance.

In many safety-critical systems, some parts of the control system may be triplicated, which is formally termed triple modular redundancy (TMR). An error in one component may then be out-voted by the other two. In a triply redundant system, the system has three sub components, all three of which must fail before the system fails. Since each one rarely fails, and the sub components are expected to fail independently, the probability of all three failing is calculated to be extraordinarily small; often outweighed by other risk factors, such as human error. Redundancy sometimes produces less, instead of greater reliability – it creates a more complex system which is prone to various issues, it may lead to human neglect of duty, and may lead to higher production demands which by overstressing the system may make it less safe.

What is the difference between fault-tolerant designs and fail-safe designs? A fault-tolerant system is designed to avoid total service failure caused by faults at any single point. Typically, a fault-tolerant design applies redundancy or multiple safety barriers to enable the system to continue its intended mission, possibly with reduced performance or increased response time in the event of some partial failure, rather than to fail completely. An example of a fault-tolerant design is an aircraft with multiple engines, so that it will keep flying even if one of the engines failed. A fail-safe system is designed to fail in a safe and controlled manner, so that the failure will not endanger lives or properties, or at least be no less safe than when it is operating correctly. For example, the brakes on a train are designed to apply when the brake control system fails, to ensure safety by stopping the train. It must be noted that a fail-safe system can also suffer 'wrong-side failure', as when, for example, a malfunctioning traffic light shows green rather than flashing red or goes dark; but is to have a very low probability of this occurring. In some cases, it may not be acceptable for one or even more failures to cause a system to cease functioning. Unlike a fail-safe system that puts safety ahead of function or mission objective, a 'failoperational' system will continue to operate in spite of control systems failure. An example is the thermostats in home air-conditioners.

PLC Systems use Fail-Safe Technology

Industrial automation is now considerably more flexible and open. Modern machines and systems also stand out due to their significantly increased productivity. This is due in no small part to the fact that relay technology has been replaced by the freely programmable controller and decentralization – at least for demanding applications. In spite of this change in technology, very different products and systems were often used until now for safety-oriented functions and standard tasks. If more complex safety tasks are involved, however, the efficiency of an automation solution can be significantly increased even if the safety technology consistently follows the trend toward intelligent PLCs.

A fail-safe PLC serves to control processes and immediately switches to a safer state or remains in the current state if a fault occurs. It provides an integrated, efficient safety solution in systems with increased safety requirements.

Programming is done in Siemens PLCs using the Step 7 languages LAD and FBD and TUV-certified (German Technical Inspectorate) function blocks. The connection to the standard and safety-oriented modules can be optionally made via PROFINET, the open Ethernet standard or via PROFIBUS.
The European guidelines apply today as those that reflect the highest safety standard and are accepted far beyond the boundaries of Europe. In order to ensure the functional safety of a machine or system, the safety-relevant parts of the protective and control systems behave in such a manner in the event of a fault that the system remains in a safe state or is put into a safe state. To this end, special requirements that are defined in standards are placed on the products. Corresponding product certificates can document the compliance with these standards.

Any possible hazards to people and the environment cannot just be averted at the national level. They must always comply with the regulations and rules of the location where the machine or system is operated. Thus the free exchange of goods within the framework of global markets requires internationally agreed codes of practice.

Safety requires protection against a variety of risks. These can be overcome as follows:

- Design in accordance with risk-reducing design principles and risk assessment of the machine
- Technical protection measures, if necessary by the use of safety-related controllers
- Electrical safety

Functional safety involves the part of the safety of a machine or plant that depends on the correct function of its control or protection equipment.

The analysis of risk follows a set procedure.

**BGIA is now IFA**

The name BGIA for years was associated with the German insurance industry responsible for setting up rules for plant safety or workplace safety. The new name reflects a change in social accident insurance.

The research institutes of the German Social Accident Insurance (DGUV) received new names and abbreviations. As of 1 January 2010, the former BGIA in Sankt Augustin is now be named the "Institute for Occupational Safety and Health of the German Social Accident Insurance", abbreviated as "IFA". Why look to Germany? They have traditionally led the way in quantifying safety in the workplace.

The Internet address of the institute changed accordingly:

As of 1 January 2010, the Institute for Occupational Safety and Health of the DGUV (IFA) is to be found at [www.dguv.de/ifa](http://www.dguv.de/ifa).

