Sección Española

PLCs de Seguridad frente a PLCs de Propósito General

MANUEL LÁZARO GALLARDO
SIEMENS

RESUMEN

Mediante el presente trabajo se pretenden analizar las aplicaciones de automatización en general, particularizando en especial para las aplicaciones de seguridad, desde el punto de vista de los equipos a utilizar, es decir se dará una visión de cómo surgen los PLCs de propósito general, que ámbito tienen y su posible introducción en aplicaciones de seguridad. A partir de aquí se presentan las características de las aplicaciones de seguridad y la necesidad de contar con un nuevo equipo con características especiales para este tipo de aplicaciones, y es aquí donde surge el PLC de seguridad.

1. INTRODUCCION

Aspectos históricos de la automatización

Los PLC's se empezaron a utilizar por primera vez en la industria en la década de los 60. En aquellos momentos eran utilizados sistemas de control basados en relés y contactores, cuyo principal problema residía en que cuando las necesidades de producción cambiaban también debía hacerlo el sistema de control y esto implicaba reconexionar a veces cientos incluso miles de relés. Esta tarea requiere un enorme esfuerzo de diseño y mantenimiento, que al final se traducía en altos costes del sistema.

Los nuevos PLCs, de aquellos momentos, ofrecían prestaciones que superaban con creces estas limitaciones, tenían un tiempo de vida largo y las modificaciones del programa se realizaban de un modo sencillo y rápido. Además, cada vez fueron más robustos para poder trabajar en entornos industriales, a la vez que son más fiables. En definitiva esto supuso el comienzo de la sustitución del relé y de la electrónica de estado sólido por los sistemas electrónicos programables (como el PLC).

Conforme transcurrieron los años los PLCs fueron cada vez más potentes, sus microprocesadores son cada vez más rápidos, tienen mayor capacidad de memoria, se le incorporaron posibilidades de comunicación con otros PLCs y con sistemas de visualización, se descentralizó la periferia, en definitiva, aumentaron tanto sus prestaciones que hoy en día desempeñan su labor en multitud de campos dentro de la industria que no eran imaginables en los comienzos.

El DCS viene por un camino diferente son sistemas muy fiables que incluyen desde muy pronto el concepto de redundancia, pero su orientación es exclusiva en aplicaciones de proceso.

Los sistemas basados en relés siguieron utilizándose durante algún tiempo en aplicaciones concretas donde prima la seguridad, es decir en aquellas aplicaciones donde lo que se pretende no es controlar un proceso y procurar que funcione eficientemente sin que pare la producción, sino en aquellas aplicaciones cuya función es

llevar la planta a un estado seguro cuando se cumple alguna situación predefinida que pueda provocar algún accidente, ya sea con daños a personas, daños medioambientales o daños a los propios equipos.

Ante este tipo de aplicaciones de seguridad los relés cumplen está función eficazmente porque presentan mayor nivel de seguridad que el PLC.

Surge por lo tanto la necesidad de crear un equipo basado en sistemas electrónicos programables, decir un PLC, pero con un nivel de seguridad mayor que el PLC general, y es ahí donde entra en juego el PLC específico para aplicaciones de seguridad.

2. OBJETIVOS

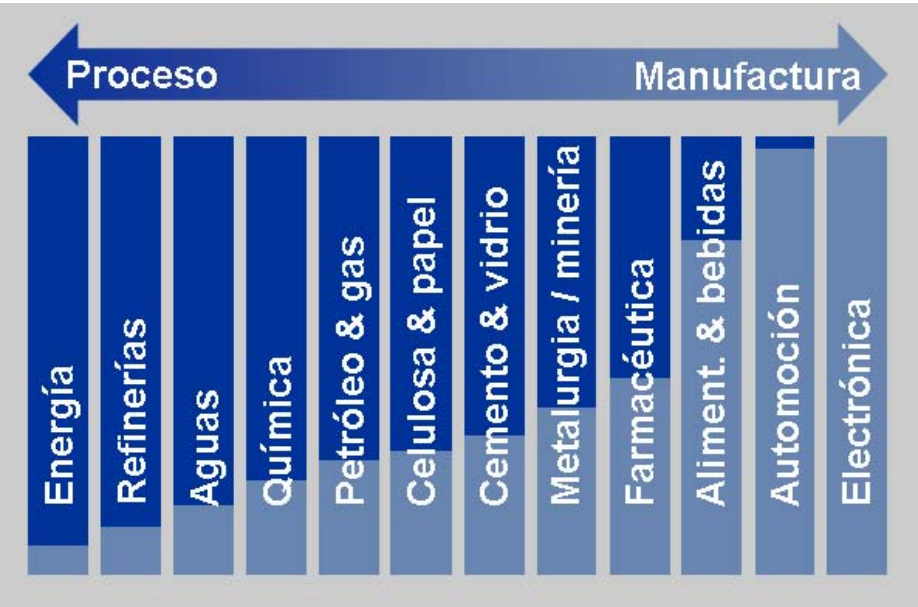
Mediante el presente artículo se trata de fijar las posiciones, dentro de la industria, del PLC de propósito general y del PLC de seguridad argumentando en cada caso la idoneidad de cada uno en su campo y centrándonos en particular en las aplicaciones de seguridad, donde puede surgir el conflicto entre ambos.

