Universidad de Mendoza

Facultad de Ingeniería

Tesis de Maestría en Teleinformática

“Extensión del Concepto de Canal Negro a un Enlace Radioeléctrico”

Ing. Juan Carlos Artal

Director de Tesis:
Ing. Alfredo Iglesias

Mendoza, Diciembre 2013

AGRADECIMIENTOS

Quiero agradecer especialmente a mi esposa Cristina por su amor y su apoyo constante para que yo pudiese preparar este trabajo. También a mi hija Maria Sofía por poner alegría a tantas horas de labor.

A mis padres que, con su ejemplo, me enseñaron el camino del esfuerzo y la dedicación como herramientas indispensables para alcanzar las metas importantes de la vida. A mi hermano Jorge como modelo de perseverancia y excelencia.

A Alfredo Iglesias por su acompañamiento durante toda la elaboración de la tesis, por sus palabras siempre justas para orientarme en los momentos de dudas y por la confianza depositada en mí.

Al personal de la oficina de Siemens Argentina S.A. en Mendoza, en particular a Daniel Cañadas y Carlos Hernández que tomaron como propia la concreción del proyecto y que sin su gran apoyo hubiese sido imposible la implementación práctica de este trabajo. También a Gabriel Pulido por aportar su conocimiento y por su gran apoyo técnico.

RESUMEN

Lograr una mayor seguridad en la fabricación de bienes de consumo a través de sistemas automatizados de control es un objetivo que la sociedad exige cada vez con más fuerza desde hace varias décadas. Los fabricantes de estos sistemas automatizados de control se han visto obligados a cumplir con los requerimientos de la sociedad logrando desarrollar sistemas cada vez más rápidos y seguros haciendo uso de normas internacionales establecidas a nivel mundial.

Llevar los sistemas de control a una condición de parada segura cuando los procesos salen de sus condiciones normales, para evitar provocar daños a las personas, instalaciones o medioambiente, no es una tarea sencilla y es aún más compleja cuando los distintos componentes del sistema están separados distancias de varios kilómetros.

En este caso es posible comunicar estos componentes vía enlaces radiales pero la confiabilidad del sistema se ve comprometida debido a la inestabilidad del medio físico por sobre el cual se desarrolla la comunicación.

La solución al problema de falta de confiabilidad en el medio de transmisión se resuelve implementando diagnósticos de la propia comunicación. Esto se logra utilizando protocolos de comunicación, llamados protocolos seguros, que poseen la suficiente capacidad de diagnóstico para asegurar la confiabilidad de la comunicación.

Este concepto es el fundamento de lo que ha sido denominado “Canal Negro” en los sistemas de seguridad industrial: si se hace uso de un protocolo suficientemente seguro, la confiabilidad de la información es independiente del medio de transmisión utilizado (canal negro), siempre que éste cumpla con su función, o sea que esté disponible.

Existen varios protocolos de seguridad certificados por organizaciones internacionales como seguros. Estos protocolos han sido evaluados bajo los más altos estándares mundiales legitimando su confiabilidad. Dentro de ellos se ha elegido para la implementación práctica de esta tesis el protocolo PROFIsafe soportado por PROFIBUS y PROFINET Internacional (PI).

Este trabajo demuestra que extendiendo el principio de canal negro a un enlace radial y utilizando un protocolo seguro como es PROFIsafe, es posible garantizar la confiabilidad de la información en ambos extremos del enlace de forma tal que puede ser utilizado en un sistema manual de parada de emergencia a distancia de un proceso industrial.

INDICE GENERAL

CAPITULO I

1. Introducción

Los sistemas de control industrial tienen como función básica mantener el proceso de producción bajo control y que el producto de salida cumpla con las especificaciones deseadas.

Tan importante como cumplir con su objetivo principal es el de no provocar daños al entorno cuando las variables monitoreadas salen de sus cauces normales. Es indispensable entonces que los procesos industriales sean útiles y seguros.

Esta seguridad no sólo aplica a los procesos de fabricación de bienes de consumo sino también a la fabricación de máquinas, máquinas herramientas, medios de transporte (vehículos, aviones o trenes), a instalaciones en donde existen equipos rotantes (compresores, bombas) y en lugares donde se almacenan elementos peligrosos y hasta en la industria nuclear.

La mayoría de las veces la implementación de un sistema seguro se circunscribe a un espacio reducido, como por ejemplo dentro de una máquina herramienta. Algunas veces puede abarcar una zona más amplia como es una planta de proceso. En otras oportunidades las distancias son mucho mayores y es necesario realizar el tendido de cables o fibras ópticas. En algunas aplicaciones particulares, en donde participan elementos en movimiento, la comunicación entre las distintas partes, se desarrolla a través de enlaces inalámbricos tales como wi-fi. Sin embargo si las distancias son importantes ya no se pueden utilizar sistemas inalámbricos de corto alcance sino que es necesario recurrir a un diseño

de radioenlaces para comunicar los distintos elementos que componen el sistema.

Este es el caso de un ducto que transporta algún tipo de líquido inflamable o contaminante a lo largo de varios kilómetros. La rotura del caño en un determinado lugar, una vez detectada (probablemente por un sensor de presión), debe ser causal de paro de la o las bombas que impulsan el fluido y seguramente debe también accionar el cierre de válvulas o compuertas que aíslen la zona de rotura para evitar escapes mayores. La distancia entre el lugar en donde se detectó el derrame y la bomba es de varios kilómetros. Entre el sensor y la sala de bombas se ha establecido un enlace radial para detectar este tipo de contingencias. Es necesario entonces que la señal de parada llegue hasta la sala de bombas en forma inmediata y segura. Para lograr esto debemos cerciorarnos que la comunicación entre ambos puntos esté siempre activa y que si se interrumpe por alguna razón, la interrupción sea detectada en un tiempo prudencial y se actúe en consecuencia.

Puede darse que la comunicación se mantenga activa pero que por diversos factores naturales, eléctricos, magnéticos, atmosféricos, etc. La información llegue a destino con errores, lo que puede provocar o un falso accionamiento del sistema de parada o un no funcionamiento del mismo. Muchos son los factores que pueden llevar a que una comunicación como la del ejemplo no sea confiable.

La solución a estos problemas de falta de confiabilidad en la transmisión se soluciona implementando diagnósticos de la propia comunicación. Si es posible enviar por el medio inalámbrico, además de las señales de interés, señales de diagnóstico que nos aseguren que el enlace está establecido en todo momento y que lo hace sin ningún

problema tendremos la certeza de que, cuando se produzca el suceso, la señal llegará en forma correcta a destino.

Es de suma importancia entonces que también los diagnósticos sean seguros. Esto se logra apoyándose en protocolos de comunicación con la suficiente capacidad de diagnóstico que los haga probadamente seguros.

Es decir que por un lado tenemos un medio (el canal de comunicación) que es intrínsecamente inestable e inseguro y por otro lado (superpuesto o sobre el canal de comunicación) un protocolo que es probadamente seguro y que nos garantiza la confiabilidad de la comunicación.

Este es el principio de lo que ha sido denominado “Canal Negro”. Para hacer un medio de transferencia de información seguro no es relevante la confiabilidad o el tipo canal de comunicación utilizado (canal negro) siempre que cumpla con su función (o sea que esté disponible), si por encima de él se monta un protocolo seguro.

Existen varios protocolos de seguridad certificados por organizaciones internacionales como seguros. Estos protocolos han sido evaluados bajo los más altos estándares mundiales certificando su confiabilidad. Dentro de ellos se ha elegido para la implementación práctica de esta tesis el protocolo PROFIsafe soportado por PROFIBUS y PROFINET Internacional (PI).

Este trabajo utiliza el concepto de canal negro para darle confiabilidad un enlace radioeléctrico. El desafío entonces es garantizar la seguridad del canal de comunicaciones establecido a través de un enlace radial y demostrar que el mismo es apto para ser aplicado a un sistema de parada de emergencia a distancia, que en este caso consideraremos de accionamiento manual.

El trabajo está estructurado de forma tal que en el capítulo dos se hace una introducción teórica a los buses de campo industriales, su historia, su clasificación, sus requerimientos y fortalezas para luego pasar a Ethernet y su uso en el ambiente industrial. En este capítulo también se aborda la problemática del riesgo en el ambiente industrial, normativas y soluciones tecnológicas para su reducción. Se introducen conceptos fundamentales para el desarrollo y entendimiento de los protocolos seguros y del porqué de su uso en este trabajo.

En el capítulo tres se hace una descripción del estado del arte y de las características de los dos protocolos utilizados en los ensayos prácticos: PROFINET protocolo compatible con la IEEE 802.3 y PROFIsafe protocolo seguro (Safety Ethernet) certificado para ser usado hasta SIL3.

En el capítulo cuatro se desarrollan los ensayos para demostrar la aplicabilidad del concepto de canal negro a una comunicación establecida mediante radioenlaces. Se describe el equipamiento y software utilizados, la topología del sistema implementado y las pruebas realizadas.

El capítulo cinco resume las conclusiones de los ensayos y en el capítulo seis se sugieren desarrollos futuros que amplían el campo de aplicación de este trabajo.

CAPITULO II

2. Marco Teórico

2.1 Sistemas de Control en Plantas de Proceso

Actualmente casi la totalidad de los procesos de producción de bienes de consumo masivo son fabricados haciendo uso de sistemas automatizados que minimizan el esfuerzo del hombre y aumentan considerablemente la eficiencia y productividad. El uso de estos sistemas se traduce en una mejor calidad y en mayores volúmenes de bienes producidos, que no serían posibles si sólo se contara con el esfuerzo y la habilidad manual del hombre para fabricarlos. Estos sistemas automatizados llamados más precisamente, sistemas de control industrial son utilizados hace décadas en las grandes cadenas de producción.

En la década de los cuarenta del siglo pasado, la fabricación de productos en forma automática se apoyaba en tecnología neumática. Los sistemas de control de las plantas de proceso o fábricas estaban basados en dispositivos alimentados por aire comprimido. Desde la sala de control partían decenas de cañerías de cobre de pequeño diámetro, con aire a presión en su interior, que servían para mover los actuadores neumáticos que regulaban las distintas variables del proceso productivo. La señal de control analógica se basaba en la transmisión de una señal neumática variable de 3 a 15 psig (libras por pie cuadrado manométrica, del inglés “Pounds Square Inches Gauge”). El control primario residía en sofisticados controladores mecánicos-neumáticos. Operaciones matemáticas tales como multiplicaciones, integrales o derivadas eran resueltas por estos controladores a través de levas, resortes, orificios de

restricción con pasajes de aire y otros elementos mecánicos, convirtiendo a estos dispositivos en verdaderas obras de arte de la ingeniería. El registro de las variables se hacía en rollos de papel giratorios sobre los que escribía una pluma alimentada por un tintero que debía recargarse periódicamente. Todos los controladores se ubicaban en la sala de control en paneles o paredes verticales. El operador debía estar de pie frente a estos paneles para verificar el funcionamiento de la planta y tomar las acciones correctivas necesarias. Era entonces el operador de planta el encargado de coordinar la acción de cada uno de los controladores para llevar a todo el proceso de producción dentro de condiciones normales. Es lógico deducir que eran sistemas muy costosos y de difícil mantenimiento. Una pinchadura, quizás por corrosión, en alguno de los caños de aire podía producir desbalances de presiones dentro del sistema neumático con consecuencias indeseadas para la producción.

En la década de los sesenta se comenzaron a dejar de lado los sistemas neumáticos y comenzó a imponerse lo que se conoce como señal analógica de corriente eléctrica de 4-20 mA, a través de un par de hilos conductores. La alimentación eléctrica de los dispositivos en campo se hacía a través de este mismo par de cables por los que se recibía o enviaba la señal de control. La industria reemplazó la presión de aire por una variable eléctrica, la corriente. En vez de utilizar caños con aire, la vinculación con los elementos de sensado y actuación en campo se comenzó a realizar por cables. Esto disminuyó el costo y el mantenimiento de las instalaciones. Se desarrollaron dispositivos de conversión corriente/presión y presión/corriente para hacer de vínculo entre los antiguos sistemas neumáticos y los nuevos sistemas eléctricos. El estándar 4-20 mA fue revolucionario y por demás confiable. Aún hoy es ampliamente utilizado, sobre todo en el manejo de aquellas señales o variables que si escapan de sus valores normales pueden provocar daños

a las personas, al medioambiente o a las instalaciones. Muchas empresas en la actualidad requieren que las señales analógicas relacionadas con los sistemas de parada de emergencia sean cableadas bajo el estándar 4-20 mA. Esta señal es fácil de medir con un multímetro por lo que el mantenimiento y la detección de fallas está al alcance de cualquier persona de mantenimiento por más que no tenga acabados conocimientos de automatización.

El advenimiento de la electrónica de escala facilitó el desarrollo de circuitos integrados que posteriormente dieron lugar a los procesadores digitales. Estos procesadores digitales posibilitaron la construcción de primitivas computadoras que comenzaron a ser utilizadas para monitorear y controlar los sistemas automáticos en las plantas de proceso. Aparecieron grandes (por su tamaño) computadoras que hacían de enlace entre el operador de la planta y el proceso. Rudimentarios sistemas operativos y consolas de operador comenzaron a poblar las salas de control. Muchos cables, tecnologías de wire-ripping y también electrónica discreta eran comunes en esta etapa de desarrollo de la tecnología. Cada fabricante de sistemas de control de plantas de proceso comenzó a desarrollar su propio estándar. Se requería ser un verdadero especialista para entender y programar estos sistemas. Lo desarrollado por un fabricante era muy diferente de lo desarrollado por otro fabricante. Las necesidades de estandarización se comenzaban a hacer evidentes. Sin embargo el estándar de 4-20 mA seguía siendo dominante a la hora de llevar las señales al campo a la sala de control.

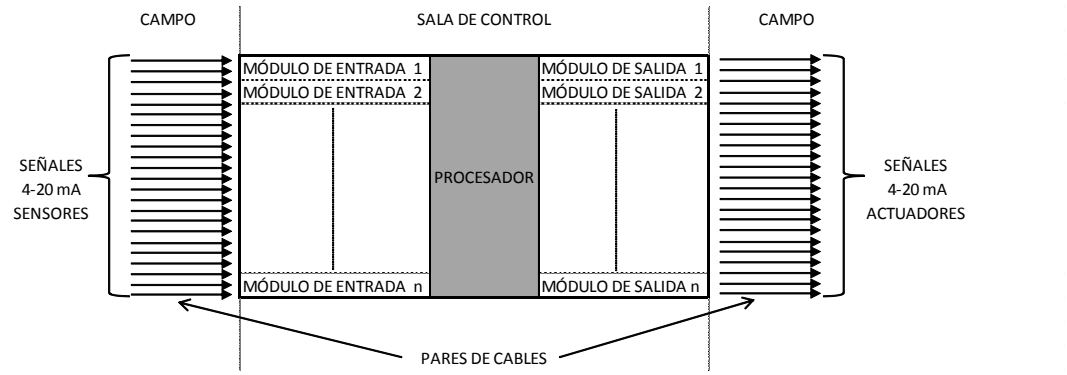

Gráfico 2.1 - Sistema de control con procesadores y módulos de entrada/salida integrados. Cableado discreto en 4-20 mA

En el gráfico 2.1 se observa cómo las señales estaban cableadas desde los sensores a los módulos de entrada. Luego pasaban a ser tratadas por el procesador, el cual resolvía la lógica programada y a través de los módulos de salida enviaba los comandos a los actuadores. Las señales de entrada y salida eran del tipo analógico (corrientes de 4-20 mA).

