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:

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 ≤ 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.
Choose: What is a safety PLC Part 3 of 4 series
In the Video there is a description of the KCPL Explosion. The Vendor referenced was A-B with a description that follows:

"KCP&L wins $135 million judgment"

Kansas City, Mo. ? A jury has determined a Milwaukee parts manufacturer should pay more than $135 million in damages related to a 1999 gas explosion that destroyed a Kansas City Power & Light Co. plant.

A spokesman for Allen-Bradley Corp. said the company was disappointed with Friday’s verdict and said it would appeal. Allen-Bradley recently became part of Rockwell Automation Inc. in Milwaukee.

Jurors in Jackson County assessed damages at $452 million, and found KCP&L was liable for 70 percent.

Tom Robinson, a spokesman for KCP&L, said the utility was “gratified the jury recognized we should receive compensation.”

The explosion at KCP&L’s Hawthorn 5 plant on Feb. 17, 1999, left it out of operation for 838 days. The utility claimed a loss of $552 million for rebuilding the plant, lost business and other expenses.

KCP&L blamed what it called defective computer safety equipment, but Allen-Bradley blamed the utility and wastewater that leaked into the equipment.

“They both had to be at fault,” jury foreman Bob Palmer said.

KCP&L said it did not cause the explosion. It blamed an errant Allen-Bradley guidebook for installing switching equipment that malfunctioned and opened the gas line, which caused the explosion.

Allen-Bradley contended a short circuit from sewer water caused the malfunction that opened the gas line. It blamed the sewer problem and poorly trained KCP&L technicians who repaired the damage.

KCP&L asked jurors to place a value of $621 million on damage that included the cost of rebuilding and lost income and to find Allen-Bradley negligent for much of that.

Allen-Bradley contended that number should be only $130.6 million and all blame should be on KCP&L.
The local report from the Kansas City Star follows:

“Fire, Explosion at KCP&L’s Hawthorn Power Plant

By MALCOLM GARCIA - The Kansas City Star Date: 05/23/00 01:09

Firefighters from Kansas City and area departments were cautiously trying to put out a fire at KCP&L's Hawthorn plant in the East Bottoms early this morning.

Area fire departments were brought in to try to put the fire out with foam. Firefighters were being careful in how they approached the fire because of concern about explosions.

The cause of the fire was not known early this morning. No injuries had been reported.

The fire caused a brief outage across the city after 11 p.m. Monday. The outage was a result of the load being shifted from the 345,000-volt transformer to other areas of the transformation system to maintain power in the area, said Tom Robinson, a Kansas City Power & Light spokesman.

Johny Teegarden, an iron worker at the plant, was leaving to get something to eat when he heard the explosion.

"We heard a big boom and saw a big flash, and then a bunch of little fires," he said. "By the time we got out of the plant that fire was burning good."

In February 1999, the complex near Front Street and Interstate 435 was rocked by a boiler explosion.

That late-night explosion woke people 20 miles away, knocked nearby workers off their feet and launched flames 200 feet into the night sky. The explosion was caused by a buildup of natural gas used to start the plant's boiler. One minor injury was reported.

That part of the plant, which is still not functioning, was one of KCP&L's main generating plants.

KCP&L decided to rebuild the plant, which accounted for 15 percent of the utility's capacity to generate electricity. The plant is scheduled to resume operation in summer 2001.

All content ) 2000 The Kansas City Star”
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.
To better step through the process of setting up a Safety System from scratch, the lab in Lab Text Ch. 26 provides a complete wiring diagram of the project at UToledo. The following button layout shows the actual buttons used and their function. In the example from Siemens, there are a number of local switches from external devices. We provided substitutes for these switches with simple pushbuttons labelled appropriately.

