

## Conventional PLC vs. Safety PLC Controllers for Safety Instrumented Systems

Dr. William M. Goble  
www.exida.com

Safety Programmable Logic Controllers (PLCs) are special purpose machines that are used to provide critical control and safety applications for automation users. These controllers are normally an integral part of safety instrumented systems (SIS) which are used to detect potentially dangerous process situations. If such a situation occurs, the SIS is programmed to automatically take action to bring the process to a safe state. There is a serious question though, What is the difference between a safety PLC and the conventional PLC that has been successfully used for years? Why shouldn't a conventional PLC be used in critical control and safety applications?

A safety PLC was specifically designed to accomplish two important objectives:

- (1) do not fail (redundancy that works well) but if that cannot be avoided,
- (2) fail only in a predictable, safe way.

Many special design considerations are taken into account. A safety PLC will emphasize internal diagnostics, a combination of hardware and software that allows the machine to detect improper operation within itself. A safety PLC will have software that uses a number of special techniques to insure software reliability. A safety PLC will have redundancy to maintain operation even when parts fail. A safety PLC will have extra security on any reading and writing via a digital communications port.

A safety PLC also differs from a conventional PLC in that the safety PLC is typically certified by third parties to meet rigid safety and reliability requirements of international standards. Thorough, systematic methods must be applied to the design

## Conventional PLC vs. Safety PLC Controllers for Safety Instrumented Systems

and testing of safety PLCs. The experts at exida Certification S.A. in the U. S. provide third-party independent validation and verification of the safety PLC design and testing procedures.

Special electronic circuitry, careful diagnostic software analysis, and full fault injection testing of the complete design insure that safety PLCs are capable of detecting over 99% of potentially dangerous internal component failures. A Failure Modes, Effects and Diagnostic Analysis (FMEDA) is conducted on the design, indicating how each component in the system fails and how the system detects the failure. exida engineers personally perform fault testing as part of their certification process.

Tough international standards for software apply to safety PLCs. These standards demand special techniques to avoid complexity. Extensive analysis and testing carefully examines operating systems for task interaction. This testing includes real-time interaction, such as multi-tasking (when used) and interrupts. Special diagnostics called “program flow control” and “data verification” are required. Program flow checking insures that essential functions execute in the correct sequence. Data verification stores all critical data redundantly in memory and checks validity before use. During software development, a safety PLC requires additional software testing techniques. To verify data integrity checking, a series of “software fault injection” tests must be run. The programs are deliberately corrupted to insure that the PLC responds in a predictable, safe manner. The software design and testing is fully documented so that third-party inspectors can understand PLC operation. While most software

## Conventional PLC vs. Safety PLC Controllers for Safety Instrumented Systems

development does not justify this activity, it is precisely how the most insidious software design faults are uncovered.

There are certainly many similarities between a safety PLC and a conventional PLC. Both have the ability to perform logic and math calculations. Both typically have input and output (I/O) modules that provide them with the ability to interpret signals from process sensors and actuate control final elements. Both will scan inputs, perform calculations and write outputs. Both typically have digital communications ports. But the PLC was not initially designed to be fault tolerant and fail-safe. That is the fundamental difference.

The realization of many users that conventional controllers cannot be depended upon in critical protection applications creates the need for safety PLCs. The standards are high for safety PLC design, manufacture and installation. Anything less than these high standards will soon be considered irresponsible, if not negligent, from a business, professional and social point of view.