A medida que aumentó la escala de las plantas de procesos industriales la cantidad de sensores y actuadores también creció. La complejidad de los controladores también se incrementó considerablemente. Al aumentar el número de sensores y de actuadores aumentó el cableado existente entre estos y el sistema controlador. Varias decenas de cables en paralelo se extendían entonces entre sensores, controladores y actuadores.

Viendo en detalle este tipo de instalaciones podemos observar que tienen varias desventajas como son elevados costos de instalación y mantenimiento, dificultad en la detección de fallas, tiempos de reparación extensos, poca o nula capacidad de información sobre el estado de los elementos finales (sensores y actuadores), gran espacio ocupado por el cableado, etc.

Frente a tantas desventajas los ingenieros encargados de estos sistemas visualizaron la posibilidad de reemplazar todos esos cables en paralelo por un solo cable que interconectara los sensores, el controlador y los actuadores utilizando algún cierto sistema de comunicación, lo que dio origen entonces a los “Buses Industriales” o “Buses de Campo”.

2.2 Buses de Campo

Para aquellos que están familiarizados con el ambiente industrial el término “buses de campo” puede resultarle más o menos conocido, pero para aquellos que se dedican a otra actividad el concepto puede no ser del todo claro. Sin querer ser una definición, podemos decir que los buses de campo son el medio físico y lógico a través de los cuales se conectan y comunican los distintos dispositivos que intervienen en el control de una planta de proceso, fábrica, subestación eléctrica, etc. La palabra campo proviene de que estos sistemas de comunicación se extienden a lo largo de las plantas productivas interconectando los diversos dispositivos, máquinas, sensores, motores, etc. En la jerga industrial se le denomina “campo” a las instalaciones que están fuera de las oficinas y/o de las salas de control. De ahí nace el término de “buses de campo”.

Si bien se utiliza el término cableado, el soporte físico de un bus de campo se extiende de hecho, a otros medios de transmisión como son la fibra óptica y los enlaces inalámbricos.

Las ventajas de los buses de campo sobre la arquitectura tradicional del cableado duro en paralelo son varias, entre las más importantes se cuentan:

- Menos cableado, lo que ahorra espacio en las instalaciones y en el tamaño de los gabinetes de marshalling.
- Menores tiempos en el desarrollo de la ingeniería.

- Se reducen los tiempos de montaje e instalación.
- Menores tiempos de prueba y puesta en marcha.
- Es posible contar con información de autodiagnóstico del sistema.
- Los tendidos de las señales de campo son más cortos.
- Las ampliaciones o modificaciones son más fáciles de implementar.
- El sistema cuenta con mayor flexibilidad a la hora de realizar cambios de configuración.
- Mayor facilidad a la hora de implementar redundacia en los elementos del sistema.
- Calibración y configuración remota de elementos sensores y/o actuadores.
- Posibilidad de optimización de procesos.

Sin embargo los buses de campo también tienen sus desventajas, algunas de las cuales son:

- Sistemas más complejos por lo que se requiere de personal especializado para su desarrollo, construcción y mantenimiento.
- Mayores costos de los componentes del sistema.
- En general, sistemas más delicados por lo que se deben extremar las precauciones en cuanto a las interferencias electromagnéticas y frente a los esfuerzos mecánicos.
- Necesidad de contar con herramientas de diagnóstico más caras y sofisticadas.
- Pueden dar lugar a fallas generalizadas, por lo que posiblemente se necesite establecer arquitecturas redundantes.

Dentro del concepto de bus de campo están incluidos no sólo los elementos sensores y actuadores sino también la conexión o comunicación de los controladores centrales con las unidades remotas de

entrada salida (módulos I/O) que son las extensiones físicas de estos elementos controladores.

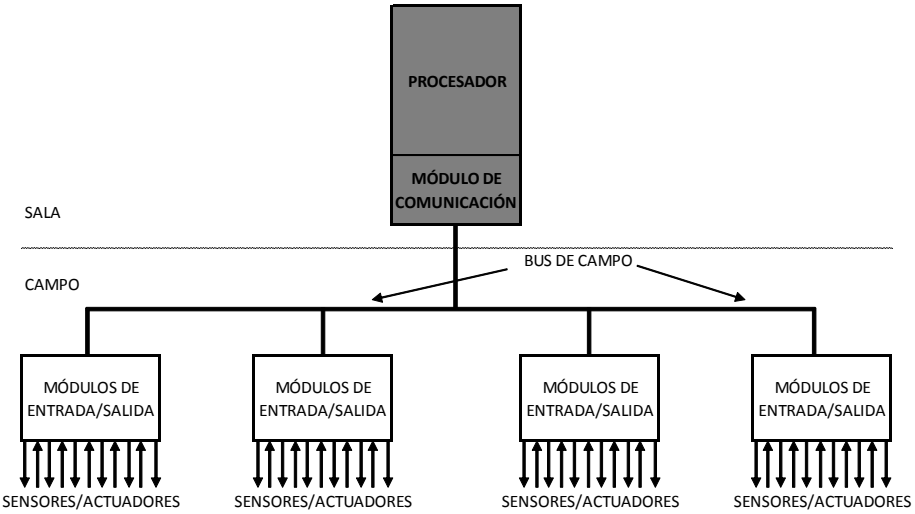

Gráfico 2.2 - Sistema de control con procesador central y módulos de entrada/salida distribuidos en campo – Bus de campo

En el gráfico 2.2 se observa la estructura de un sistema de control en el cual los módulos de entrada/salida se encuentran en el campo y se comunican con el procesador central a través de un bus que maneja señales digitales. En este caso el bus de campo se extiende entre el procesador central y los módulos de I/O, pero también se podría comunicar el procesador con los sensores o actuadores en forma directa si éstos tuviesen la capacidad de “hablar” el mismo protocolo del bus de campo.

En los buses de campo los elementos componentes del sistema de control automático interactúan a través de diversos protocolos de comunicación. Sin ser una definición exhaustiva, entiéndase por protocolo, en este caso, a un conjunto de reglas prefijadas a través de las cuales los elementos de un determinado sistema pueden comunicarse e intercambiar información. La mayoría de estos protocolos de bus de campo son, de alguna forma, propietarios. Muchos otros se basan en

normas internacionales (Ej. normas IEC: International Electrotechnical Commission) u otros estándares de la industria, algunos de los cuales son de libre acceso.

Los buses de campo nacieron hace varias décadas y aún tienen mucho camino que recorrer en el ambiente de la automatización. Son utilizados en un gran número de industrias como:

- Químicas y petroquímicas,
- Petróleo y gas,
- Energía,
- Alimentos y bebidas,
- Farmacéuticas y biotecnología,
- Pulpa y papel,
- Agua y tratamientos de agua,
- Ensamble de equipamientos,
- Empaques,
- Automotrices,
- Plásticos,
- Robóticas
- Electrónicas
- Metal y minería,
- Militar y Aeroespacial

Estudios de mercado demuestran que el uso de los buses de campo, en las distintas industrias y actividades económicas, va en crecimiento año tras año teniendo un marcado incremento el uso de buses basados en Ethernet en detrimento de los llamados buses tradicionales.

2.3 La “Guerra” de los Buses de Campo

En la década de los ochenta del siglo XX comenzaron a aparecer los primeros dispositivos de campo denominados inteligentes. Sensores de presión, temperatura, caudal o nivel comenzaron a comunicarse en forma digital con la sala de control en un ambiente ya dominado por los microprocesadores. Cada fabricante comenzó a desarrollar sus propios protocolos de comunicación entre campo y sala. La necesidad de integrar varios tipos de instrumentos digitales de distintos fabricantes en una sola red de control de campo se hizo evidente. También se hizo más evidente aún la necesidad de una estandarización de los buses de campo.

La idea original, pensada por los ingenieros, fue la de tener un solo protocolo estándar para toda la industria que fuese usado por la totalidad de los fabricantes. Esto hubiese sido el ideal para los usuario ya que cualquiera fuese la marca de su sistema de control podría conectar sin problemas dispositivos de cualquier otra marca. Lamentablemente este no fue el camino seguido y los diferentes fabricantes comenzaron a desarrollar sus propios protocolos de comunicación intentando imponerlos sobre el de sus competidores.

En la segunda mitad de los años ochenta tuvo lugar un enfrentamiento entre los dos protocolos más promisorios el PROFIBUS alemán y el FIP francés [5]. Ambos protocolos fueron declarados como estándares en sus propias naciones pero no lograron imponerse a nivel internacional. PROFIBUS nació orientado a un control distribuido con una comunicación alineada con el modelo cliente-servidor, mientras que FIP estaba más orientado a un control centralizado y a un modelo de comunicaciones productor-consumidor. Obviamente ambos protocolos tenían sus ventajas y desventajas y durante los años subsiguientes se fueron perfeccionando para tratar de superarse entre sí. Así aparecieron

protocolos mejorados como el worldFIP derivado del FIP y el ISP derivado de PROFIBUS. A mediados de los años noventa hace su aparición la "versión americana" de los buses de campo con el desarrollo del Fundation Fieldbus.

La aparición de estos y otros protocolos dio lugar a lo que se llamó la "guerra de los buses de campo" [4] que duró hasta fines del siglo pasado y que llegó hasta niveles de hostilidad diplomática entre los países que apoyaban a tal o cual protocolo. La principal víctima de esta guerra fue sin dudas el usuario final de esta tecnología, ya que se vio envuelto en una maraña de protocolos no compatibles entre sí con una gran dificultad, entre otras, para definir cuál de todos los protocolos era el más adecuado para sus necesidades.

Luego de varios años de puja, en julio de 1.999, los principales contendientes (Fieldbus Foundation, Fisher Rosemount, ControlNet International, Rockwell Automation, PROFIBUS user Organization, y Siemens) se reunieron para firmar un documento de entendimiento que logró bajar el nivel de conflictividad. Fue la International Electrotechnical Commission (IEC) la que llevó a cabo la tarea de estandarización de varios buses de campo y la encargada de publicar la norma IEC 61158 "Industrial Communication Networks – Fieldbus Specifications" el 31 de diciembre de 2000 [3]. Esta norma clasifica los buses estándares de acuerdo a las características de sus capas físicas, de enlace y de aplicación. La norma IEC 61158 fue luego superada, corregida y enmendada por la norma IEC 61784 "Industrial Communication Networks – Profiles".

2.4 Diferentes Buses de Campo

La norma IEC 61784 [3] clasifica los protocolos en diferentes "Familias de Protocolos de Comunicación" (Communication Profile Families - CPF). Diecinueve son los CPF incluidos en ella, algunos de los cuales a su vez se subdividen en diferentes versiones. La norma también enuncia los nombres comerciales con los cuales se conocen los diferentes protocolos.

Familia	Version	Nombre Comercial
CPF1		FOUNDATION Fieldbus (FF)
	CPF1 / 1	FF-H1 (Low Speed)
	CPF1 / 2	FF-HSE (High Speed Ethernet)
	CPF1 / 3	FF-H2 (High Speed)
CPF2		CIP (Common Industrial Protocol)
	CPF2 / 1	ControlNet
	CPF2 / 2	Ethernet / IP
	CPF2 / 3	DeviceNet
CPF3		PROFIBUS and PROFINET
	CPF3 / 1	PROFIBUS DP
	CPF3 / 2	PROFIBUS PA
	CPF3 / 3	PROFINET CBA
	CPF3 / 4	PROFINET IO Class A Conformance
	CPF3 / 5	PROFINET IO Conformance Class B
	CPF3 / 6	PROFINET IO Conformance Class C.
CPF4		P-NET
CPF5		WorldFIP
CPF6		INTERBUS
CPF7		SwiftNet
CPF8		CC-Link
CPF9		HART
CPF10		VNET / IP
CPF11		TCnet
CPF12		EtherCAT
CPF13		ETHERNET Powerlink
CPF14		EPA (Ethernet for Plant Automation)
CPF15		Modbus

	CPF15 / 1	MODBUS TCP
	CPF15 / 2	RTPS
CPF16		SERCOS
	CPF16 / 1	SERCOS I
	CPF16 / 2	SERCOS II
	CPF16 / 3	SERCOS III
CPF17		RAPIEnet
CPF18		SafetyNet p
CPF19		MECHATROLINK

Tabla 2.1 - Norma IEC 61784 - Familias de Protocolos de Comunicación

La lista de protocolos incluidos en la norma IEC 61784 no es exhaustiva y existen en el mercado otros buses industriales.

A pesar de que todos los buses pueden compartir en general el mismo medio físico de transmisión la realidad indica que las diferencias entre ellos son tan profundas que la interconectividad entre sí aún hoy se hace difícil.

2.5 Tiempo Real y Determinismo

Las comunicaciones en los sistemas industriales deben cumplir con requerimientos muy estrictos ya que cualquier problema en la comunicación puede desembocar en un mal funcionamiento del sistema lo que a su vez puede provocar pérdidas de producción, pérdidas económicas, roturas mecánicas, explosiones y hasta daños a las personas y al medioambiente.

Uno de los requerimientos más importantes de un sistema de comunicaciones industrial es su capacidad de trabajar en “tiempo real”. Si un sistema es capaz de reaccionar bajo todas las condiciones de operación y enfrentar en forma exitosa a todos los eventos requeridos dentro de un tiempo de respuesta determinado y esperado, entonces el

sistema es capaz de trabajar en tiempo real. De la misma forma si un sistema de comunicaciones puede intercambiar datos entre sus partes componentes dentro de un tiempo determinado y esperado entonces el sistema de comunicaciones trabaja en tiempo real para la aplicación deseada.

Muy relacionado a la capacidad de trabajar en tiempo real se encuentra la habilidad de un sistema de trabajar en forma determinística. El determinismo de un sistema describe la exacta predictibilidad en lo que respecta a su comportamiento temporal. Si es posible en forma exacta predecir el comportamiento temporal de un sistema en todos sus estados, entonces ese sistema es estrictamente determinístico.

Para los sistemas de comunicación las características de tiempo real se clasifican en dos tipos [6]. El primer tipo requiere que una acción sea ejecutada en un tiempo no mayor a un tiempo prefijado. El segundo necesita que la acción sea ejecutada dentro de una determinada ventana temporal. Este es un requerimiento indispensable cuando se necesita la sincronización de la acción. Si la acción se ejecuta antes del comienzo de la ventana de tiempo, o si se ejecuta finalizada esta ventana, la ejecución de la acción ha fallado. La desviación que se puede tolerar dentro de dicha ventana es comúnmente denominada “jitter”.