Note that the referenced Red PB, Blue PB and Green PB are not actually these colors but are labelled as such in the program. The button colors for all three are yellow.
The following is a troubleshooting page to be used if there is an error in the wiring or configuration of the program:

The figures that follow are the program listing for the programs as well as the configuration pages of the various OB’s and FB’s:

First, OB1:

<table>
<thead>
<tr>
<th>Name</th>
<th>Data type</th>
<th>Default value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial_Call</td>
<td>Bool</td>
<td></td>
<td>Initial call of this OB</td>
</tr>
<tr>
<td>Remanence</td>
<td>Bool</td>
<td></td>
<td>True, if remanent data are available</td>
</tr>
</tbody>
</table>

Network 1:

```
SafetyReference
```

Network 2:

```
SafetyReference
```

Ch 20 Safety Programming in the PLC 17
## Safety Programming in the PLC

<table>
<thead>
<tr>
<th>Local/ESTopStatus</th>
<th>ESTOP1</th>
<th>True</th>
<th>True</th>
<th>True</th>
<th>True</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E_STOP</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>ACK_NEC</td>
<td>Bool</td>
<td>true</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>ACK</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>TIME_DEL</td>
<td>Time</td>
<td>0</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Q_DELAY</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>ACK_REQ</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>DIAG</td>
<td>Byte</td>
<td>811640</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Q_DELAY</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>ACK_REQ</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>DIAG</td>
<td>Byte</td>
<td>811640</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td><strong>Static</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote/ESTopStatus</td>
<td>ESTOP1</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E_STOP</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>ACK_NEC</td>
<td>Bool</td>
<td>true</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>ACK</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>TIME_DEL</td>
<td>Time</td>
<td>0</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Q_DELAY</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>ACK_REQ</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>DIAG</td>
<td>Byte</td>
<td>811640</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td><strong>Static</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contactor/Output</td>
<td>F0BACK</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ON</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>FEEDBACK</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

**Table: Data Attributes**

<table>
<thead>
<tr>
<th>Name</th>
<th>Data type</th>
<th>Default value</th>
<th>Retain</th>
<th>Accessible from HMI/OPC UA/Web API</th>
<th>Writable from HMI/OPC UA/Web API</th>
<th>Visible in Engineering</th>
<th>Setpoint</th>
<th>Supervision</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>QBAD_1X0</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>1=QBAD signal of I/O channel of output Q</td>
</tr>
<tr>
<td>ACK_NEC</td>
<td>Bool</td>
<td>true</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>1=Acknowledgment necessary</td>
</tr>
<tr>
<td>ACK</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>1=Acknowledgment</td>
</tr>
<tr>
<td>FDB_TIME</td>
<td>Time</td>
<td>2Wms</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>Feedback time</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>Output</td>
</tr>
<tr>
<td>ERROR</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>Feedback error</td>
</tr>
<tr>
<td>ACK_REQ</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>1=acknowledgment request</td>
</tr>
<tr>
<td>DIAG</td>
<td>Byte</td>
<td>811640</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>Service information</td>
</tr>
<tr>
<td><strong>Static</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contactor/Output</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LockingSwitch_SS_Status</td>
<td>ESTOP1</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E_STOP</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>Emergency STOP</td>
</tr>
<tr>
<td>ACK_NEC</td>
<td>Bool</td>
<td>true</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>1=Acknowledgment necessary</td>
</tr>
<tr>
<td>ACK</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>1=Acknowledgment</td>
</tr>
<tr>
<td>TIME_DEL</td>
<td>Time</td>
<td>0</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>Time delay</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>1=Enable</td>
</tr>
<tr>
<td>Q_DELAY</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>Enable is OFF delayed</td>
</tr>
<tr>
<td>ACK_REQ</td>
<td>Bool</td>
<td>false</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>1=acknowledgment request</td>
</tr>
<tr>
<td>DIAG</td>
<td>Byte</td>
<td>811640</td>
<td>Non-retain</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>Service information</td>
</tr>
<tr>
<td><strong>Static</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temp</td>
<td>Constant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ch 20 Safety Programming in the PLC
### Program blocks