3. DESCRIPCION

Control industrial

Ya hemos comentado los aspectos históricos que rodean la aparición del PLC dentro de la industria, ahora vamos a centrarnos en sus funciones dentro de la misma.

Dentro de toda la gama de aplicaciones industriales el PLC tiene cabida fundamentalmente en aquellas áreas donde el tipo de señales es discreta, es decir en el mundo digital. La industria manufacturera se caracteriza principalmente por ello, y es ahí donde se centran la mayor parte de sus aplicaciones. Dentro de la industria de proceso tiene su campo más restringido conforme la aplicación podemos considerarla más pura en el ámbito del proceso.



Para el resto del control industrial donde la lógica digital queda en un segundo plano frente a los dispositivos analógicos, la instrumentación, el PLC no se adapta bien a este tipo de aplicaciones, y es ahí donde tradicionalmente se utiliza el los sistemas de control (DCS). La filosofía de este sistema es diferente a la del PLC, porque desde el principio a llevado un camino diferente, aunque se complementaron en muchos entornos dentro de la industria. Hoy en día y debido a lo potentes que son las CPU de los PLCs cada vez se igualan más las prestaciones en cuanto a ámbito de aplicaciones, existiendo aún diferencia en cuanto a forma de trabajo y entorno de desarrollo de la aplicación.

Entre las tareas típicas del PLC dentro de la industria tenemos todo lo que es la logística de entrada y salida de producto además de las tareas discretas dentro del proceso, como por ejemplo las fases de movimientos mecánicos dentro del mismo.

Aunque su función principal dentro del proceso está en el control de los enclavamientos del sistema, tarea típicamente destinada al PLC.

En cuanto al equipo en si mismo, la CPU sigue siendo prácticamente igual a las originales pero con mayores prestaciones, donde sí se ha desarrollado notablemente es en las posibilidades de comunicación, ya sea horizontalmente, comunicándose con otros PLCs o con DCSs, a través de estándares en comunicación por redes o punto a punto, o verticalmente, hacia arriba con sistemas de visualización, por un lado, y últimamente con sistemas de control de producción, y hacia abajo con todo lo que son señales de campo ya sea con remotas de entrada y salida o con instrumentos de campo, es decir descentralizando la periferia y permitiendo mucha mayor flexibilidad en las configuraciones.

Pero centrándonos en el ámbito del PLC dentro de la industria es muy importante su función controlando los enclavamientos del sistema ya sea en el ámbito general o de seguridad.

Por ello vamos a introducir algunos conceptos de seguridad

<u>Necesidad de potenciar la Seguridad</u>

Hay determinadas aplicaciones industriales, ya sean de proceso o no, donde nos encontramos con situaciones que de no ser controladas nos pueden llevar a producir accidentes de mayor o menor gravedad. De aquí surge la necesidad de emplear sistemas adecuados que puedan prevenir tales hechos, siendo sus funciones principales:

- Evitar accidentes cuando ocurre un fallo.

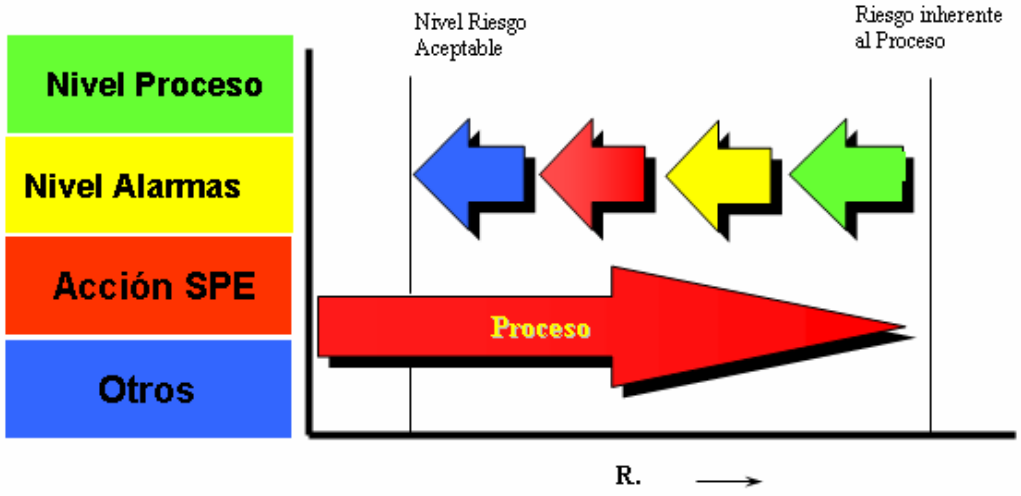
- Garantizar la máxima seguridad para las personas, evitar daños medioambientales y proteger en lo posible los propios equipos.