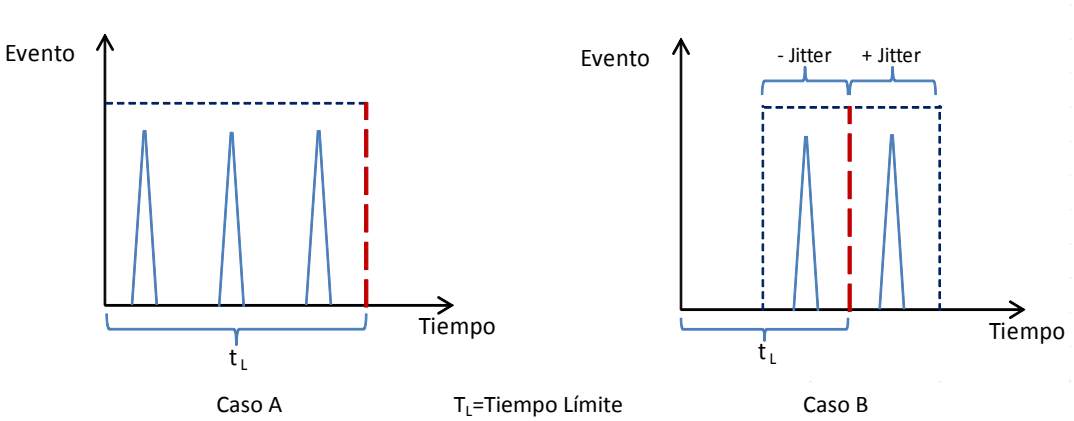

Gráfico 2.3 - Tiempo real

En general la mayoría de los buses industriales cumplen, o se pueden encuadrar, en la primera clasificación, mientras que no todos los buses industriales cumplen con los requerimientos de sincronización por tener un jitter mayor al deseado. Como ejemplo de aplicación se puede mencionar que los buses encuadrados en la primera clasificación pueden ser usados en la industria de procesos, mientras que los incluidos en la segunda clasificación son usados por ejemplo en el accionamiento de motores de cintas transportadoras.

La precisa coordinación de los diferentes componentes de un sistema automatizado se realiza en base a mecanismos de sincronización de tiempos. La ejecución de las acciones está completamente confinada al arribo del dato al dispositivo que va a ejecutar la acción. Esto significa que el patrón de tiempo de ejecución de la acción se realiza en una forma determinística, es decir de una manera predecible o en otras palabras que ante las mismas condiciones de entrada en sistema se va a comportar de la misma forma entregando siempre la misma salida.

2.6 Arquitectura de los Buses de Campo

Para el análisis de la arquitectura de los diferentes buses de campo se hace uso del conocido modelo de capas ISO – OSI (International Standard Organization - Open System Interconnection).

El análisis de los diferentes protocolos de buses industriales se realiza teniendo en cuenta las capas física, de enlace y de aplicación de cada protocolo.

En general todos los protocolos de buses de campo en su capa de enlace eliminan los ruteos y tienen un canal directo (stack de comunicación) entre la capa física y la capa de aplicación. En el gráfico siguiente se hace una comparación entre el tradicional modelo ISO - OSI de capas y la arquitectura utilizada por muchos de los buses de campo.

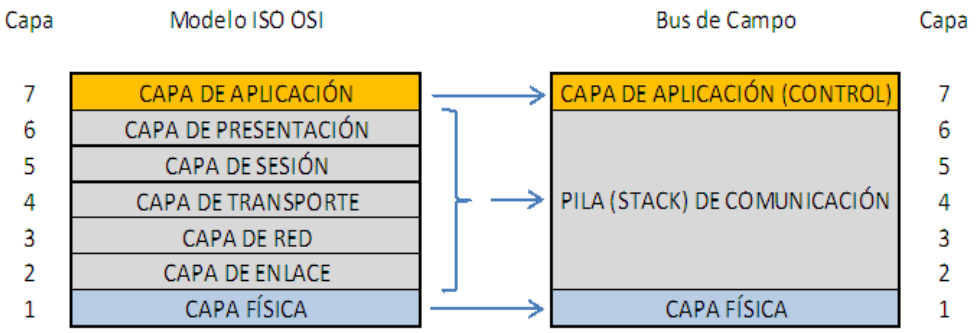

Gráfico 2.4 - Modelo de capas de los buses de campo

De todos los protocolos existentes vamos a ocuparnos sólo de los protocolos relacionados a Ethernet y Ethernet Segura que son objeto de este documento. Posteriormente veremos el concepto de protocolos seguros.

2.7 Desafíos de Ethernet en el Ambiente Industrial

Durante la década de los 90's Ethernet, junto con la tecnología de las computadoras personales ingresó de lleno al ambiente de las oficinas [6]. Los grandes fabricantes de computadoras aprovecharon la estandarización lograda por la IEE 802.3 para desarrollar y fabricar equipos que fuesen compatibles entre sí y también con los diversos dispositivos periféricos como impresoras, scanners, cámaras, etc. Ethernet se convirtió en una tecnología de facto como estándar de comunicación de los dispositivos domésticos y de oficina. Nadie en el mundo actual cuestiona que Ethernet es el gran sistema de comunicación usado alrededor del mundo. El gran desarrollo llevado a cabo sobre esta tecnología, el amplio "know how" que hay sobre la misma y los costos cada vez menores de los componentes, llevaron a los fabricantes, vendedores y usuarios a probar sus beneficios en el ambiente industrial.

Este nuevo ambiente industrial al que se tuvo que enfrentar Ethernet tiene características distintas al de una oficina y presenta nuevos desafíos. Las principales diferencias son:

- Las propiedades temporales del sistema de comunicaciones, debe garantizarse el determinismo y la velocidad de las comunicaciones.
- Una mayor resistencia a la agresividad del medio. El sistema de comunicaciones debe soportar mayores exigencias con respecto a las interferencias electromagnéticas, temperaturas extremas y exigencias mecánicas.
- Tener un mejor rendimiento en cuanto a estabilidad y seguridad, tanto desde el punto de vista de fallos del equipamiento como el de impedir el acceso a intrusos.
- La cantidad y la complejidad de los datos a transmitir.

- Es necesario un sistema simple de diseñar, implementar, aplicar y mantener ya que el personal que lo maneja no es un personal altamente capacitado en tecnologías informáticas.

Los componentes intervinientes en un sistema de comunicación industrial difieren de los que se encuentran en la oficina. Dispositivos tales como PLCs (Programmable Logic Controller / Controlador Lógico Programable), I/O Systems (Sistemas de entrada salida), HMIs (Human-Machine Interface / Interfase Hombre-Máquina) Drivers (Arrancadores suaves, variadores eléctricos), sensores, paneles PC son integrantes comunes de los sistemas de comunicación industriales y todos deben ser capaces de comunicarse, ser configurados, y diagnosticados vía Ethernet.

Por otra parte los protocolos usados en la oficina, como ya vimos, son diferentes de los protocolos utilizados en la industria. Ethernet entonces debe lidiar con protocolos como Ethernet/IP, Ethernet Powerlink, Modbus TCP, PROFINET, SERCOS III o EtherCat por mencionar los más empleados. Estos protocolos de comunicación han sido desarrollados para cumplir con los requerimientos especiales y necesarios de los dispositivos de automatismo y Ethernet debe ser capaz de no perjudicar la performance de estos protocolos.

Dentro de la oficina no es relevante el tiempo de ejecución de las diversas tareas que se llevan a cabo. Si la impresión de un documento demora 4 o 6 segundos no es relevante. Si la transferencia de un archivo de un servidor a un cliente se hace en un tiempo menor o mayor el tema no reviste extrema importancia. En cambio en el ambiente industrial es de sumo valor la velocidad con la que un sensor debe enviar la información al controlador a fin de que este tome la acción necesaria sobre el actuador correspondiente. Imaginemos la velocidad con la que el conjunto detector-controlador-actuador de una prensa de una determinada

máquina herramienta debe actuar al verificar que el operario ha colocado su mano debajo de la prensa, justo en el momento que la prensa está descendiendo. El tiempo de reacción debe ser de algunos milisegundos o quizás de sólo microsegundos para evitar el accidente del operario.

En el caso del control de motores de una imprenta en donde se desplaza el papel a ser impreso, el “jitter” del sistema de comunicación es también crucial a la hora de no dañar el papel. El sistema debe ser tanto veloz como determinístico para no perjudicar el proceso de impresión.

La estabilidad del sistema de comunicaciones es otro de los factores importantes a tener en cuenta y que marca una diferencia notable entre el mundo de la oficina y el contexto industrial. Las fallas en el sistema de comunicaciones de oficina provocan pérdida de eficiencia, demoras para llevar a cabo la recuperación de archivos, reinstalación de aplicaciones, etc. que si bien son situaciones indeseadas tienen un impacto que suele no ser de elevada magnitud, teniendo en cuenta las políticas de resguardo de la información que sostiene la mayoría de las empresas.

Pero, dentro del ambiente industrial, un fallo en el sistema de comunicaciones de la red de control puede provocar situaciones altamente peligrosas para los empleados, las instalaciones, la producción o el medioambiente. Un desperfecto menor que provoque la falla en el sistema de comunicación de la red de control puede provocar daños con costos que pueden elevarse a varios millones de dólares.

En la actualidad muchos son los pasos que se han dado para evitar los problemas de estabilidad de los sistemas basados en Ethernet. Cables con un mejor apantallamiento, el uso de fibra óptica, topologías redundantes, mayor robustez mecánica o mayor rango térmico de los componentes han sido avances que han contribuido sustancialmente a

lograr la estabilidad de Ethernet en el campo industrial. El uso de topologías adecuadas en combinación con comunicaciones full-duplex a través de switches dedicados ha servido para superar la limitación que provoca el acceso al medio físico la aplicación del mecanismo CSMA/CD. La mayor velocidad lograda en las redes Ethernet junto con la limitación de la carga de la red a no más de 10 % de su carga máxima ha posibilitado que el comportamiento de la red tenga características determinísticas que no se lograban anteriormente.

Otro de los puntos importantes a tener en cuenta en las redes Ethernet es la seguridad, analizada desde el punto de vista de la intrusión de personas no autorizadas. El conectar la red industrial a Internet tiene ventajas desde el punto de vista de acceso a la información del proceso desde fuera de la planta o fábrica. Esto puede ser de gran ayuda a la hora de posibilitar el acceso externo de especialistas para la resolución de problemas o configuración de equipos. Sin embargo hay que ser muy cuidadoso en cuanto a la infraestructura y topología del sistema de comunicación. Es por lo tanto más que necesario el uso de firewalls y la implementación de políticas de seguridad que prevengan el ingreso de intrusos en el sistema de comunicación. En la actualidad ya hay virus que afectan a los sistemas de control como son los conocidos Stuxnet o Flame.

Por último y no menos importante es que los sistemas basados en Ethernet deben ser amigables para el usuario. En este caso la aplicación final que se implemente debe ser fácil de entender y de utilizar por el operario o técnico de la planta. Ningún operador de planta tiene el conocimiento suficiente como para entender en forma exhaustiva los fundamentos de la comunicación Ethernet o del stack IP/TCP/UDP o de algún otro protocolo de capas superiores que esté implementado en el

sistema de control. Por ejemplo los detalles internos de cómo funciona el protocolo DHCP en la asignación dinámica de direcciones IP o la parametrización de un firewall dentro de la planta debe poder hacerse de una forma muy sencilla y amigable para el técnico que está encargado del mantenimiento del sistema.

2.8 Consideraciones con Respecto a la Red [6]

2.8.1 Uso de Switchs

Las redes Ethernet actuales están estructuradas en base a switches. En contraste con el mecanismo de acceso CSMA/CD, no hay un medio compartido por lo que los dispositivos no tienen que competir por el acceso al medio. En vez de esto cada dispositivo puede establecer una conexión full dúplex con el switch. Como resultado, no hay una contienda por acceder al medio y cada nodo puede enviar datos en forma independiente de los otros. Así es imposible que ocurra una colisión. Cualquier dato que llegue al switch será inmediatamente enviado a su destino. Supongamos tener cuatro dispositivos conectados a un switch. El dispositivo 1 puede enviar un dato al dispositivo 2 mientras los dispositivos 3 y 4 intercambian información entre ellos. Puede darse que los dispositivos 1 y 3 envíen simultáneamente datos al dispositivo 4. En ese caso los datos serán almacenados en el buffer del switch y transmitidos en secuencia. Por supuesto este encolamiento de los datos provoca un retardo en el envío de la información. En los sistemas de comunicaciones que trabajan en tiempo real la cantidad de datos a ser enviada y recibida está claramente definida y el número de dispositivos integrantes también es conocido por lo que, sujeto a la velocidad de transmisión de la red, se puede conocer el máximo retardo que se tiene en la red.

2.8.2. Manejo de los Tiempos por Segmentación

Debido a que en la red pueden ser intercambiados diferentes tipos de datos con distintos perfiles de carga, es necesario hacer un manejo diferenciado de estos datos. Los datos utilizados para visualización, envío de información a la red gerencial de la compañía, actualización de software, modificación de parámetros de configuración o programación de los dispositivos de una red de Ethernet de control pueden cargar en forma importante la red. Se puede hacer un cuidadoso manejo de estos datos dentro de la red sin impactar sobre el rendimiento previsto de la misma. Es sabido que mientras mayor sea la cantidad de switches que existen entre dos dispositivos de la red, mayor será el tiempo de repuesta de esa red por lo que generalmente las redes de control utilizan una topología en anillo o de estrella simple. Esta topología complementada con una segmentación entre la red que trabaja en tiempo real y la red que no tiene dicho requerimiento puede evitar la recarga de la primera por lo datos intercambiados con la segunda. Un método efectivo para lograr esto es, por ejemplo, configurar un segmento entre ambas redes de 10 Mbps mientras los dispositivos en la red de control (red en tiempo real) se comunican en 100 Mbps. El acceso externo a la red de tiempo real obviamente se deberá hacer a través de firewalls y routers.

2.8.3. TCP ó UDP

El protocolo TCP es un protocolo orientado a la conexión. Es decir que al comienzo de la comunicación se establece una conexión virtual entre los dispositivos que van a intercambiar datos. Esta conexión virtual se cierra una vez que ha finalizado el intercambio de datos. Cualquier pérdida de datos es detectada y el dato perdido es retransmitido hasta que el intercambio sea exitoso. TCP también asegura que los datos transmitidos se mantengan en la secuencia correcta.