Application of the Machinery Directive 2006/42/EC [1] has been mandatory since 29 December 2009. The directive lists products that are described as "logic units to ensure safety functions". These products are stated in Annex IV of the Machinery Directive. This appendix lists products which owing to their function are a source of particularly high hazards in the event of a fault. Accordingly, stricter requirements apply to the conformity assessment method. The affected components and the possible assessment methods are stated below.

1 What products are described as "logic units to ensure safety functions"? Products are affected by this provision when:

   a) they are safety components (see below) and are therefore governed by the Machinery Directive; and
b) they are "logic units to ensure safety functions" in accordance with Annex IV, No. 21 (see below).

Concerning a): safety component in accordance with the Machinery Directive Article 1 of the Machinery Directive states its scope. The products considered here fall under c) safety components. In Sub-point c), Article 2 contains the definition of a safety component:

c) "safety component" means a component

• which serves to fulfil a safety function
• which is independently placed on the market,
• the failure and/or malfunction of which endangers the safety of persons, and
• which is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function.

If the above definition is applied for example to a safety PLC (Programmable Logic Controller), the following conclusion is reached: a safety PLC

• serves to fulfill a safety function
• is placed independently on the market, i.e. it is not supplied solely fitted to a machine
• endangers the safety of persons in the event of its failure and/or malfunction
• is not necessary for the machinery to function when used solely for the implementation of safety functions, or can be substituted by a conventional PLC for the purpose of the functioning of the machine, if non safety related functions are also performed.

Under the provisions of the Machinery Directive, a safety PLC is therefore classified as a safety component. As this example shows, the definition applies both to products which are employed solely for safety functions and to products which at the same time fulfill both safety functions and machine functions. An additional aid for determining whether a component is a safety component can be found in Annex V of the Machinery Directive. This contains a non-exhaustive list of safety components. Concerning b): logic units to ensure safety functions The background to the inclusion of these components in Annex IV is the growing use of functional safety products in machine controls. The Machinery Directive also lists the "logic units to ensure safety functions" in Annex V, but does not define these components. Clarification is provided by the "Guide to application of the Machinery Directive 2006/42/EG" [2]:

Logic units to ensure safety functions
In accordance with Annex IV of the Machinery Directive

On 29 December 2009, application of the new Machinery Directive, 2006/42/EC, becomes mandatory. One of the associated changes concerns "logic units to ensure safety functions". These are now referred to in Annex IV of the directive. This product group is not precisely defined, however. Owing to the reference to these products in Annex IV of the Machinery Directive, stricter requirements apply to the conformity assessment procedure for application of the CE mark.

For the purpose of defining logic units to ensure safety functions, the IFA has made an article available for download in which it classifies the components frequently employed in machine controls. The products concerned include safety PLCs (programmable logic controllers), power drive systems with integrated safety functions, safety switchgear, and any components for which the manufacturer states a Category, Performance Level or Safety Integrity Level. The classification of a component as a "logic
unit to ensure safety functions” constitutes an estimation made by the IFA in liaison with other German test bodies.

A risk is defined below:

<table>
<thead>
<tr>
<th>Risk related to the considered danger</th>
<th>Severity of the possible harm for the considered danger</th>
<th>and</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Probability of occurrence of that harm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency and duration of exposure</td>
</tr>
<tr>
<td>Probability of occurrence of the dangerous event</td>
</tr>
<tr>
<td>Possibility to avoid or limit the harm</td>
</tr>
</tbody>
</table>

A process to reduce risk is defined as:

Independent safety devices may be used in the design of a safety system. Two such devices are given below. The first is a safety relay. The second is a two-hand safety circuit. Both are stand-alone and are not to be incorporated in the PLC system other than as an add-on to an existing PLC system. They have been supplanted by the safety PLC with the function of these devices incorporated into the PLC itself after 2003 and the changes in standards permitting safety functions to be allowed inside the PLC.
Movement into Safety

Some years ago, I had a part-time job with a local machine builder. This individual provided all electrical control equipment except a program. That job was left to me. Most of the projects involved a press of some kind. They were slow and used pneumatic power to press the material for a car hood liner. All had two buttons to start the press. They were spaced far enough apart that the operator could not operate both with the same hand. Both hands had to be in a position away from the press far enough that they were safely out of the way of the movement of the press down.

In those early days, the buttons were programmed in the PLC. There was about a half second time delay allowed between the two buttons turning to initiate the press to start. Any delay beyond the half second would have not allow the press to begin.

Later, there was a device that handled this action with an output that allowed the PLC program to execute. The device was similar to the one below.