- Reducir el riesgo real a un nivel aceptable utilizando las medidas adecuadas.

El riesgo se puede definir como la probabilidad de que suceda algún hecho peligroso, es por lo tanto una combinación de la probabilidad de que un hecho ocurra y la gravedad del daño en si mismo.

Teniendo en cuenta la definición de riesgo, la forma más clara de protegernos contra estos riesgos en las plantas es minimizar éste hasta un nivel aceptable. Partiendo de la existencia de un nivel de riesgo inherente se tratará de emplear los medios adecuados para reducirlo hasta este nivel aceptable.

El riesgo inherente es definido de forma objetiva mientras que el nivel de riesgo aceptable es un parámetro subjetivo que depende de condicionantes externos.



La herramienta que nos permite reducir el nivel de riesgo a un nivel aceptable es un Sistema Instrumentado de Seguridad (SIS), que podemos definirlo como el sistema compuesto de sensores, operador lógico y elementos finales de control con el propósito de llevar el proceso a un estado seguro cuando unas condiciones predeterminadas son violadas, cuando hablamos de operador lógico, hoy en día es sin duda un PLC.

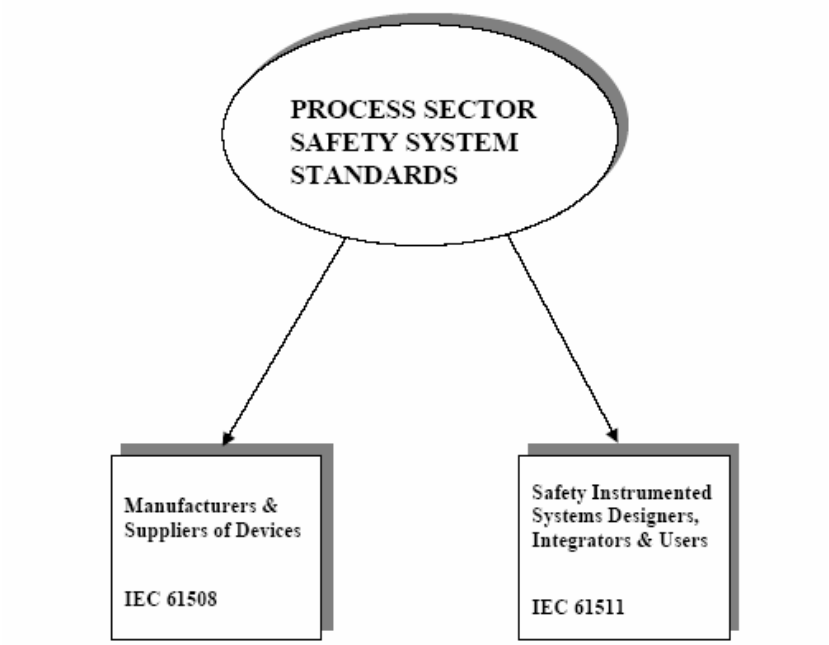
En resumen cuando hablamos de una aplicación de seguridad estamos hablando de utilizar un sistema cuya finalidad no es mantener una producción procurando que ésta no pare, sino que su cometido es llevar la planta a un estado seguro cuando se produzca alguna situación potencialmente peligrosa, de ahí que no se busca un sistema orientado fundamentalmente al proceso sino un sistema fiable que cuando se requiera que entre en funcionamiento tengamos certeza de que lo hará.

Standard y legislación

La IEC 61508 es el estándar reconocido internacionalmente para aplicaciones de seguridad, fue publicado por primera vez durante 1999/2000 con el fin de ser la mejor herramienta de ingeniería para el uso de sistemas electrónicos programables en aplicaciones de seguridad. Su ámbito es general dentro de la industria cubriendo todos los sectores de la misma.