En contraste a esto UDP es un protocolo no orientado a la conexión. Los paquetes de datos son enviados en forma absolutamente independiente uno de otros. Si alguno de los paquetes se pierde no hay una retransmisión. Tampoco se controla si los paquetes arriban en la secuencia correcta. Para las aplicaciones en tiempo real se usa normalmente el protocolo UDP ya que el concepto de retransmisión es contradictorio con las demandas del tiempo real. En principio UDP es más adecuado para trabajar en la industria ya que si se pierde algún dato, en la próxima retransmisión o refresco de datos se actualizaría el valor, en cambio TCP intentaría repetir la transmisión del viejo dato hasta que la comunicación fuese exitosa.

En la mayoría de los casos no es la red la que provoca cuellos de botella en la transmisión de datos. Generalmente se asume que son los protocolos del stack los que provocan la mayor demora de procesamiento, como vemos que sucede en el caso de la retransmisión de los paquetes en TCP.

Pero si los protocolos del stack son desarrollados en hardware en vez de ser desarrollados en software los tiempos se pueden reducir considerablemente. En este caso los protocolos son manejados en circuitos integrados en forma independiente de la CPU. Estos integrados son ubicados entre los circuitos de Ethernet y la CPU. De esta forma se agiliza la ejecución de los protocolos de capa 3 y 4, comparada con su ejecución por software, y además su tratamiento se independiza de las otras operaciones que pueda estar llevando a cabo la CPU.

2.9. Ethernet en Tiempo Real

Desde un principio el stack Ethernet IP/TCP/UDP es no determinístico ya que fue creado para que varias computadoras se comuniquen entre sí utilizando un medio común en forma más o menos equitativa. El uso del mecanismo de acceso CSMA/CD es la razón por la cual el flujo y volumen de las comunicaciones dentro de la red están en permanente cambio y que no sigan un determinado patrón de comunicación. El tiempo exacto en el cual un mensaje va a llegar al receptor o una acción va a ser ejecutada depende de la carga de la red y del momento de acceso del dato a la misma. La organización en la red es flexible por lo que el tiempo de intercambio de datos entre dos puntos puede estar sujeto a variaciones.

Es necesario entonces trabajar en el manejo de la información y en la arquitectura de transporte para lograr un comportamiento en tiempo real y determinístico de los paquetes enviados utilizando Ethernet.

2.9.1 Arquitecturas de Transporte en Tiempo Real

Para el tratamiento de la información en tiempo real a través del stack Ethernet se abren tres posibilidades [1] [6].

- La primera de las opciones es aquella en que los datos críticos (tiempo real) y los no críticos comparten el mismo stack Ethernet IP/TCP/UDP. Se trata de hacer trabajar el stack sobre Ethernet IP/TCP/UDP de forma predecible en el tiempo. Dentro de los buses de campo esta arquitectura es la adoptada por los buses Ethernet I/P y Modbus TCP.

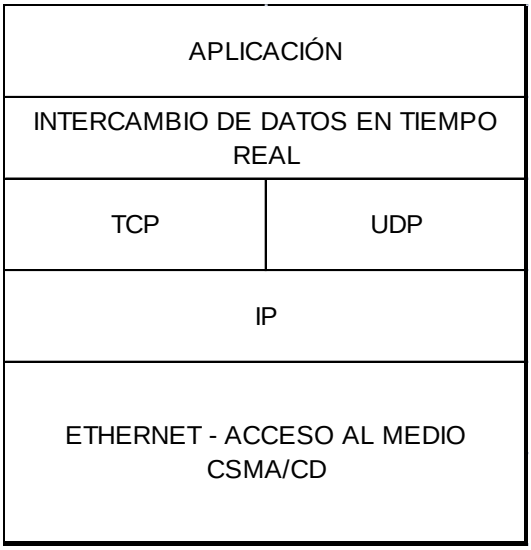

Gráfico 2.5 - Estándar Ethernet IP/TCP/UDP / Ethernet I/P - Modbus TCP

- En la segunda opción se observa que los datos no críticos se intercambian vía el tradicional stack Ethernet IP/TCP/UDP mientras que los datos críticos by-passean esta estructura a través de una comunicación en tiempo real. Es decir se usa Ethernet estándar en forma muy limitada y sólo para operaciones que no son críticas en cuanto a su ejecución temporal. Powerlink y PROFINET V2 adoptan esta estructura para el manejo de los datos.

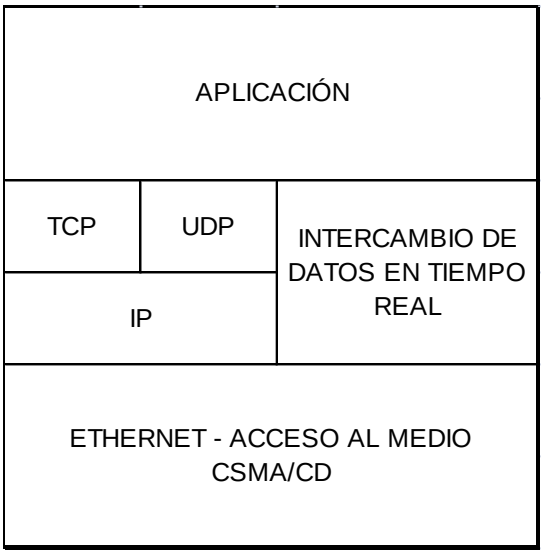

Gráfico 2.6 - By-pass de capa 3 y 4 / Powerlink - PROFINET V2

- En la última opción también se by-pasea el stack Ethernet IP/TCP/UDP para los datos en tiempo real pero en vez de hacer el tratamiento vía software se hace vía hardware.

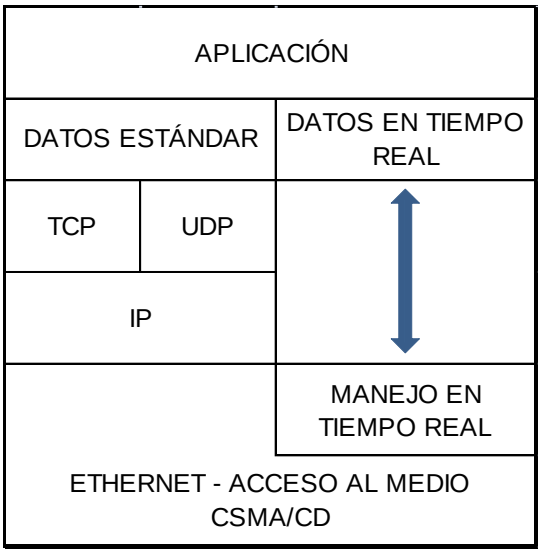

Gráfico 2.7 - Intercambio de datos en tiempo real por hardware / Sercos III – Ethercat – PROFINET V3

Además de la arquitectura de comunicaciones hay otros factores que influyen en la respuesta del sistema y que hay que tener en cuenta. La topología física y lógica de la red, la capacidad de manejar mensajes multicast o broadcast o el tipo de información a enviar deben ser parámetros a definir cuidadosamente a la hora de implementar la red de comunicaciones.

2.9.2 Buses de Campo Basados en Ethernet

En la actualidad existe un buen número de buses de capo basados en Ethernet de los cuales los más conocidos son:

- Modbus TCP
- Ethernet I/P
- PROFINET

- FF HSE
- Sercos III
- Powerlink

Si bien todos estos protocolos están basados en Ethernet las diferencias en las capas de aplicación hacen que todas estas soluciones sean incompatibles entre sí.

Entre todos los buses de campo existentes elegimos para este trabajo el protocolo de comunicaciones PROFINET.

2.10 Riesgo

Toda actividad industrial o, en general, toda actividad productiva tiene riesgos inherentes a la propia actividad. El riesgo de lesiones personales, daños materiales y daños al medio ambiente es intrínseco de todos los procesos industriales.

A lo largo de la historia muchos son los ejemplos que muestran que la actividad industrial no ha estado exenta de peligros y accidentes. Miles de millones de dólares gastados en remediaciones del medioambiente, muchas vidas perdidas en accidentes en fábricas, cuantiosos daños a la propiedad en ciudades y pueblos ha sido el precio que se ha debido pagar en aras de la producción de bienes para el consumo.

Por más que sea lo deseable, el “riesgo cero” no existe. Se puede reducir y minimizar pero siempre en toda actividad va a existir un riesgo remanente o residual.

Podemos definir al riesgo como: Una medida de la probabilidad de ocurrencia y de la consecuencia de un efecto adverso indeseable. O sea: ¿Que tan frecuentemente puede pasar, y cuáles son las consecuencias si sucediera?.

En este punto es necesario plantearse la pregunta del por qué son entonces toleradas las actividades riesgosas. La respuesta es sencilla y es debido a que estas actividades proveen algún beneficio. El riesgo sin ninguna perspectiva de recompensa representa un riesgo en estado puro y es raramente aceptado. El riesgo que se toma por una potencial recompensa es lo que se conoce como “riesgo especulativo” y es la base para la mayoría de las actividades humanas. Tanto el riesgo como el beneficio deben ser medidos para determinar de manera inteligente la mejor opción a seguir antes de desarrollar cualquier actividad. En la medición del riesgo debe considerarse tanto la probabilidad de ocurrencia como la consecuencia. Las consecuencias pueden provocar a su vez varios tipos de daños diferentes que deben ser evaluados en forma separada.

El daño también puede considerase como pérdida del beneficio, razón por la cual tanto el beneficio como el daño deben ser medidos. Por último todas las formas de daño significativo deber ser consideradas para medir correctamente el riesgo.

Una vez que ya sabemos que la actividad productiva va a tener un riesgo, el siguiente paso es saber cuál es límite máximo de riesgo aceptable o tolerable. Un riesgo es inaceptable para la sociedad cuando ésta no está dispuesta a soportar dicho riesgo en aras del beneficio que la actividad productiva genera. Es decir que el límite lo establece la sociedad [8]. Este límite no es absoluto, depende de cada sociedad en particular y de la evolución que ha ido teniendo la humanidad a lo largo de los siglos. Un ejemplo claro es la construcción del canal de Panamá. Sabido es que miles de personas murieron en la construcción del canal, sin embargo la sociedad, en ese momento, estuvo dispuesta a pagar dicho precio a cambio del beneficio que generaría, para la comunidad mundial, la

apertura del canal. En la actualidad sería inadmisible un costo de vidas humanas como el de aquella época. Otro ejemplo más cercano y actual es el número de accidentes viales que se producen anualmente en la Argentina. La sociedad argentina ya está acostumbrada y, aunque estemos en los primeros puestos en las estadísticas de número de accidentes por número de habitantes, acepta tal número de víctimas. En un país como Suiza tal número de accidentes sería inadmisible y la sociedad estaría reclamando a las autoridades medidas urgentes para mejorar la situación. Como resumen, se puede afirmar que la sociedad es la que determina los niveles de riesgo aceptables y que luego las corporaciones y los gobiernos son los encargados de aplicar políticas de reducción de riesgo para lograr dichos niveles.

Podemos considerar entonces como máximo riesgo aceptable a aquel que una sociedad está dispuesta a soportar a cambio de algún beneficio. Dentro de la actividad productiva suceden casos en donde los riesgos son mayores que los máximos permitidos. Nadie intentaría poner una central nuclear en medio de una ciudad populosa. La sociedad no lo permitiría. En estos casos para poder desarrollar la actividad productiva hay que llevar a cabo algún tipo de reducción de riesgos.

2.10.1 Manejo del Riesgo

Entre el límite de riesgo inaceptable y el riesgo ampliamente aceptado hay una zona intermedia en donde el riesgo “vale la pena” o es tolerado por los beneficios que genera. A esta zona se la llama zona A.L.A.R.P. (As Low As Reasonably Practicable) es decir tan bajo como sea razonablemente posible [8]. El manejo de los riesgos implica reducirlos hasta que los mismos alcancen un umbral que esté por debajo del riesgo inaceptable o intolerable es decir entrar a la zona A.L.A.R.P. y dentro de

la misma reducirlos hasta que el beneficio obtenido sea comparable con la reducción de riesgo lograda.

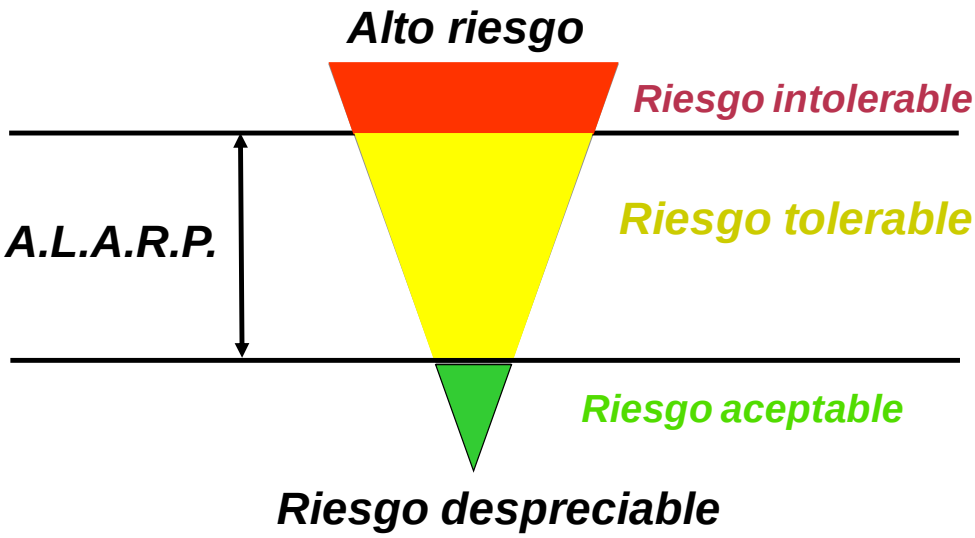

Gráfico 2.8 - A.L.A.R.P.

Surge de la definición que el riesgo posee dos componentes fundamentales, una es la probabilidad de ocurrencia (frecuencia) y la otra es la consecuencia (daño). El siguiente gráfico muestra esquemáticamente el manejo del riesgo. Si la consecuencia y la frecuencia son elevadas entonces el riesgo resultante será alto y será necesario tomar medidas para reducirlo o minimizarlo.

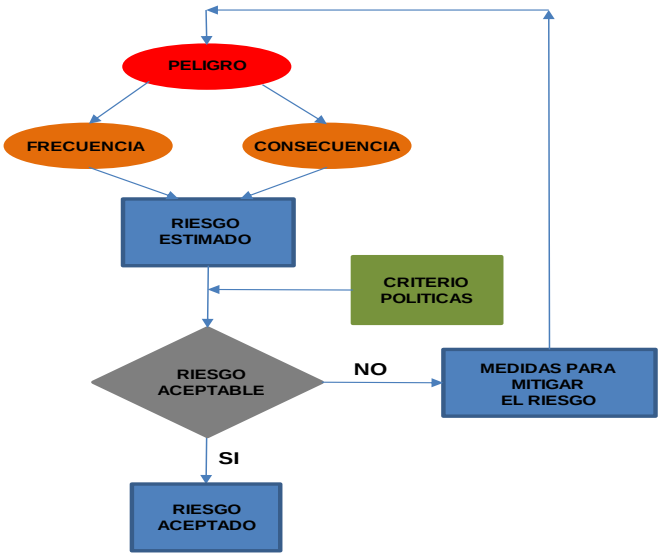

Gráfico 2.9 - Manejo del riesgo

El primer paso necesario es llevar a cabo un proceso de valoración y determinar un riesgo estimado. Si el riesgo estimado, valorado a través de las políticas de las empresas y/o de los criterios de la sociedad, es alto se deberán tomar medidas para mitigar o reducir ese riesgo. Si por el contrario se estima que el nivel de riesgo es aceptable, no es necesario aplicar medidas correctivas. En el caso de que sea necesario reducir el riesgo debemos introducir capas que de alguna forma nos aíslen o protejan de ese riesgo. Una capa de protección es algún elemento interpuesto entre el peligro y nosotros para reducir el riesgo. Un ejemplo de capa de protección es la crema que en verano nos colocamos sobre la piel, con algún factor de protección, para reducir el riesgo de quemaduras por efecto de los rayos ultravioleta. Otro ejemplo de capa de protección es la baranda que se coloca en un balcón para minimizar o reducir el riesgo de una caída.