Since we have heard much from Siemens and Allen-Bradley in this text, we give time to another voice – Schneider – the French automation giant who is the owner of multiple PLCs including the original PLC – Modicon. The following, however, are not PLCs but rather discrete devices that pre-dated PLCs for safety functions:

**Schneider Electric XPSBF1132P**
SAFETY RELAY FOR TWO HAND CONTROL STATIONS, OUTPUT: 2; AUX: 2 SOLID STATE; 24VDC

Operating principle

Two-hand control stations are designed to provide protection against hand injury. They require machine operators to keep their hands clear of the hazardous movement zone. The use of two-hand control is an individual protective measure, which can safely protect only one operator. Separate two-hand control stations must be provided for each operator in a multiple-worker environment. Safety modules XPSBA, BC and BF for two-hand control stations comply with the requirements of European standard EN 574/ISO 13851 for two-hand control systems.

The control stations must be designed and installed such that they cannot be activated involuntarily or easily rendered inoperative. Depending on the application, the requirements of type C standards specific to the machinery involved must be met (additional personal protection methods may have to be considered).

To initiate a hazardous movement, both operators (two-hand control pushbuttons) must be activated within an interval of 0.5 s (synchronous activation). If one of the two pushbuttons is released during a hazardous operation, the control sequence is cancelled. Resumption of the hazardous operation is possible only if both pushbuttons are returned to their initial position and reactivated within the required time interval.

The control sequence does not occur if:

• Both two-hand control push buttons are pressed during a time period greater than 0.5 seconds,
• A short-circuit is present in a push button contact,
• The feedback loop is not closed at start-up.

The safety distance between the control units and the hazardous zone must be sufficient to ensure that when only one operator is released, the hazardous zone cannot be reached before the hazardous movement has been completed or stopped.

This device has been replaced in most applications by an instruction in the PLC, specifically a safety PLC with the safety instruction pre-approved for the purpose.
Legal requirements and standards regarding safety at work in North America

An essential difference between the legislation associated with safety at work between North America and Europe is the fact that in the US there is no standard legislation regarding machinery safety that addresses the responsibility of the manufacturer/supplier. There is a general requirement that the employer must provide a safe place of work.

US – general

The Occupational Safety and Health Act (OSHA) from 1970 is responsible in regulating the requirement for employers to ensure safe working conditions. The core requirements of OSHA are listed in Section 5 “Duties”:

(a) Each employer
   (1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;
   (2) shall comply with occupational safety and health standards promulgated under this Act.

The requirements from the OSH Act are administered and managed by the Occupational Safety and Health Administration. OSHA deploys regional inspectors who check whether workplaces fulfill the applicable regulations. The regulations, relevant for safety at work of the OSHA, are defined and described in OSHA 29 CFR 1910.xxx.

The following is stated at the beginning of the regulations for the Safety and Health Program:

(b)(1) What are the employer’s basic obligations under the rule? Each employer must set up a safety and health program to manage workplace safety and health to reduce injuries, illnesses and fatalities by systematically achieving compliance with OSHA standards and the General Duty Clause.

And later

(e) Hazard prevention and control

(e)(1) What is the employer’s basic obligation? The employer’s basic obligation is to systematically comply with the hazard prevention and control requirements of the General Duty Clause and OSHA standards.

(h)(6)(xvii)

Controls with internally stored programs (e.g., mechanical, electro-mechanical, or electronic) shall meet the requirements of paragraph (b)(13) of this section, and shall default to a predetermined safe condition in the event of any single failure within the system. Programmable controllers which meet the requirements for controls with internally stored programs stated above shall be permitted only if all logic elements affecting the safety system and point of operation safety are internally stored and protected in such a manner that they cannot be altered or manipulated by the user to an unsafe condition.

The OSHA regulations define minimum requirements to guarantee safe places of employment. However, they should not prevent employers from applying innovative methods and techniques, e.g. “state of the art protective systems” in order to maximize the safety of employees.

In conjunction with specific applications, OSHA specifies that all electrical equipment used to protect
employees, must be certified for the intended application by a nationally recognized testing laboratory (NRTL) authorized by OSHA. OSHA requires that all electrical products used by employees must be treated and approved for their intended use by an OSHA Approved Nationally Recognized Testing Laboratory.

NFPA 79

This Standard applies to the electrical equipment of industrial machines with rated voltages less than 600 V (a group of machines that operate together in a coordinated fashion is considered as a machine).

The comparison of European SIL and US Category (Cat) is shown below. Category 3 and 4 require safety equipment installed to protect employees.