#### Main_Safety_RTG1_DB [DB1]

<table>
<thead>
<tr>
<th>Name</th>
<th>Data type</th>
<th>Start value</th>
<th>Retain</th>
<th>Accessible from HMI/OPC UA/Web API</th>
<th>Visible in HMI engineering</th>
<th>Setpoint Supervision</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>InOut</td>
<td></td>
<td></td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td><strong>ACK_GI_Instance</strong></td>
<td>ACK_GI</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=acknowledgment for reintegration</td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td></td>
<td></td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>ACK_GI_INST</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=acknowledgment necessary</td>
</tr>
<tr>
<td>ACK</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Time delay</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td></td>
<td></td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=enable</td>
</tr>
<tr>
<td>Q_DELAY</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Stop enable</td>
</tr>
<tr>
<td>ACK_REQ</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=acknowledgment request</td>
</tr>
<tr>
<td>DIAG</td>
<td>Byte</td>
<td>B16400</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Service information</td>
</tr>
<tr>
<td><strong>Static</strong></td>
<td></td>
<td></td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td><strong>GuardStatus</strong></td>
<td>ESTOP1</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td></td>
<td></td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=acknowledgment necessary</td>
</tr>
<tr>
<td>E_STOP</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Emergency STOP</td>
</tr>
<tr>
<td>ACK_GI_INST</td>
<td>Bool</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Time delay</td>
</tr>
<tr>
<td>ACK</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=acknowledgment</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td></td>
<td></td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=enable</td>
</tr>
<tr>
<td>Q_DELAY</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Enable is OFF delayed</td>
</tr>
<tr>
<td>ACK_REQ</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=acknowledgment request</td>
</tr>
<tr>
<td>DIAG</td>
<td>Byte</td>
<td>B16400</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Service information</td>
</tr>
<tr>
<td><strong>Static</strong></td>
<td></td>
<td></td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td><strong>RemoteEstopStatus</strong></td>
<td>ESTOP1</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td></td>
<td></td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=acknowledgment necessary</td>
</tr>
<tr>
<td>E_STOP</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Emergency STOP</td>
</tr>
<tr>
<td>ACK_GI_INST</td>
<td>Bool</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Time delay</td>
</tr>
<tr>
<td>ACK</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=acknowledgment</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td></td>
<td></td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=enable</td>
</tr>
<tr>
<td>Q_DELAY</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Enable is OFF delayed</td>
</tr>
<tr>
<td>ACK_REQ</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=acknowledgment request</td>
</tr>
<tr>
<td>DIAG</td>
<td>Byte</td>
<td>B16400</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Service information</td>
</tr>
<tr>
<td><strong>Static</strong></td>
<td></td>
<td></td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td><strong>Contacts</strong></td>
<td>FEEDBACK</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td></td>
<td></td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=enable output</td>
</tr>
<tr>
<td>ON</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>Feedback input</td>
</tr>
<tr>
<td>FEEDBACK</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>QBAD channel of output</td>
</tr>
<tr>
<td>ACK_GI_INST</td>
<td>Bool</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>1=acknowledgment necessary</td>
</tr>
</tbody>
</table>
### Ch 20 Safety Programming in the PLC

<table>
<thead>
<tr>
<th>Name</th>
<th>Data type</th>
<th>Start value</th>
<th>Retain</th>
<th>Accessible from HMIVOPC UA/Web API</th>
<th>Visible in HM/engi-neering</th>
<th>Setpoint</th>
<th>Supervision</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACK</td>
<td>Bool</td>
<td>false</td>
<td></td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>false</td>
<td>Acknowledgment</td>
</tr>
<tr>
<td>FDB_TIME</td>
<td>Time</td>
<td>D:100000</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>Feedback time</td>
</tr>
<tr>
<td>Q</td>
<td>Bool</td>
<td>false</td>
<td></td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>false</td>
<td>Feedback error</td>
</tr>
<tr>
<td>ERRDR</td>
<td>Bool</td>
<td>false</td>
<td></td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>False</td>
</tr>
<tr>
<td>ACK_REQ</td>
<td>Bool</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>I=acknowledgment request</td>
</tr>
<tr>
<td>DIAG</td>
<td>Byte</td>
<td>8100600</td>
<td>true</td>
<td>true</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>Service information</td>
</tr>
<tr>
<td>Latching</td>
<td>Bool</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>False</td>
</tr>
<tr>
<td>Locking</td>
<td>Bool</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>Service information</td>
</tr>
</tbody>
</table>