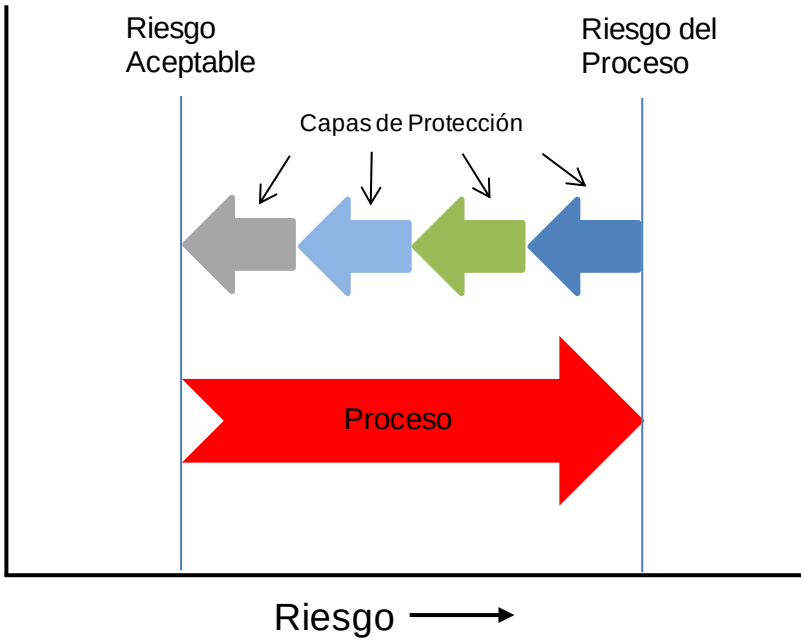

Gráfico 2.10 - Reducción del riesgo

De la misma forma se puede reducir el riesgo de una actividad productiva o industrial colocando capas de protección. Si con la implementación de una capa no se logra el nivel de reducción adecuado entonces se podrán ir colocando otras capas complementarias para lograr el objetivo buscado.

Colocando distintos tipos de capas de protección sobre el proceso podemos llegar a bajar el riesgo a un nivel aceptable. Esto se visualiza mejor en el llamado gráfico de capas, también llamado de la cebolla, en este caso aplicado a la actividad industrial.

En el centro del gráfico (Gráfico 2.11) se encuentra el proceso productivo con sus riesgos inherentes. Sobre el proceso existe una primera capa de protección que es el sistema básico de control (BPCS) encargado de mantener a las variables de proceso dentro de sus valores normales, respetando máximos y mínimos.

Por sobre la capa del sistema básico de control se ubica, como otra capa de protección, el sistema de alarmas que le avisa al operador que alguna variable ha salido de su valor normal para que éste tome la acción correctiva necesaria.

La siguiente capa es una capa de protección pasiva. Supongamos un recipiente sometido a presión, mientras mayor sea el espesor de la pared del recipiente, mayor será su capacidad de soportar una sobrepresión reduciendo la posibilidad de una explosión.

Posteriormente tenemos la capa correspondiente a los sistemas instrumentados de seguridad. La implementación de esta capa es de gran interés para nuestro trabajo y será vista en detalle más adelante. De todas maneras y a modo de introducción podemos definir a un Sistema Instrumentado de Seguridad como un sistema automático diseñado para reducir riesgos y programado para llevar el proceso a un estado seguro.

La próxima capa de protección es la denominada capa de protección intrínseca. En el ejemplo del recipiente a presión esta capa puede estar representada por una válvula de alivio que libere la presión del recipiente disminuyendo la sobrepresión y reduciendo el riesgo de una explosión. Si el evento se dispara más allá de esta capa se considera que el proceso se ha salido de control y que puede afectar al entorno fuera del ámbito industrial. Así las capas de protección física o diques de contención, la de respuesta de emergencia en la planta y la de respuesta de la comunidad ante emergencias están destinadas a minimizar el impacto sobre la sociedad.

La capa de protección llamada Sistema Instrumentado de Seguridad es un sistema de parada de emergencia automático que cumple con

estrictas características y funcionalidades dictadas por lo que se denomina

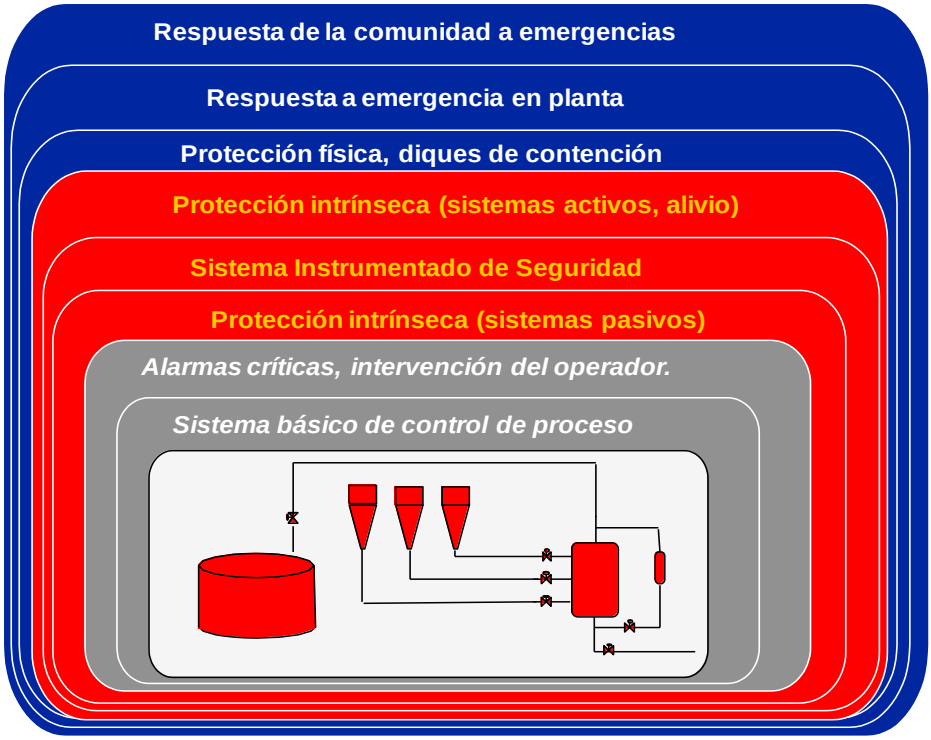

Gráfico 2.11 - Capas de protección

"Seguridad Funcional"

2.10.2 Seguridad Funcional

El ser humano consciente del impacto que la actividad industrial y productiva provoca fue utilizando las herramientas que tuvo a su alcance en cada momento de la historia para tratar de minimizar los riesgos. En los últimos tiempos la automatización de los procesos productivos fue ganando espacio y evolucionando hasta llegar al estado actual. La automatización por ende también comenzó a ser utilizada por el hombre para funciones de protección frente a los riesgos inherentes de los procesos productivos [9]. Por esta razón, es difícil encontrar hoy una

máquina, una fábrica o una estación de servicios que no cuente con un botón de parada de emergencia, o un sistema de protección ante fallos, lo que indica la presencia de algún sistema de seguridad.

En la década de los 70's del siglo pasado los sistemas de seguridad estaban construidos con elementos eléctricos o electromecánicos. Sistemas compuestos de cables y relés eran utilizados para la protección de equipos y personas. Posteriormente, la aparición de los circuitos integrados hizo que se fuesen dejando de lado los elementos electromecánicos y que se comenzara a utilizar la electrónica de estado sólido. Plaquetas y circuitos electrónicos fueron entonces los encargados de continuar vigilando la seguridad de los procesos de fabricación.

En la década de los 80's se comenzaron a utilizar los PLC's (Programmable Logic Controller) para fines de seguridad. Se introdujo así una nueva variable que no había estado presente hasta ese momento: la programación de los equipos de seguridad. Es también en esta época en la que se comienzan a utilizar procedimientos metódicos para la evaluación de riesgos de los cuales el más conocido y utilizado es el llamado HAZOP (HAZard and OPerability). En esa época el diseño y desarrollo de los sistemas de seguridad se basaba en la experiencia y en las mejores prácticas conocidas en la industria. Sin embargo los accidentes seguían sucediéndose con las consiguientes pérdidas humanas, monetarias y, en muchos casos, con impacto al medioambiente. Era cada vez más evidente la necesidad de contar con mejores herramientas de diseño, construcción, prueba y mantenimiento de los sistemas de seguridad y esto llevó a que distintas organizaciones a nivel mundial, especialistas en la materia, comenzaran a desarrollar y publicar normas sobre el tema. Países como Inglaterra, Estados Unidos y Alemania comenzaron a publicar sus propias normas nacionales las

cuales debían ser cumplidas por los fabricantes a la hora de diseñar y construir los sistemas de seguridad.

Varias son las normas que se publicaron al respecto hasta que en el año 2000 la IEC (International Electrotechnical Commission) termina de completar y publicar la norma IEC 61508 “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems” [15] [16] convirtiéndose en la piedra fundamental de la seguridad en la industria. Esta norma es genérica para toda la industria pero aplica especialmente a proveedores y fabricantes de elementos y equipamiento de seguridad basados en componentes eléctricos, electrónicos o electrónicos programables. Posteriormente se publicaron otras normas derivadas de esta norma madre con son la IEC 61513 “Nuclear Power Plants - Instrumentation And Control Important To Safety - General Requirements For Systems” para la industria nuclear, o la IEC 61511 “Functional Safety - Safety Instrumented Systems For The Process Industry Sector” para la industria de procesos.

Cabe destacar que tanto el vocablo “safety” como el vocablo “security” se traducen al español como “seguridad”. Sin embargo “safety” y “security” tienen significados disímiles en la lengua inglesa y no tienen una traducción literal en la lengua hispana. “Safety” se refiere a la seguridad contemplada desde el punto de vista de “daño” a personas, bienes, medioambiente, etc. mientras que “security” se refiere a la seguridad contemplada desde el punto de vista de “robo o pérdida” de alguna cosa.

Hecha la aclaración es importante destacar que la norma IEC 61508 define los conceptos de Seguridad (Safety) y de Seguridad Funcional (Functional Safety)

Seguridad: Es la ausencia de un riesgo inaceptable que provoque daño físico o daño a la salud de las personas, ya sea directamente, o indirectamente como resultado de daños a la propiedad o el medio ambiente.

Seguridad Funcional: Es la parte de la seguridad, considerada como un todo, que depende del buen funcionamiento de un equipo o sistema de acuerdo a como sean sus entradas.

La Seguridad Funcional es la detección de una condición potencialmente peligrosa que provoca la activación de un dispositivo de corrección o de protección.

El concepto de Seguridad que toma la norma IEC 61508 a lo largo de toda su extensión es la ausencia de un riesgo que dañe a las personas, que sea inaceptable para la sociedad, cuando ese daño sea provocado por perjuicios al medioambiente o a la propiedad.

La norma describe a la Seguridad Funcional como aquella parte de la seguridad en donde interviene y se acciona algún tipo de dispositivo que está destinado a evitar alguna situación de peligro. Ejemplo de Seguridad Funcional puede ser la activación de un detector de humo que ante la presencia de humo activa el sistema de mitigación de fuego evitando así el inicio un incendio. Otro ejemplo es el de la detección de alto nivel de fluido por parte de un switch, en un tanque que contiene líquido inflamable, provocando el cierre de la válvula de ingreso al tanque, evitando así el derrame del fluido y un potencial incendio o explosión.

2.10.3 Seguridad Funcional en Sistemas de Control de Procesos

Los conceptos del manejo del riesgo son tomados por la norma IEC 61511 para el caso de la industria de proceso y tratados en forma sistemática y ordenada para lograr la reducción del riesgo. La seguridad funcional a la que hace referencia la norma IEC 61511 se implementa con los llamados Sistemas Instrumentados de Seguridad (SIS – Safety Instrumented Systems).

De acuerdo a esta norma un Sistema Instrumentado de Seguridad se define como un sistema instrumentado usado para implementar una o más Funciones Instrumentadas de Seguridad. Un SIS está compuesto por una combinación de sensores, procesadores (o interpretadores) de lógica y elementos finales.

A menudo se prefiere una definición funcional del SIS como un sistema compuesto de sensores, procesadores de lógica y elementos finales con el propósito de:

- Llevar automáticamente un proceso industrial a su estado seguro cuando ciertas condiciones específicas han sido violadas,
- permitir que el proceso avance al próximo estado cuando las condiciones específicas se han cumplido (funciones permisivas) o
- tomar acción para mitigar las consecuencias de un peligro industrial

Un Sistema Instrumentado de Seguridad tiene por objetivo disminuir la probabilidad de ocurrencia de un evento indeseado.

Cuando la norma nombra a un sistema instrumentado de seguridad se refiere a un sistema destinado a cumplir funciones de seguridad y que

está compuesto por componentes Eléctricos, Electrónicos o Programables Electrónicos (E/E/PE).

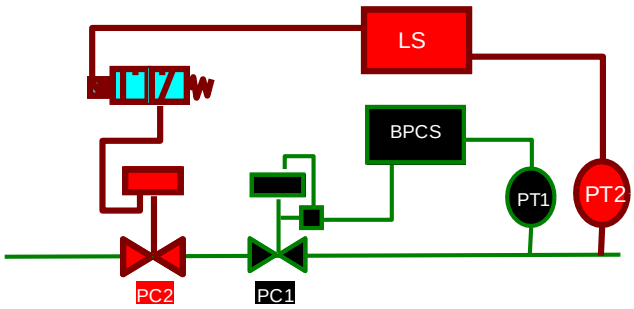

Gráfico 2.12 - Sistema Instrumentado de Seguridad

En el Gráfico 2.12 se visualiza un esquema simplificado de un lazo de control de presión en donde también se ha implementado una función de seguridad con un SIS. Por un lado se tiene un lazo normal de control de presión formado por un sensor de presión (PT1), un sistema básico de control del proceso (BPCS) y un elemento final que en este caso es una válvula controladora de presión (PC1). Este sistema es el encargado de controlar, supongamos, la presión de entrada de gas a un quemador de un horno en una fábrica. Debido al riesgo inherente de que este lazo de control falle, es decir, que ingrese más gas al horno y se produzca una explosión se decidió en este caso colocar un SIS para que actúe en el caso de que el lazo básico de control falle. El SIS está formado por un sensor de presión de seguridad (PT2) un interpretador de lógica (LS) y una válvula controladora de presión de seguridad (PC2). EL SIS funcionará solo en aquel caso en el que el sistema de control básico falle y que la presión salga de sus valores normales. En este caso vemos que sobre el proceso se han colocado dos capas de protección, el sistema básico de control de procesos y el SIS. Cabe mencionar que el diseño y construcción del SIS se realiza bajo estándares mucho más estrictos y su probabilidad de falla es mucho menor que los del lazo de presión original.