The following gives a timeline of Siemens’ development of safety equipment. The most significant date here is 2003, the year NFPA70 allows safety PLCs in the US marketplace.
Next we have a lab using Safety PLC equipment. Siemens’ Reference Book on S7-1200 Safety can be found at:

- Industrial Software SIMATIC Safety - Configuring and Programming Manual (642 pgs)
- Safety Programming Guideline for SIMATIC S7-1200/1500 (48 pgs)
- Industrial Controls SIRIUS Safety Integrated Application Manual Application Manual (200 pgs)

This last manual has an example program similar to our lab with an outline of how to program and successfully implement the application. We are given a program complete and ready to go. All that is needed is to successfully wire the application. This may sound easy but in fact is not. The task still is difficult. When successful, the run light will turn on and the two relays will click ‘on’. This signifies the running of the motor which would be attached to the two relays in an industrial application.

Our Equipment includes:

- Siemens CPU 1214FC DC/DC/DC PLC
- Siemens SM 1226 F-DI DC Input Module
- Siemens SM 1226 F-DQ DC Output Module
- Two Siemens Sirius 3RH2122-2BB40 Relays
- An Emergency Stop Station

Since several non-safety Inputs and Outputs are used in the lab, we will use the pushbutton station from the lab, shown below:
The two figures below show the completed wiring job with the PLC ready to run the program.

Use the relays pictured at right instead of the ones above for the run relays. These relays have screw terminals instead of push terminals and are more secure with smaller wire. They also may be reused many more times. For a wiring diagram, refer to Chapter 2.
The relays to be removed are circled in the figure above.

Note:

“

**Sensor evaluation**

There are two types of sensor evaluation:

- **1001** evaluation – sensor signal is read once
- **1002** evaluation - sensor signal is read twice by the same → F-I/O and compared internally

“

Also, note that the two relays are extremely difficult to secure the wires in the terminals. You would be advised to substitute the relays from Ch. 2’s lab (24 VDC ones) instead.

It was noted that the use of timers in the fail-safe portion of the program was extremely burdensome on the time overhead of the system. Any use of timers should be limited. The solving of logic twice (once for positive logic and once for negative logic determines that with each tick of the timer, the logic must be evaluated again). That is a large over-head and should be avoided.

**Summary**

The chapter is a first try to define the type of safety needed in the factory. There is no need to provide the same equipment as is provided for a rocket to the moon – especially one carrying human cargo. However, equipment is to be safe and the need for safe PLCs has grown through the years.

The German BGIA approach is introduced. If one were to design a system especially for the European market, these documents would be essential. Moving the machine from Europe to the US will show
many of the techniques employed to meet the standards of the EU.

There is included a major lab demonstrating the implementation of the safe PLC by Siemens. The S7-1200 is used. GO FOR IT!

Questions

1. The following is a two-hand control station by Schneider Electric. Describe how this function has been moved into the PLC. Be specific.

   **Schneider Electric XPSBF1132P**

   SAFETY RELAY FOR TWO HAND CONTROL STATIONS, OUTPUT: 2; AUX: 2 SOLID STATE; 24VDC

2. The following describes how an input, logic and output interacts in a safety circuit for Siemens. Describe how logic can be guaranteed to be safe in this configuration. In your answer describe both logic written by the user and logic approved and provided by the manufacturer.

![Diagram](image)

3. There was a chart comparing Categories (Cat) with SIL values. Show the comparisons between the two and show where fail-safe is required.

   At what level is the power-supply incorporated into the safety hardware?

4. If you were to walk up to a Siemens PLC or an Allen-Bradley PLC, what would give you an indication where the safety I/O is housed? Give an example of each:

Ch 20 Safety Programming in the PLC 12
5. What is Stuxnet?

From Wikipedia, the following:

**Stuxnet** is a malicious computer worm, first uncovered in 2010 by Kaspersky Lab. Thought to have been in development since at least 2005, Stuxnet targets SCADA systems and was responsible for causing substantial damage to Iran's nuclear program. Although neither country has openly admitted responsibility, the worm is believed to be a jointly built American/Israeli cyberweapon.⁷

Stuxnet specifically targets programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material. Exploiting four zero-day flaws,⁴ Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart.⁶ Stuxnet's design and architecture are not domain-specific and it could be tailored as a platform for attacking modern supervisory control and data acquisition (SCADA) and PLC systems (e.g., in factory assembly lines or power plants), the majority of which reside in Europe, Japan and the US.⁸ Stuxnet reportedly ruined almost one fifth of Iran's nuclear centrifuges.⁹ Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade.⁶