Existen otros estándares particulares para determinados sectores industriales, como la IEC 61511 que es exclusiva para industria de proceso, la IEC 61513 para centrales nucleares, o la IEC 62061 para maquinaria.

Para industria de proceso la IEC 61508 está dirigida a fabricantes y suministradores de dispositivos, mientras que la IEC 61511 está dirigida a diseñadores de SIS, integradores y usuarios finales.



PLCs de propósito general en aplicaciones de seguridad

Ha quedado claro que el PLC es un sustituto natural de los sistemas basados en relés en las aplicaciones generales dentro de la industria pero qué ocurre en aplicaciones de seguridad.

Ya hemos comentado que una de las facetas del PLC de propósito general es la de realizar los enclavamientos de una planta pero cuando estos enclavamientos forman parte de una aplicación de seguridad en las cuales existen unos riesgos más elevados de poder llegar a una situación peligrosa este tipo de PLC ya no parece recomendable.

Vamos a compararlos en primer lugar con los relés. El PLC tiene, obviamente, mucha más funcionalidad y flexibilidad que los relés, sin embargo, hay una diferencia muy importante respecto a estos, y a tener en cuenta en aplicaciones de seguridad, y es que no tienen las mismas características ante fallos. Los relés en caso de fallo abren el circuito, por lo tanto su estado seguro se da a circuito abierto, mientras que los sistemas electrónicos de estado sólido no. Los dispositivos de estado sólido (transistores, triacs, etc) tienen la misma probabilidad de fallar a circuito abierto como cerrado. Estos sistemas electrónicos tienen, evidentemente, menor probabilidad de

fallos que los relés pero esto no es lo que cuenta para un sistema de seguridad sino que cuando hace falta el sistema esté disponible, y en los PLCs es difícil detectar posibles fallos en las señales si estas no están en uso.

Para subsanar este problema podríamos dotar a los PLCs de un nivel adecuado de diagnósticos. Por ejemplo, si nos fijamos en una aplicación en una fábrica en la cual un PLC estuviera controlando un transporte de producto de una zona a otra mediante una cinta transportadora, el sistema no requeriría necesariamente un amplio nivel de diagnósticos porque cuando el sistema falle será fácil ver que algo va mal porque la cinta funcionará mal. Pero qué ocurre si en vez de esta aplicación estoy controlando una presión en un proceso, en la cual el que se sobrepase un nivel alto de presión no ocurre en condiciones normales ¿ Sería capaz el sistema de detectar, por ejemplo, un fallo en la lectura de la presión o un cortocircuito en un triac en un módulo de salida ?

El principal problema de las aplicaciones de seguridad es que son aplicaciones en el que su modo de operación normal es en estado dormido, son sistemas normalmente pasivos, que están a la espera de que ocurra un hecho predeterminado para entrar en funcionamiento, por ello si no somos capaces de diagnosticar todos nuestros dispositivos para saber si funcionan correctamente con antelación quizás sea demasiado tarde porque va a ser cuando se requiera que entren en funcionamiento.

Podríamos tener fallos, y permanecer latentes, sin detectarlos, porque el sistema no está activando y desactivando entradas y salidas de un modo regular.

Un parámetro importante en este tipo de aplicaciones es la disponibilidad, que me indica la probabilidad de que un sistema no falle. Y en cuanto a los fallos existen dos tipos:

- Fallo seguro (desenergizando):
    - Es perceptible.
    - Inicia una parada parcial o total
    - No está planificado.
    - Implica costes de producción.
- Fallo peligroso:
    - Está oculto.
    - Función de seguridad inhibida.
    - Peligro potencial.
    - Deben localizarse mediante tests, por el sistema o mantenimiento.

La duda que surge es evidentemente si un PLC de propósito general tienen suficiente capacidad de diagnósticos para poder detectar estos fallos peligrosos que son los que pueden provocar situaciones de peligro, y como reacciona ante ellos.

PLCs de seguridad

Los PLCs de seguridad son algo diferentes a los PLCs de propósito general en cuanto a diseño. Un PLC de seguridad ha sido diseñado para incrementar los diagnósticos a un nivel muy por encima de los PLCs estándar. Se trata de corregir el problema de los fallos no detectados, que pueden ocurrir en un PLC de propósito general en tareas de seguridad que normalmente están en un estado durmiente. El hecho es, que si el PLC no ha sido diseñado para detectar este tipo de fallos, latentes, entonces es altamente improbable que estos fallos lleguen a ser aparentes hasta que el PLC es requerido para llevar a la planta a un estado seguro. En ese momento, dependiendo del fallo, el PLC podría actuar sólo como si fuera un simple retardo hacia una situación peligrosa que sería inevitable.