Un concepto importante a tener en cuenta es la independencia de las capas de protección. Cualquiera sea el tipo de protección que se coloque sobre un proceso es necesario que la función de una capa no se vea afectada por el mal funcionamiento o falla de la otra capa. La necesidad de colocar una segunda capa de protección, en este caso el SIS, surge de estudios sistemáticos y minuciosos establecidos en la norma IEC 61511.

Un sistema de seguridad puede estar encargado de realizar una o varias tareas relacionadas a la seguridad. Cada una de esas tareas son denominadas “Funciones de Seguridad” las cuales al ser realizadas mediante un sistema instrumentado se las define como “Funciones Instrumentadas de Seguridad”.

Una Función Instrumentada de Seguridad (SIF) es una función a ser implementada por un SIS la cual tiene por finalidad lograr mantener el proceso en un estado seguro frente a un evento peligroso específico.

En otras palabras una SIF es un conjunto formado por una serie de acciones específicas y sencillas y un equipo E/E/PE, necesario para identificar un peligro especifico y actuar de tal forma que puedan evitarse resultados peligrosos.

Un SIS puede abarcar múltiples SIF cada una de las cuales tendrá como objetivo ejecutar una acción diferente para llevar al proceso a un estado seguro. La implementación de una función de seguridad puede incluir múltiples elementos sensores, módulos acondicionadores de señal, diversos elementos finales y servicios auxiliares específicos tales como alimentación eléctrica o aire de instrumentos.

Además de los conceptos de SIS y SIF la norma introduce otro concepto importante que es el ciclo de vida de la seguridad [8].

Por ciclo de vida de la seguridad se entiende al proceso que va desde la visualización de la necesidad de contar con un sistema instrumentado de seguridad hasta la etapa de desmantelamiento final de dicho sistema de seguridad. Básicamente el Ciclo de Vida de Seguridad consta de tres fases [2]:

1) Fase de análisis
2) Fase de realización o implementación
3) Fase de operación

La fase de análisis define que grado de seguridad necesita un determinado proceso. La fase de implementación está destinada a especificar como se obtiene la seguridad que se necesita y la fase de operación a mantener la seguridad en todo momento. Cada una de estas fases a su vez cuenta con distintas tareas a llevar a cabo para lograr los objetivos deseados.

La fase de implementación tiene especial significación para esta tesis debido a que es la fase que establece, entre otros puntos, los requerimientos que debe tener el software a ser utilizado en los equipos electrónicos programables (PE) a los que hace referencia la norma y, dentro de las características del software, los requisitos a cumplir por los buses de comunicación de los sistemas de seguridad.

El otro concepto que introduce la norma es el de los niveles de seguridad llamados SIL (Safety Integrity Levels). Los niveles de seguridad son una medida de cuan confiable es un sistema instrumentado de seguridad. La noma reconoce cuatro niveles de seguridad integral siendo el nivel menos estricto el nivel uno y el más estricto el nivel cuatro.

Antes de continuar con la descripción de los niveles de seguridad de un sistema instrumentado de seguridad describiremos los tipos de falla y

los modos de operación que reconoce la norma en los sistemas de seguridad.

a) Tipos de falla [20]

- Falla aleatoria (de hardware)
- Falla sistemática

La falla aleatoria está relacionada a los conceptos de fortaleza y estrés de los componentes del sistema y es posible cuantificarla de tal forma que se puede estimar cuál será la tasa de falla de un determinado componente. La falla aleatoria es una falla que ocurre en un momento cualquiera como resultado de uno o más mecanismos de degradación. Usualmente es una falla permanente debido a la pérdida de funcionalidad de un componente del sistema relacionado con el hardware.

La falla sistemática es una falla relacionada de manera determinística con cierta causa, la cual sólo puede ser eliminada mediante modificación del diseño o del proceso de fabricación, procedimientos operacionales, documentación u otras técnicas específicas. Las fallas debidas al software son fallas sistemáticas. Las fallas de programación también son fallas sistemáticas.

Las normativas de la Seguridad Funcional protegen contra fallas sistemáticas mediante reglas, guías, procedimientos y metodologías que permiten prevenir errores de diseño.

b) Modos de operación [20]

De acuerdo a la norma IEC 61511 el modo de operación de los sistemas instrumentados de seguridad se clasifican en:

- Modo en demanda
- Modo continuo

Modo “en demanda” es aquel en el que la frecuencia de demanda de operación sobre el sistema de seguridad no es mayor a una vez al año, ni mayor al doble del período de pruebas de funcionamiento.

Modo “continuo” es aquel en que la demanda de operación sobre el sistema de seguridad es permanente o que la frecuencia de la demanda es mayor que una vez por año, o mayor al doble de la frecuencia del intervalo de pruebas periódicas.

Para cada modo de operación la norma establece la probabilidad de falla esperada del sistema lo que da lugar a los denominados niveles de integridad de seguridad ó SIL (Safety Integrity Levels).

Los niveles de integridad en el modo de baja demanda indican la probabilidad de falla ante una demanda de acción del sistema. Los niveles de integridad en modo continuo se especifican en fallas por hora (FPH) de funcionamiento [2].

Nivel de Seguridad en Integridad	Probabilidad Promedio de Falla en Demanda (modo de operación en baja demanda)	Factor de Reducción de Riesgo (RRF)
SIL 4	$\geq 10^{-5}$ a $< 10^{-4}$	100000 a 10000
SIL 3	$\geq 10^{-4}$ a$< 10^{-3}$	10000 a 1000
SIL 2	$\geq 10^{-3}$ a $< 10^{-2}$	100 a 100
SIL 1	$\geq 10^{-2}$ a$< 10^{-1}$	100 a 10

Gráfico 2.13 - Niveles de integridad en seguridad – Modo en baja demanda

Nivel de Seguridad en Integridad	Probabilidad de Falla (Modo de Operación Continuo) (Fallas por Hora)
SIL 4	$\geq 10^{-9}$ a $< 10^{-8}$
SIL 3	$\geq 10^{-8}$ a $< 10^{-7}$
SIL 2	$\geq 10^{-7}$ a $< 10^{-6}$
SIL 1	$\geq 10^{-6}$ a $< 10^{-5}$

Gráfico 2.14 - Niveles de integridad en seguridad – Modo en alta demanda

Los cálculos de las probabilidades de falla de los diferentes componentes del sistema exceden el alcance de esta tesis por lo que no serán desarrollados en la misma.

Los conceptos importantes a tener en cuenta de la norma son:

- Las fallas debidas a errores en software o a errores en la programación de los equipos electrónicos programables son fallas sistemáticas.
- El modo de operación del software o del programa de un sistema de seguridad es considerado de modo continuo por lo que aplica la segunda tabla de Niveles de Integridad de la Seguridad.
- La probabilidad de falla de un sistema de seguridad es la sumatoria de las probabilidades de falla de todos los componentes integrantes del sistema.
- La probabilidad de falla está inversamente relacionada con la capacidad de reducción de riesgo. A menor probabilidad de falla mayor factor de reducción de riesgo.

La capacidad de reducción de riesgo de un sistema instrumentado de seguridad está directamente relacionada con la capacidad de diagnóstico

del sistema. Mientras mayor sea la capacidad del sistema de detectar fallas, menor será la posibilidad de que existan fallas ocultas.

Para afirmar los conceptos desarrollados podemos indicar que toda actividad productiva conlleva algún tipo de riesgo. Cuando el riesgo es elevado hay que reducirlo hasta llegar a la zona A.L.A.R.P. y dentro de ella, disminuirlo todo lo que sea prácticamente posible. Para minimizarlo o reducirlo se colocan capas de protección. Una de las posibles capas de protección son los sistemas automáticos de seguridad. La existencia o no de estos sistemas depende del estudio de evaluación de riesgo que sea llevado a cabo para cada proyecto en particular. De existir la necesidad de instalar un sistema automatizado de este tipo los diseñadores se remiten a normativas internacionales para definir y diseñar sistemas que logren alcanzar la reducción de riesgo deseada. La norma internacionalmente aceptada es la IEC 61508. Esta norma establece el nivel de reducción de riesgo en base a cuatro niveles llamados SIL. Por ende sabiendo el SIL se conoce el factor de reducción de riesgo logrado por el sistema. El SIL del sistema está vinculado a la sumatoria de las probabilidades de falla de los componentes integrantes del sistema. Dentro de estas probabilidades de falla están incluidas las fallas por software. Este tipo de fallas son del tipo sistemática y son evaluadas sobre un sistema de alta demanda o de funcionamiento continuo.

Un SIS aplicado a la industria de proceso costa básicamente de los elementos sensores, del módulo interpretador de lógica y de los actuadores. Entre el procesador de lógica y los elementos finales (sensores y actuadores) se ubican los módulos de entrada/salida que tienen la función de agrupar las señales provenientes de campo y se comunican con el procesador vía un bus de campo que debe ser un “bus de campo seguro”. La probabilidad de falla debida a la comunicación en

este bus de campo seguro aporta a la sumatoria de probabilidades de falla que hacen al nivel SIL del SIS.

En la práctica se considera que, como máximo, el 15% de la probabilidad de falla del sistema se puede atribuir al procesador y el 85% al resto de los componentes del sistema como son actuadores y sensores.

Dentro del 15% atribuible al interpretador de lógica se considera que sólo el 1% es debido a fallas en el procesador y/o en el bus de campo seguro. Si para un SIS de nivel SIL 3 la probabilidad de falla es ≥ 10^{-8} a < 10^{-7}, entonces la probabilidad de falla del bus de campo debe estar entre ≥ 10^{-10} a < 10^{-9} horas.

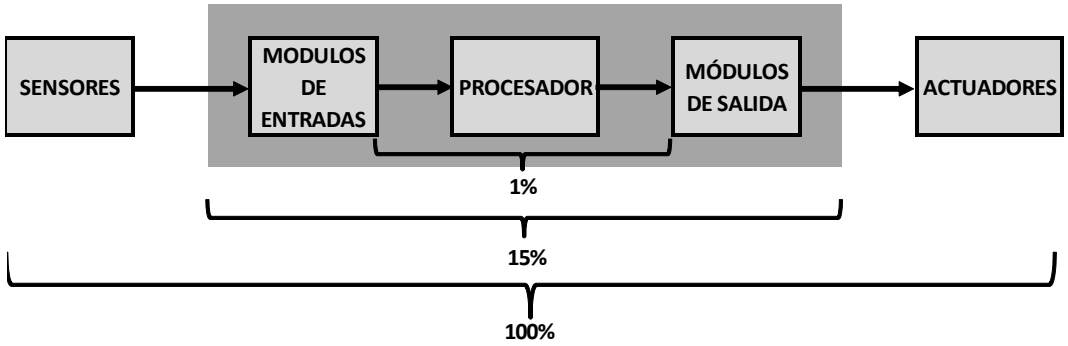

Gráfico 2.15 - Porcentaje de probabilidad de falla en un sistema electrónico programable

A nivel internacional existen organizaciones como el TÜV de Alemania o Exida de EE.UU que se encargan, a pedido del fabricante, de realizar la certificación de los productos para determinado nivel de SIL.

Como vemos un bus de campo de seguridad debe cumplir con requerimientos muy estrictos. Los buses de campo seguros utilizan protocolos certificados para la comunicación entre los distintos módulos, estos protocolos son conocidos como Safety Protocols (protocolos seguros). Dentro de los protocolos de seguridad se encuentran los

protocolos seguros basados en Ethernet o comúnmente denominados “Safety Ethernet” uno de los cuales será utilizado para la implementación práctica de esta tesis.

Los protocolos Safety Ethernet más conocidos son PROFINET, Sercos III, Ethernet/IP Safety y openSafety.

2.11 Canal Negro (Black Channel)

Si bien es cierto que dentro del cálculo de la probabilidad de falla por hora (PFH) es posible incluir la falla de hardware no tiene sentido atar un determinado tipo de comunicación a un hardware específico [6]. Debido a esto muchos de los buses seguros de la actualidad hacen uso del concepto de canal negro.

El concepto de canal negro (black channel) deriva del concepto de caja negra (black box). El concepto de caja negra implica que lo que interesa es la entrada y el resultado a la salida de la caja sin tener en cuenta lo que existe o sucede en el en dicha caja. Sólo cuenta que se ingresa un dato a la entrada y se obtiene un dato a la salida, sin interesarse de los procesos internos que se desarrollan en la caja negra para lograr el resultado de salida. El concepto de black channel es similar al de la caja negra con la diferencia de que la caja negra suele ser una pieza de hardware mientras que el bus o canal de comunicación es transparente para la seguridad del sistema, es decir pareciera no estar allí. El bus de campo no ejecuta ninguna función relacionada con la seguridad y sólo se utiliza como el medio de transporte de la información.

En contraposición al concepto de black channel se encuentra el concepto de “white channel” o canal blanco. En este caso se requeriría que todos los componentes de hardware y software del canal de comunicación seguro fuesen diseñados y construidos bajo los estrictos

estándares de la normativa internacional de seguridad (IEC 61508 y otras). Esto es, todos los componentes del canal de comunicación, interfases, convertidores, repetidores, switchs, routers, cables, conectores, barreras de seguridad, etc. necesitarían de la correspondiente certificación para poder ser usados en el canal de comunicación seguro.

El concepto de black channel utiliza un bus no seguro para llevar a cabo la transmisión. Como gran ventaja el black channel permite utilizar hardware estándar y no seguro para la construcción de redes seguras.

Al no realizase ningún cambio en las capas físicas de la red de comunicación es necesario incorporar funciones relacionadas a la seguridad en una capa ubicada por encima del stack de comunicación y por debajo de la capa de aplicación en el modelo de capas OSI. Esta nueva capa es la encargada de que los datos a transferir lo hagan con una confiabilidad tal que permita asegurar un servicio de comunicación seguro. La capa de seguridad es la encargada de ejecutar todas las funciones de seguridad relacionadas con la transmisión de datos y es la que verifica permanentemente la integridad del enlace. Con el esquema de black channel se puede llegar a cumplir los requerimientos necesarios de SIL 3 en modo de alta demanda.