### Program blocks

#### SafetyDataExchange [DB3]

**General**

<table>
<thead>
<tr>
<th>Name</th>
<th>Number</th>
<th>Type</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafetyDataExchange</td>
<td>3</td>
<td>DB</td>
<td>DB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Data type</th>
<th>Start value</th>
<th>Retain</th>
<th>Accessible from HMIVOPC UA/WebAPI</th>
<th>Visible in HM/engi-neering</th>
<th>Setpoint</th>
<th>Supervision</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlobalACK_REQ</td>
<td>Bool</td>
<td>false</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>False</td>
</tr>
<tr>
<td>GlobalSafeOK</td>
<td>Bool</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>False</td>
</tr>
<tr>
<td>LocalStepOK</td>
<td>Bool</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>False</td>
</tr>
<tr>
<td>RemoteStepOK</td>
<td>Bool</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>False</td>
</tr>
</tbody>
</table>
### Program blocks / System blocks / STEP 7 Safety

#### F_Systeminfo_DB [DB30001]

<table>
<thead>
<tr>
<th>Name</th>
<th>Data type</th>
<th>Start value</th>
<th>Retain</th>
<th>Accessible from HMI/OPC/UA/Web API</th>
<th>Writable from HMI Engineering</th>
<th>Visible in HMI Engineering</th>
<th>Setpoint Supervision</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCValue</td>
<td>DWord</td>
<td>1640</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
</tbody>
</table>

#### RTG1Sysinfo [DB30000]

<table>
<thead>
<tr>
<th>Name</th>
<th>Data type</th>
<th>Start value</th>
<th>Retain</th>
<th>Accessible from HMI/OPC/UA/Web API</th>
<th>Writable from HMI Engineering</th>
<th>Visible in HMI Engineering</th>
<th>Setpoint Supervision</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODE</td>
<td>Bool</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>F_SYSINFO</td>
<td>Bool</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>TOYC_CURR</td>
<td>UInt</td>
<td>0</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>TOYC_LONG</td>
<td>UInt</td>
<td>0</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>TRTG_LONG</td>
<td>UInt</td>
<td>0</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>TRTG_CURR</td>
<td>UInt</td>
<td>0</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>F_PRG_SIG</td>
<td>DWord</td>
<td>DWA16#284F015</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>F_PRG_DAT</td>
<td>DTL</td>
<td>DTL#2021-6-19-20:26:30.8</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>YEAR</td>
<td>UInt</td>
<td>2021</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>MONTH</td>
<td>UInt</td>
<td>4</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>DAY</td>
<td>UInt</td>
<td>1</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>WEEKDAY</td>
<td>UInt</td>
<td>5</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>HOUR</td>
<td>UInt</td>
<td>19</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>MINUTE</td>
<td>UInt</td>
<td>20</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>SECOND</td>
<td>UInt</td>
<td>20</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>S0000200</td>
<td>UInt</td>
<td>0</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>F_RTO_SIG</td>
<td>DWord</td>
<td>DWA16#1F90059E</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>F_RTO_DAT</td>
<td>DTL</td>
<td>DTL#2021-6-19-20:26:30.8</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>YEAR</td>
<td>UInt</td>
<td>2021</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>MONTH</td>
<td>UInt</td>
<td>4</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>DAY</td>
<td>UInt</td>
<td>1</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>WEEKDAY</td>
<td>UInt</td>
<td>5</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>HOUR</td>
<td>UInt</td>
<td>19</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>MINUTE</td>
<td>UInt</td>
<td>20</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>SECOND</td>
<td>UInt</td>
<td>20</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>S0000200</td>
<td>UInt</td>
<td>0</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>VERS_SAF</td>
<td>DWord</td>
<td>DWA16#16000000</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
</tbody>
</table>

Ch 20 Safety Programming in the PLC  24
To better understand the above configuration and program, turn to the following Siemens Manual:

**SIEMENS**

**SIMATIC**

**S7**

**S7-1200 Functional Safety Manual**

Equipment Manual

V4.6, 11/2022
A5E03470344-AC

This manual steps through a number of videos showing the complete configuration of a system similar to the one outlined in the lab and above.
In this manual are found a number of informational websites. The first gives information for overall maintenance of the safety system in a plant:

```
Note
Important note for maintaining operational safety of your plant

Plants with safety-related features are subject to special operational safety requirements on the part of the operator. Even suppliers are required to observe special measures during product monitoring. For this reason, we inform you in the form of personal notifications about product developments and features that are (or could be) relevant to operation of systems from a safety perspective.

By subscribing to the appropriate notifications, you will ensure that you are always up-to-date and able to make changes to your system, when necessary.

Log onto Industry Online Support. Go to the following links and, on the side, right click on "email on update":

- SIMATIC S7-300/S7-300F (https://support.industry.siemens.com/cs/ww/en/p/13751)
- SIMATIC S7-400/S7-400H/S7-400F/FH (https://support.industry.siemens.com/cs/ww/en/p/13828)
- SIMATIC WinAC RTX (F) (https://support.industry.siemens.com/cs/products?mfn=ps&pnid=13917&lc=en-WW)
- Distributed I/O (https://support.industry.siemens.com/cs/ww/en/p/14029)
```
The next shares information concerning various manuals involved in PLC programming of the Safety System:

"" Documentation and information

S7-1200 and STEP 7 provide a variety of documentation and other resources for finding the technical information that you require.

- The S7-1200 Functional Safety Manual presents an overview of the Siemens Safety software and fail-safe CPUs and signal modules (SMs) and a Getting Started configuration and programming example. However, the focus of the manual is the S7-1200 fail-safe SMs. SM installation, configuration, diagnostics, applications, and technical specifications are emphasized.

The English version of the S7-1200 Functional Safety Manual is the authoritative (original) language for Functional Safety-related information. All translated manuals refer back to the English manual as the authoritative and original source. Siemens identifies the English manual as the authoritative and original source in the case of discrepancies between the translated manuals.

- The SIMATIC Safety - Configuring and Programming, Programming and Operating Manual provides information that enables you to configure and program SIMATIC Safety fail-safe systems. In addition, you will obtain information on acceptance testing of a SIMATIC Safety fail-safe system. Before configuring and programming an actual live fail-safe operation, it is essential that you refer to this manual.

- The S7-1200 Programmable Controller System Manual provides specific information about the operation, programming, and the specifications for the complete S7-1200 product family. In addition to the system manual, the S7-1200 Easy Book provides a more general overview to the capabilities of the S7-1200 family.

- The S7-1200 Functional Safety Manual: SIMATIC Safety - Configuring and Programming, Programming and Operating Manual; S7-1200 Programmable Controller System Manual; and the S7-1200 Easy Book are available as electronic (PDF) manuals. You can download or view the electronic manuals from the Siemens Industry Online Support Web site (http://support.industry.siemens.com). These manuals are also available on the Documents Disk that ships with every S7-1200 CPU.

- The STEP 7 (TIA portal) online help information system provides immediate access to the conceptual information, specific instructions, and error code event IDs that describe the operation and functionality of the programming package and basic operation of SIMATIC CPUs.

- The Siemens Industry Online Support Web site (http://support.industry.siemens.com) provides access to the electronic (PDF) versions of the SIMATIC documentation set. Existing documents are available from the Product Support link. With this online documentation access, you can also drag and drop topics from various documents to create your own custom manual.

You can access online documentation by clicking "mySupport" from the left side of the page and selecting "Documentation" from the navigation choices. To use the mySupport Documentation features, you must sign up as a registered user.

- Siemens also provides online comprehensive support for your use of safety technology. A Safety Evaluation Tool assists you in determining required safety levels, Functional Examples guide you in your safety applications, and Siemens training (SITRAIN) classes offer training in safety standards and products. Visit the following web sites to access these support activities:
  - Safety Evaluation Tool (http://www.siemens.com/safety-evaluation-tool)
  - Functional examples (http://www.siemens.com/safety-functional-examples)
  - SITRAIN (http://www.siemens.com/sitrain-safetyintegrated)""
Also shared in the beginning pages of this manual are the instructional videos prepared for stepping through the configuration process along with full explanations in the manual itself:

"2.1.1 Instructional videos

The "Getting Started" chapter contains eleven instructional videos. Nine instructional videos take you step-by-step through many of the configuring and programming tasks. These instructional videos show the completed task at the beginning of the video, with a fadeout to a step-by-step tutorial that demonstrates all of the required sub-tasks:

- "Procedure" (Page 29) (shows a wiring overview of the S7-1200 Fail-Safe application example)
- "Step 1: Configuring the S7-1200 CPU 1212FC, CPU 1214FC, or CPU 1215FC" (Page 32) (step-by-step tutorial)
- "Step 6: Creating an F-FB" (Page 51) (step-by-step tutorial)
- "Step 7: Programming the safety door function" (Page 52) (step-by-step tutorial)
- "Step 8: Programming the emergency stop function" (Page 54) (step-by-step tutorial)
- "Step 9: Programming the feedback monitoring" (Page 56) (step-by-step tutorial)
- "Step 10: Programming the user acknowledgment for reintegration of the fail-safe SM" (Page 58) (step-by-step tutorial)
- "Step 11: Programming of the main safety block" (Page 59) (step-by-step tutorial)
- "Step 12: Compiling the safety program" (Page 60) (step-by-step tutorial)
- "Step 13: Downloading the complete safety program to the fail-safe CPU and activating safety mode" (Page 61) (step-by-step tutorial)
- "Step 13: Downloading the complete safety program to the fail-safe CPU and activating safety mode" (Page 61) (second video; shows the end result of the LAD programming steps)

This documentation gives a very good start to mastering the safety systems from Siemens. The goal is to understand a system well enough to start one up. That first system can be the one in the lab."
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.
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:

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.\(^1\)

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,\(^2\) 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.\(^3\) 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.\(^4\) Stuxnet reportedly ruined almost one fifth of Iran's nuclear centrifuges.\(^5\) Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade.\(^6\)“
Appendix A

Safety Lab taken from Vendor Presentation – Slides Only

How to Integrate a Safety PLC – S7-1215F (must change to 1214F for UToldeo Lab Exercise)

5. TIA Portal: Hardware configuration

1. Create a new project
2. Name the project “Safety Wiring Demo”
3. Store the project in the \Student\Trainee folder on the desktop.
4. Press “Create”
5. TIA Portal: Hardware configuration

1. Add a new device
2. Leave Device Name as default “PLC_1”
3. Select “Controllers”
4. Highlight CPU S12/HPCDCDC/DCC, 46217215-1Z-F40-FX08
5. Verify Part Number and Firmware (Note: You will need to change this from the default V4.4) – ask your instructor why
6. Select “Open Device View”
7. Click “Add”

5. TIA Portal: Hardware configuration

1. Highlight the CPU in the workspace
2. Using the Inspector Window, Select “Properties”, “General”
3. Highlight the “Startup” property
4. Change the properties as shown:
   1. Warm restart – Run
   2. Startup CPU event mismatch

5. TIA Portal: Hardware configuration

1. Highlight “System and clock memory”
2. Enable “System memory bits” & “Clock memory bits”

Note: System and Clock memory can be used for non-safe programs only.
5. TIA Portal: Hardware configuration – Technical Info

- From S7-1500 System Manual, 12/2017 (A5E03481192-AE), Chapter 8.2.
  **Note**
  **Communication**
  The communication (e.g. test functions with the PG) always works with priority 15. To prevent extending the program runtime unnecessarily in time-critical applications, these OBs should not be interrupted by communication. Assign a priority > 15 for these OBs.
- Per Siemens Hotline, for S7-1200F, communication has the same priority class as OB1.
- From SIMATIC Safety - Configuring and Programming Manual, 03/2017 (A5E02714440-AF), Chapter 5.2.1.
  (S7-1200, S7-1500). The F-OB should be created with the highest priority of all OBs.

**Conclusion:**
For S7-1200F, F-OB priority should be set to >=9.
For S7-1500F, F-OB priority should be set to >=16.

---

5. TIA Portal: Hardware configuration

1. Double-click “Safety Administration” in the project tree
2. Under F-OB time group 1 (RTG1), change Priority = 15
   **Note:** This is optional for the S7-1200

---

5. TIA Portal: Hardware configuration

1. Highlight “PLC_1” in the project tree
2. Press the Compile button in the toolbar
3. Save the project
5. TIA Portal: Hardware configuration

1. Select the “Libraries” tab from the Task Card
2. Expand “Global libraries”
3. Drag “1200F Wiring Tags” from the Master Copy folder of “1200F Wiring” folder to the “PLC tags” folder of PLC_1
   
   *Note:* We are using the using a library element to save time when typing in the Tags that will be used in this lab.
   