Por el contrario, el PLC de seguridad tiene una arquitectura diferente y está constantemente vigilando los fallos internos y errores de cableado externos. Algunos fallos sólo nos serán informados y con respecto a otros será tomada la acción correctiva necesaria para mantener el sistema en estado seguro.

En resumen se trata de equipos orientados principalmente a que cuando se requiere su funcionamiento estén en perfectas condiciones de funcionamiento, para ello la característica principal que disponen es la capacidad de diagnosticar tanto los fallos internos con los posibles fallos externos al propio equipo.

Aplicaciones de seguridad

Desde el punto de vista tecnológico ya hemos visto las diferencias de ambos tipos de PLCs, centrándolas en aplicaciones de seguridad.

Sin embargo desde un punto de vista de aplicación podríamos decir que es posible diseñar un sistema de seguridad utilizando PLCs de propósito general. Esta afirmación implica para la ingeniería lo siguiente:

- Tener que prever una cantidad extra para software.
- Mayor número de horas de ingeniería.
- Documentación extra.
- Cableado especial y rutinas software para diagnósticos.
- Mayor mantenimiento con el fin de asegurarnos del funcionamiento de los componentes.

Comparando el PLC general, con estas implicaciones, con el PLC de seguridad se puede apreciar inmediatamente los beneficios de éste principalmente:

- Herramientas y librerías software certificadas para seguridad que nos aseguran el perfecto funcionamiento de las funciones.
- Menor documentación debido a la estándar procedente de estos equipos.
- Menor número de horas de ingeniería, ya que existen soluciones claras para cada tipo de configuración.
- Los diagnósticos están incorporados en los equipos, con un hardware certificado, con lo que se reduce la elaboración de los mismos.
- Debido, fundamentalmente, a la incorporación de diagnósticos se reduce el mantenimiento de equipos.

Evidentemente de esto se deduce una reducción de costes a la hora de realizar estas aplicaciones con PLCs de seguridad. Pero por encima de argumentos relacionados con la reducción de costes está el que nos proporciona mayor seguridad sobre la solución final de la aplicación, tenemos un respaldo de los fabricantes que nos aseguran que sus equipos cumplen unas especificaciones y que lo hacen idóneos para cumplir unos niveles de seguridad.

Y aquí hemos llegado a otro importante argumento que es el de la certificación, para este tipo de aplicaciones es muy importante disponer de certificados de organismos independientes, como el TÜV, que nos indican el grado de seguridad (SIL o AK) al que llega un equipo para una configuración determinada. Con esta información en el

momento que determinamos el grado de seguridad de las funciones de nuestra aplicación, inmediatamente sabemos la configuración de un equipo determinado para ese grado de seguridad.

Es difícil, asimismo, realizar una aplicación de seguridad sin buenos datos de seguridad y fiabilidad, por ello el propietario del sistema, normalmente el usuario final, tiene que justificar que el grado SIL asignado al comienzo del proyecto coincide con el grado SIL al final del mismo, teniendo en cuenta los equipos instalados. Para ello los fabricantes de PLCs de seguridad suministran los datos necesarios para hacer estos cálculos.

El estándar IEC61508 acuerda que cada subsistema hardware que es usado para implementar una función de seguridad tiene que ser clasificado como subsistema Tipo A o Tipo B. Los subsistemas tipo A tienen modos de fallo completamente determinables mientras que los dispositivos Tipo B no.

El índice SFF (Safe Failure Fraction) es una medida de la tolerancia a fallos de dispositivo y que tiene 4 niveles:

- <60
- 60 -90
- 90-99
- >99

Para un PLC considerado Tipo B, el SFF del PLC debe ser >60% para SIL 1 y mayor de 90% para SIL 2, para un sistema que no emplea total redundancia de procesador y módulos de entrada/salida.

Y para hacer estos cálculos hacen falta datos detallados por parte del fabricante de sus dispositivos.

4. CONCLUSIONES

Los fabricantes de PLCs de propósito general son incapaces de asegurar que sus paquetes software son seguros, ni son capaces de dar alguna idea de la fracción de fallos seguros y peligrosos que presenta su diseño hardware.

Normalmente tampoco pueden suministrar suficiente detalle para aplicaciones seguras de acuerdo a IEC 61508. En resumen, los ingenieros deberían considerar el uso del PLC general en aplicaciones de seguridad con mucho cuidado antes de verse involucrados en una situación que les será muy costosa y no del todo satisfactoria desde el punto de vista de la seguridad.