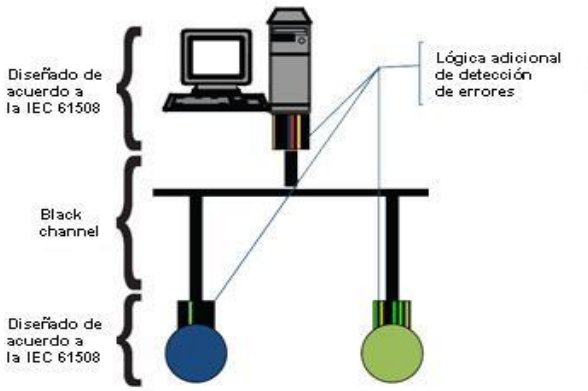

Gráfico 2.16 - Concepto de Canal Negro o "Black Channel"

El mismo medio de comunicación es compartido por los datos seguro y no seguros. Dispositivos seguros y no seguros también pueden estar conectados físicamente en el mismo bus sin perjudicar la seguridad del bus.

Para cumplir con los exigentes requerimientos de seguridad, un dato seguro debe poder pasar sin modificaciones desde el transmisor-seguro al receptor-seguro sin importar que tipo de sistema de transmisión se esté utilizando.

Un punto por más determinante para que un bus sea seguro es la capacidad del bus de detectar errores. En el caso del black channel no se utilizan los mecanismos de detección de errores del propio medio de comunicación sino que la capa de seguridad provee y ejecuta sus propios mecanismos de seguridad. Estas “medidas de seguridad” viajan encapsuladas entre los nodos o dispositivos entre los que se establece la comunicación.

Básicamente no hay restricciones en la velocidad de transmisión, en el número de dispositivos conectados o tipo de hardware usado mientras los tiempos de reacción de la aplicación de seguridad puedan estar garantizados.

La detección de datos corruptos vía el uso de un chequeo de redundancia cíclica (CRC) adicional cumple un rol fundamental a la hora de cumplir con los requerimientos de seguridad del bus.

La IEC 61508 considera la probabilidad de falla de un circuito seguro como la sumatoria de fallas de todos los componentes que integran dicho circuito. Esto es incluye todos los sensores, los actuadores los medios de transferencia de datos (esto es el bus seguro) y los procesos lógicos que se desarrollan en la función de seguridad. En el diseño de un sistema

seguro una pequeña porción de la probabilidad de falla de todo el sistema se reserva para el bus seguro siendo esta porción usualmente del 1% al 2% de la probabilidad de falla total. Es decir que esta es la porción de probabilidad de falla reservada para el black channel. Para el caso de un sistema que es apto para trabajar en SIL 3 la probabilidad de falla en alta demanda o modo continuo es de 10^{-7}/h entonces la probabilidad de falla del black channel deberá ser de 10^{-9}/h. Seleccionando un adecuado polinomio (que se corresponda con la longitud del marco usado en la comunicación) se puede construir un CRC que asegure que se cumple con el error residual de la probabilidad de falla en la detección de datos corruptos no detectados. Así el black channel se independiza del sistema de detección de errores del protocolo de comunicación del bus de campo estándar ya que utiliza su propio sistema de detección de errores.

Además de un CRC propio el black channel realiza otras mediciones de seguridad para asegurarse que los errores de los datos recibidos por el nodo seguro están por debajo del límite máximo permitido para el SIL deseado.

El siguiente cuadro muestra cuales son los posibles errores en una transmisión de datos y cuáles son las probables mediciones que deben implementarse en el black channel para minimizar los errores de comunicación.

ERROR	MEDICIÓN			
	NUMERACIÓN CONSECUTIVA	TIME OUT	NOMBRE DE CÓDIGO (PARA EMISOR Y RECEPTOR)	INTEGRIDAD DEL DATO (CRC)
REPETICIÓN DEL DATO	X			
PÉRDIDA DEL DATO	X	X		
INSERCIÓN	X	X	X	
SECUENCIA INCORRECTA	X			
CORRUPCIÓN DEL DATO				X
RETARDO DEL DATO		X		
ENMASCARAMIENTO (CON MSJ ESTÁNDAR)		X	X	X
FIFO (ERRORES EN ROUTERS INTERMEDIOS)		X		

Tomado de "The Industrial Communication Technology Handbook", Richard Zurawski, CRC Press 2005, pp. 28-1-28-19.

Gráfico 2.17 - Medidas de seguridad en protocolos seguros

Algunas medidas para detectar errores son:

- Numeración consecutiva: Confirmar que el mensaje transmitido es recibido y reensamblado en la secuencia correcta es importante especialmente para aquellos mensajes que tienen la opción de tomar más de una ruta para llegar desde el transmisor al receptor.
- Time Out: En la actualidad existen muchos buses de campo que tiene alguna forma de mecanismos de confirmación de recepción de mensajes. Sin embargo la mayoría de los protocolos Ethernet industrial usan UDP como protocolo de transporte el cual no posee algún método de confirmación de recepción de mensajes, por lo tanto se hace indispensable que el black channel disponga su propio sistema.
- Nombre de código (Codename): Es el método utilizado para asegurar que el mensaje es transferido entre los dos nodos finales entre los que se quiere establecer la comunicación y no otros nodos.

El utilizar una capa de seguridad como es el black channel permite a los fabricantes poder alcanzar los límites impuestos por la IEC 61508 [7]

en forma más sencilla y económica. El protocolo de seguridad es independiente del protocolo de transporte utilizado (Foundatin fieldbud, Modbus/TCP, Ethernet-IP, etc) y todos los mecanismos de seguridad son provistos por el protocolo seguro.

El concepto de black channel asegura que la confiabilidad en la seguridad del SIS es independiente del canal de comunicación utilizado.

CAPITULO III

3. Estado del Arte

3.1 PROFINET

3.1.1 Características de PROFINET

PROFINET es el estándar Ethernet abierto de PROFIBUS y PROFINET International (PI). PROFINET es 100% compatible con Ethernet de acuerdo a la IEEE 802.3. Este protocolo está estandarizado de acuerdo a IEC 61158 y la IEC 61784-2. Algunas características relevantes son:

- 100 Mbps de transmisión de datos sobre cobre o de transmisión sobre fibra óptica (100 Base TX y 100 Base FX)
- Transmisión full duplex
- Ethernet basado en switchs
- Autonegociación de los parámetros de transmisión
- Autocrossover (uso de cables directos o cruzados)

PROFINET utiliza UDP/IP como protocolo para el intercambio de datos a demanda. En paralelo al uso de UDP/IP el intercambio cíclico de datos en tiempo real se hace a través de TCP.

PROFINET está compuesto por dos protocolos PROFINET CBA y PROFINET IO [12]. PROFINET CBA (Component Based Automation) es utilizado para la comunicación en tiempo real entre controladores ya sea dentro de una misma o entre distintas máquinas. PROFINET IO se utiliza para la comunicación entre el controlador y la periferia distribuida en un

sistema de control. PROFINET IO permite dos modos de transmisión en tiempo real: RT (Real Time) e IRT (Isochronous Real Time) cuya diferencia radica en la velocidad de respuesta en la transmisión. PROFINET CBA y PROFINET IO pueden trabajar en combinación o en forma separada de acuerdo a los requerimientos del proyecto que se esté llevando a cabo. En esta tesis trabajaremos con PROFINET IO por lo que serán descriptas las características de este protocolo, no así las de PROFINET CBA.

En PROFINET IO RT todos los datos de proceso y alarmas se transmiten en tiempos de intercambio de datos en ciclos que están en el orden de las decenas de milisegundos. En el caso de PROFINET IRT los tiempos de intercambio de información están en el orden de los pocos microsegundos. PROFINET IRT tiene su gran campo de aplicación en la sincronización de ejes.

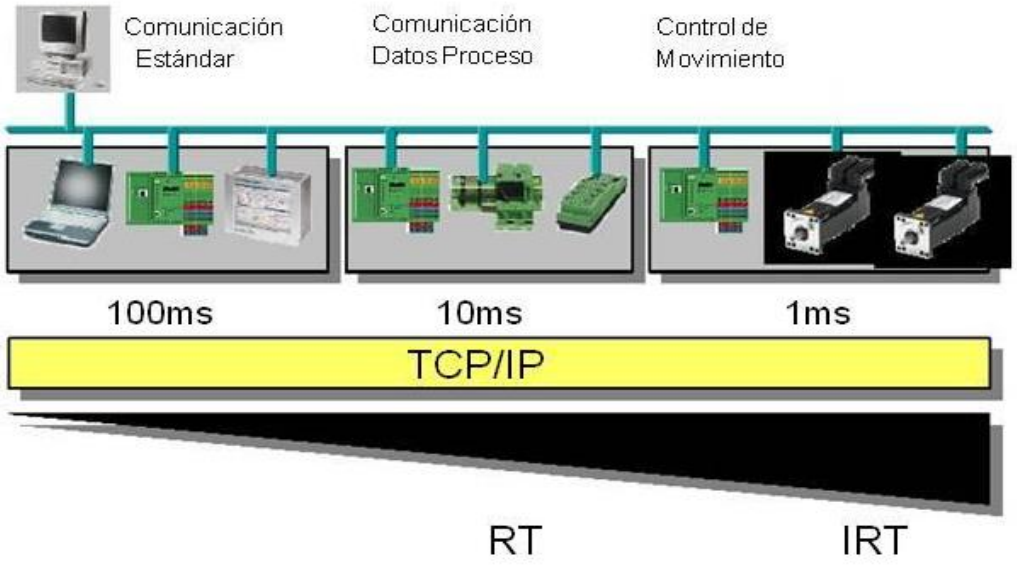

Gráfico 3.1 - Tiempos de transmisión de PROFINET

Los dispositivos de campo PROFINET IO son direccionados teniendo en cuenta su MAC y su dirección IP. La asignación de una dirección IP particular a un dispositivo de campo la realiza el Controlador IO utilizando el Protocolo DCP (Discovery Configuratin Protocol). Como alternativa en algunos casos es utilizado DHCP. Todos los dispositivos de campo son identificados por sus propiedades de funcionamiento y sus características técnicas en un archivo denominado GSD (General Station Description) que es creado por el fabricante del dispositivo de campo.

3.1.2 Comunicación en PROFINET IO

PROFINET IO incluye protocolos para los siguientes servicios [12]:

- Resolución de direcciones para los dispositivos de campo.
- Transmisión cíclica de datos de entrada salida (modos RT e IRT).
- Transmisión acíclica de alarmas.
- Transmisión acíclica de datos de configuración, parámetros diagnósticos, etc.
- Redundancia para la información en tiempo real.

La combinación de estos servicios de comunicación en el nivel más alto del stack hace posible implementar servicios de diagnósticos, detección de topologías y reemplazos en línea de equipamientos, entre otros servicios.

La comunicación RT en PROFINET se basa en un intercambio cíclico de información utilizando el modelo productor/consumidor. El productor es usualmente el dispositivo en campo y el consumidor es el PLC o controlador.

Los mecanismos de comunicación de capa dos (de acuerdo al modelo IS/OSI) son suficientes para esto. Para ello se utiliza el concepto de VLAN

de acuerdo a la IEEE 802.1Q (priorización de marcos de datos) y en particular el ethertipo 0x8892 que permite una rápida transmisión de los marcos PROFINET en las capas superiores del dispositivo de campo. Los marcos RT son automáticamente priorizados en comparación con los marcos UDP/IP. Esto es necesario para priorizar la transmisión de los datos en los switchs a fin de evitar que los marcos RT se vean demorados por los marcos UDP/IP. Este tipo de comunicación es soportada por hardware estándar sin que tenga que poseer características especiales.

En PROFINET IO se han definido varias clases de comunicación RT:

RT_CLASS_1: Es una comunicación RT asincrónica dentro de la subred. Es la más comúnmente utilizada y se la usa en paralelo con la comunicación UDP/IP. Para la priorización se utiliza el ethertipo 0x8892 y el marco es enviado por el canal RT en forma inmediata para su procesamiento. Switchs industriales estándar pueden utilizarse para este tipo de comunicación.

RT_CLASS_2: Los marcos pueden enviarse en forma síncrona o asíncrona. Para el caso de la comunicación asíncrona los marcos tiene el mismo tratamiento que los de clase 1. Para la comunicación síncrona se define en forma precisa el comienzo del ciclo del bus para todos los nodos estableciendo el tiempo exacto de transmisión de datos. Para este tipo de comunicación es necesario contar con hardware especializado que soporte la operación síncrona.

RT_CLASS_3: Es un método de comunicación síncrono en donde la máxima desviación en el inicio del ciclo del bus es de 1 µseg. No hay demoras de ningún tipo en la comunicación y es necesario contar con hardware especializado. Esta comunicación es conocida como IRT (Isochronous Real Time).

RT_CLASS_UDP: Es una comunicación asíncrona que se utiliza para la comunicación entre diferentes subredes. Switchs convencionales se pueden utilizar para este tipo de comunicación.

Los datos transmitidos cíclicamente en tiempo real lo hacen sin “acknowledges” entre el proveedor y el consumidor y la comunicación es monitoreada a través de “watchdogs”. Los eventos y alarmas del sistema son enviados vía una comunicación acíclica. Los mensajes multicast son transmitidos desde un productor a múltiples nodos a través de un mecanismo desarrollado en PROFINET denominado Multicast Communication Relation. Este mecanismo permite enviar información en forma directa desde el productor a varios, o a todos los consumidores. Dentro de un segmento se utilizan mensajes RT y si la información debe enviarse a otros segmentos se los hace utilizando mensajes RT_CLASS_UDP.

El intercambio de información acíclica se utiliza con los fines de parametrizar y configurar los nodos I/O. Esto se realiza a través de mensajes de lectura/escritura utilizando los mecanismos estándar IP/UDP

Todos los dispositivos de campo PROFINET IO se conectan a través de switches y pueden ser identificados en la red de forma unívoca a través de su interfaz PROFINET. Para ello cada interfaz PROFINET dispone de:

- una dirección MAC (ajustada de fábrica)
- una dirección IP
- un nombre (NameOfStation)

Los switchs en SIMATIC (productos Siemens utilizados en esta tesis) cumplen con las propiedades de tiempo real en PROFINET con dos mecanismos: "Store and Forward" y "Cut through".

La comunicación isócrona en tiempo real es un procedimiento de transferencia en el que una parte del tiempo de transferencia está reservado para la transferencia de datos cíclica.

Para ello, el ciclo de comunicación se divide en una parte determinista y en una parte abierta. En el canal determinista se transportan los telegramas IRT cíclicos, mientras que los telegramas TCP/IP y RT se transportan en el canal abierto. De este modo, las dos transferencias de datos coexisten sin molestarse.

Con la implementación del procedimiento de transferencia en ERTEC-ASICs (Enhanced Real-Time Ethernet Controller) se consiguen tiempos de ciclo de 0,25 ms y una precisión de inestabilidad a corto plazo de menos de 1 µs.