   *Note:* Each tag will be verified in the following steps

5. TIA Portal: Hardware configuration

1. Open the “Device Configuration” for PLC_1
2. Select “Hardware catalog” from the Task Card
3. Drag F-DI (6ES7229-1DA32-0XB0) into Slot 2 of the PLC.
4. Drag F-DQ (6ES7226-6DA32-0XB0) into Slot 3 of the PLC.

5. TIA Portal: Hardware configuration

1. Highlight the PLC in Slot 1
2. Using the Inspector Window, Select “Properties” “I/O Tags”
3. Verify the following tags
   1. 10.0 – RFID Switch Status
   2. 11.5 – Contactoff feedback
   3. Q1.9 – Local/StepLED

   *Note:* It is important to make sure you’re adding the tags to the appropriate address, as this is the way we wired the module.
6. TIA Portal: Hardware configuration

1. Highlight the F-Di in Slot 2
2. Using the Inspector Window, Select “Properties”, “General”
3. Select “DI parameters”
4. Enable the “Short-circuit test”

6. TIA Portal: Hardware configuration

1. Select “Channel parameters”, “Channel 0.8”
2. Make the following changes:
   1. Sensor evaluation – 1oo2 evaluation
   2. Discrepancy time – 250ms
   3. Sensor supply - Internal

Sensor evaluation

There are two types of sensor evaluation:

- 1oo1 evaluation – sensor signal is read once
- 1oo2 evaluation - sensor signal is read twice by the same → F-I/O and compared internally
5. TIA Portal: Hardware configuration

1. Select "Channel parameters", "Channel 1, 9"
2. Make the following Changes:
   1. Sensor evaluation – 1en2 evaluation
   2. Discrepancy time – 50ms

5. TIA Portal: Hardware configuration

1. Select "Channel parameters", "Channel 2, 10"
2. Make the following Changes:
   1. Channel 2 – Uncheck "Activated"
   2. Channel 10 – Uncheck "Activated"
   3. Deactivate the rest of the channels on this module

5. TIA Portal: Hardware configuration

1. Using the inspector window, select "IO Tags"
2. Verify the following tags:
   1. I8.0 – Local Estop
   2. I8.1 – Guard Switch
   3. I10.0 – Value Status _Local Estop
   4. I10.1 – Value Status _Guard Switch

Note: The Value Status inputs provide information on the validity of the corresponding channel value.
5. TIA Portal: Hardware configuration

1. Highlight the F-DQ in Slot 3.
2. Using the Inspector Window, Select “Properties”, “General”
3. Select “DO parameters”, “Channel 0”
4. Uncheck the “Activated”

5. TIA Portal: Hardware configuration

1. Using the Inspector Window, Select “IO Tags”
2. Verify the following tags:
   1. Q17.1 – GuardedLED
   2. Q17.2 – ContactorLeft
   3. Q17.3 – ContactorRight
   4. N17.1 – ValueStatus_GuardedLED
   5. N17.2 – ValueStatus_ContactorLeft
   6. N17.3 – ValueStatus_ContactorRight

   Note: The Value Status Inputs provide information on the validity of the corresponding channel value.

6. TIA Portal: Software programming

1. Right-click on “Main_Safety_RTG(FB1) program block”
2. Select “Properties…”
3. Change the programming language to “LAD”
4. Press “OK”

   Note: The default programming language is FB, we will be working with LAD.
6. TIA Portal: Software programming

1. Double click "blen_Safety_RTC1/FB11" for editing.
2. Drag the "ACK_GL" block from the "Safety functions" folder of "Basic instructions" to Network 1.
3. When the window appears, select "Multi-Instance".
4. Leave Instance Data name as default.
5. Press "OK".

6. TIA Portal: Software programming

1. Using the favorites bar, add the logic as shown.

7. TIA Portal: Software programming

1. Using the favorites bar, add the logic as shown.

Note: Each Safety Module KO0 Point provides a "Value Status" which shows if the module is OK and has not "Fast shared" or gone to a Safe State. The Profinet Pushbutton station provides a "QBAD" bit.
6. **TIA Portal: Software programming**

1. Drag "ESTOP1" from the Safety Functions Folder and place it on Network 3 as shown.
2. Fill in tags as shown.
   - **Note:** Be sure to use the Multi-Instance option for the Instance Data when prompted during insertion. Define the Variable as "LocalEstopStatus".

---

6. **TIA Portal: Software programming**

1. Drag "ESTOP1" from the Safety Functions Folder and place it on Network 4 as shown.
2. Fill in tags as shown.
   - **Note:** Be sure to use the Multi-Instance option for the Instance Data when prompted during insertion. Define the Variable as "GuardStatus".

---

6. **TIA Portal: Software programming**

1. Drag "ESTOP1" from the Safety Functions Folder and place it on Network 4 as shown.
2. Fill in tags as shown.
   - **Note:** Be sure to use the Multi-Instance option for the Instance Data when prompted during insertion. Define the Variable as "GuardStatus".
8. TIA Portal: Software programming

1. Drag “FDBACK” from the Safety Functions Folder and place it on Network 6 as shown.
2. Fill in tags as shown. (Be sure to change the FDB_Time = 600ms)

Note: Be sure to use the Multi-Instance option for the Instance Data when prompted during insertion the FDBACK block. Define the Variable as “Contactor”.

Note: We are adding a new variable, “Contactor Output”, we will define it on the next slide.

Note: Be sure to add the Feedback Time input to the block.

---

9. TIA Portal: Software programming

1. Right-click on the “Contactor Output” variable and select “Define tag…”
2. Change the Section to “Local Static” press “Define”

Note: By using local static memory, this bit is stored with the Instance Data for this FB, but is available globally if needed.

---

10. TIA Portal: Software programming

1. Return to Network #2 and add logic as shown
   a. #Contactors ERROR
6. TIA Portal: Software programming

1. Using the Favorites Bar, add the logic as shown on Network 7

Safety data transfer to non-safe DB

Advantages of using Data-coupling DB:
- Lean runtime group
- Better overview of the exchanged data
- Changes in the diagnostic and signaling context in the standard user program do not affect the safety program’s signature
- Minimal risk of downtimes caused by data corruption due to write access to the safety program
- Simplified usage of F-works
- Changes to the standard user program can be loaded without stopping the CPU
- Standard user program and safety program can be created independently of each other, provided that interfaces have already been defined

Refer to S7-1200F/1500F programming guideline:
https://support.industry.siemens.com/cs/en/view/109752255

Note: We are placing multiple Rungs in one Network.
Note: This Network will transfer the Safety Data to the Non-Safety Data Block.
6. TIA Portal: Software programming

1. Using the Favorites Bar, add the logic as shown on Network 9
2. Highlight PLC_1 in the project tree
3. Press the Compile button in the Toolbar
4. Save the project

Note: This Network will transfer the Safety Data to the Non-Safety Data Block.
Note: Safety Program is complete

---

6. TIA Portal: Software programming

1. Double-click on "Main (OB1)" in the Program blocks folder to open for editing
2. Add the logic shown for Networks 1, 2, 3

Note: The "NOT" instruction can be found in the Bit logic operations folder of the Instructions Task Card.

---

6. TIA Portal: Software programming

1. Add the logic shown for Networks 4 & 5
2. Highlight PLC_1 in the project tree
3. Press the Compile button in the Toolbar
4. Save the project
7. Commissioning and Testing

1. Highlight PLC in the project tree
2. Press the Download button in the Toolbar
3. When the Extended download window appears, set IP address interface as shown
4. Press “Start search”
5. Highlight S7-1200 in the list (Note: this PLC was factory reset and does not have an assigned IP address)
6. Press “Load”

7. Commissioning and Testing

1. Change Start modules to “Start Module”
2. Press “Finish”

Note: The PLC will show a fault because we have not commissioned the Profinet Push button station.

7. Commissioning and Testing

1. Press “Load”
7. Commissioning and Testing

1. Double-click on "Devices & Networks."
2. Right-click on the Command_Signal Graphic.
3. Click "Assign device name."

7. Commissioning and Testing

1. Right-click on the graphic of the "Command_Signal.
2. Press "Assign PROFIstate address."
1. Click the checkbox for "Assign".
2. Press the "Identification" button.
3. Click the checkbox for "Confirm".
4. Press the "Assign PROFIbus addr." button.
5. Press "Close".
6. Press the blue button to clear the "Passivation Fault" on the module. The PLC fault should clear.