Los dispositivos PROFINET se integran a través de un archivo GSD. Las características de un dispositivo PROFINET se describen en estos archivos GSD (General Station Description) que contienen todos los datos necesarios para la configuración.

En PROFINET IO, el archivo GSD está disponible en formato XML. La estructura del archivo GSD cumple la ISO 15745, el estándar internacional para descripciones de dispositivos.

Todos los dispositivos PROFINET se basan en el protocolo TCP/IP y requieren, por tanto, una dirección IP para funcionar en la Ethernet.

Las direcciones IP de los dispositivos I/O tienen siempre la misma máscara de subred que el controlador I/O y se asignan en orden ascendente a partir de la dirección IP del controlador I/O. En caso necesario, esta dirección IP puede modificarse manualmente.

Para que un dispositivo I/O pueda ser direccionado por un controlador I/O, es necesario que posea un nombre de dispositivo, ya que la dirección IP está asignada de forma fija al nombre de dispositivo. En PROFINET se ha elegido este procedimiento porque es más fácil manejar nombres que direcciones IP complejas.

De forma estándar, el dispositivo I/O no posee ningún nombre. Sólo tras asignarle un nombre de dispositivo con la PG o el PC (elementos de configuración), el dispositivo I/O podrá ser direccionado por el controlador I/O, p. ej. para transferir los datos de configuración (incluida la dirección IP) durante el arranque o para intercambiar datos en funcionamiento cíclico.

Además del nombre del dispositivo, al conectar un dispositivo I/O, STEP 7 (software de Siemens para la configuración del sistema) también asigna un número de dispositivo, comenzando por "1".

Mediante este número de dispositivo se puede identificar el dispositivo I/O en el programa de usuario. A diferencia del número de dispositivo, el nombre del dispositivo no se puede ver en el programa de usuario.

3.1.3 Dianóstico de Red

El diagnóstico de la red se lleva a cabo utilizando el protocolo de gestión de redes simples SNMP (Simple Network Management Protocol) que utiliza el protocolo de transporte UDP sin conexión. Este protocolo comprende dos componentes de red, similares al modelo cliente/servidor. El gestor SNMP monitoriza los nodos de la red, en tanto que los agentes SNMP recopilan en los diversos nodos las informaciones específicas de la red y las depositan de forma estructurada en la MIB (Management Information Base). Con esta información, un sistema de administración de redes puede realizar un diagnóstico detallado de la red.

3.1.4 Detección de la Topología de Red

LLDP (Link Layer Discovery Protocol) [13] es un protocolo que permite detectar los equipos más próximos. Gracias a este protocolo, un equipo puede enviar informaciones sobre sí mismo, así como guardar en la MIB LLDP las informaciones recibidas de sus equipos vecinos.

Estas informaciones se pueden consultar vía SNMP. Con esta información, un sistema de administración de redes puede determinar la topología de la red. El protocolo LLDP es implementado vía software por lo que no requiere algún soporte de hardware especial.

En los dispositivos PROFINET de campo la resolución de direcciones está basada en el nombre simbólico del dispositivo el cual está asociado a su dirección MAC. Luego de que el sistema se ha configurado, la herramienta de ingeniería carga toda la información requerida para el intercambio de datos en el controlador I/O inclusive las direcciones IP de los dispositivos I/O que posee conectados. Basado en el nombre y en su (dirección MAC asociada) el controlador I/O puede reconocer los dispositivos de campo que están configurados y asignarles una dirección IP utilizando el protocolo DCP (Discovery and Configuration Protocol) que se encuentra integrado en PROFINET IO. En forma alternativa el direccionamiento puede ser realizado a través de un servidor DHCP.

3.1.5 Clases de Conformidad de Hardware

En la actualidad PROFINET cubre todos los requerimientos de perfomance para las exigencias de los distintos proyectos de ingeniería, desde proyectos menos exigentes como pueden ser plantas de proceso hasta proyectos en donde las exigencias son altas como por ejemplo en la sincronización de ejes. No es necesario entonces para una determinada ingeniería contar con todas las funciones de PROFINET sino sólo con

aquellas que son suficientes para desarrollar el proyecto en forma satisfactoria. Por lo tanto PROFINET puede ser escalado de acuerdo a las funcionalidades necesarias y se han clasificado eses funcionalidades en las llamadas clases de conformidad (CCs) en donde cada una tiene un determinado alcance. Como resultado de esto es más fácil para los desarrolladores de la ingeniería seleccionar dispositivos de campo y componentes del bus que explícitamente cumplen con las características mínimas requeridas. Todos los dispositivos dentro de la clase de conformidad elegida reúnen los requerimientos mínimos necesarios. Una detallada descripción de las clases de conformidad pueden encontrarse en el documento “PROFINET Conformace Classes” de PNO.

Las CCs definidas son tres y las áreas de aplicación de las mismas son:

- CC-A: Se hace uso de la infraestructura de Ethernet ya instalada y se incluyen las funcionalidades básicas de PROFINET. Todos los servicios de IT se pueden utilizar sin restricciones. Típicas aplicaciones de esta clase se dan en la automatización de industria de proceso y de edificios. La comunicación inalámbrica (wi-fi) es posible en esta clase de conformidad.
- CC-B: A las propiedades de la CC-A se suman en esta clase la posibilidad de reemplazo de dispositivos sin la necesidad de contar con una herramienta de ingeniería determinada. Ejemplos de esto se dan en sistemas de automatización con un alto grado de control de máquinas en donde las demandas de determinismo son relativamente bajas.
- CC-C: Además de las funcionalidades de la CC-B esta clase soporta transmisión de datos de alta precisión y determinismo incluyendo aplicaciones isócronas. La redundancia, ya integrada en

esta clase, posibilita la continuidad de la cadena de datos sin inconvenientes si se produce alguna falla. Un ejemplo típico de la aplicación de esta clase se da en el campo del control de movimientos.

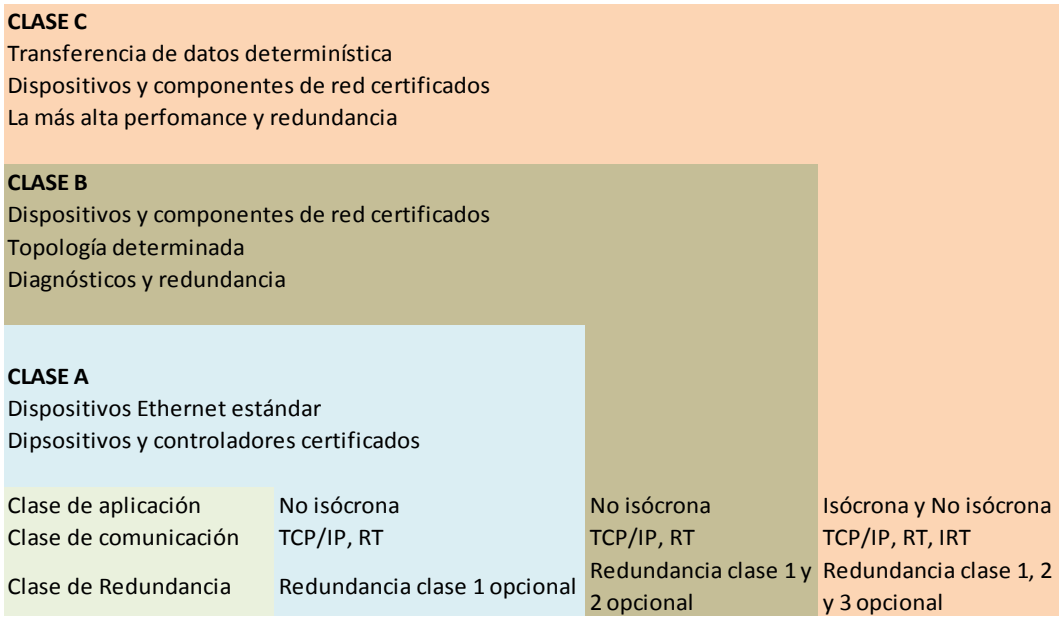

Gráfico 3.2 - Clases de conformidad de hardware de PROFINET

3.1.6 Marco PROFINET RT

La siguiente imagen muestra el marco PROFINET y la utilización de V-LANS para el manejo de mensajes en RT.

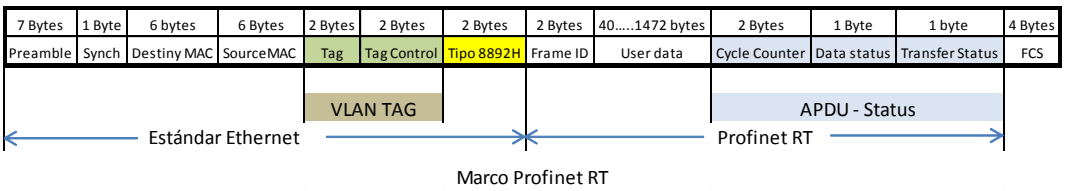

Gráfico 3.3 – Marco PROFINET

El marco PROFINET RT se corresponde con el marco estandarizado definido en la IEEE 802.3. Hace uso de V-LANs de acuerdo con la IEEE

802.1Q con lo cual prioriza los mensajes y utiliza para indicar que se trata de un marco PROFINET el ethertype 0x8892. Dentro del espacio propiamente reservado a PROFINET encontramos dos bytes destinados al Frame ID o Application ID que informa sobre los datos recibidos, si corresponden a datos de transmisión cíclica o si corresponden a datos de transmisión acíclica (eventos o alarmas). Posteriormente aparecen los datos de proceso y por último cuatro bytes destinados a conocer el estado de la comunicación y de los dispositivos.

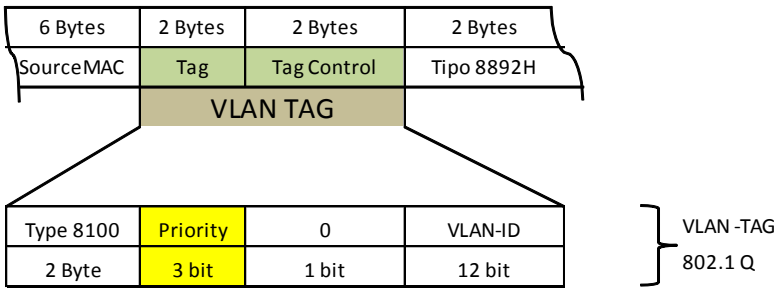

Gráfico 3.4 - V-LAN TAG 802.1 Q

3.2 PROFIsafe

3.2.1 Caracterísiticas de PROFIsafe

La tecnología PROFIsafe es una capa adicional que se ubica por encima de las capas de aplicación formadas por los protocolos PROFIBUS o PROFINET. Este protocolo permite transmitir mensajes seguros junto con mensajes estándar en el mismo canal de comunicaciones y reduce la probabilidad de ocurrencia de errores en la transmisión de datos entre un controlador seguro y un dispositivo de campo seguro. En nuestro caso PROFIsafe es el protocolo seguro que se monta sobre PROFINET para darle seguridad a la transmisión de datos. PROFIsafe está desarrollado solamente en software por lo que es de útil implementación en proyectos de automatización de fábricas e industrias

de proceso. También es posible utilizarlo en medios de transmisión inalámbricos tales como WLAN y Bluetooth con las precauciones de seguridad necesarias. Este trabajo utiliza PROFIsafe para darle seguridad en la transmisión de datos vía un enlace radial.

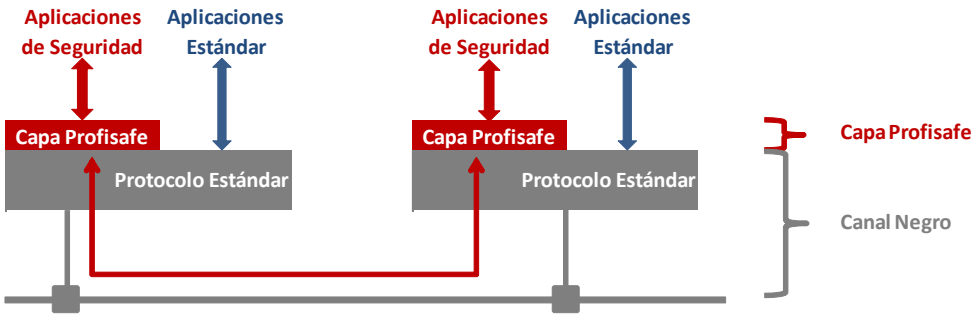

Gráfico 3.5 - (Ethernet Industrial) Canal Negro - Profisafe sobre Profinet IO

PROFIsafe puede ser usado para aplicaciones de seguridad hasta SIL 3 de acuerdo a la norma IEC 61508 / IEC62061 o categaría 4 de acuerdo a la norma EN 954-1 o PL “e” de acuerdo a la ISO 13849-1.

PROFIsafe hace uso del concepto de “canal negro” [19] y no tiene impacto sobre la perfomance de los protocolos sobre los que se encuentra montado. Como todos los protocolos que hacen uso del canal negro es independiente de los medios de transmisión utilizados, de las velocidades de transmisión y de los mecanismos de detección de errores de los protocolos base.

PROFIsafe hace uso de algunos principios básicos de comunicación para su implementación. Uno de ellos es la comunicación cíclica entre el controlador y sus dispositivos de campo asociados. Esta forma de comunicación basada en el principio de envío y recepción de respuestas (polling) sirve para detectar en forma inmediata la falla de un dispositivo. El otro principio que usa PROFIsafe es la comunicación 1 a 1 entre el

controlador del bus y sus dispositivos de campo, esto sirve para asegurar la autenticidad de los mensajes.

Para PROFIsafe cualquier tipo de switch puede ser utilizado y se pueden conectar en línea hasta cien de estos dispositivos. La dirección segura dentro de una isla PROFIsafe debe ser única. Islas PROFIsafe que poseen el mismo espacio de direcciones seguras sólo pueden ser conectadas a través de routers con multipuertos.

Muchos son los errores que pueden producirse en los mensajes que se transmiten entre dos dispositivos en redes complejas debido a fallas de hardware, interferencias electromagnéticas, demoras en dispositivos activos u otras influencias. Los mensajes pueden perderse, repetirse, insertarse en algún lugar, demorarse, aparecer en secuencias incorrectas o mostrar información corrupta. Además en el caso de mensajes seguros se puede dar un error de direccionamiento en el caso de que a un dispositivo seguro le llegue un mensaje estándar como si fuese un mensaje seguro. También puede producirse demoras en los componentes activos del bus debido a diferentes velocidades de transmisión que puedan existir en la red.

Ante estos problemas PROFIsafe establece una serie de mecanismos de seguridad que permiten minimizar estos errores y poder ser utilizado en sistemas de hasta SIL 3. Estos mecanismos de seguridad son [14] [19]:

Mecanismo / Error	Números consecutivos (Signo de vida)	Fuera de tiempo (Time out)	Nombre de código (Para emisores y receptores)	Integridad de los datos (CRC)
Repetición	X			
Pérdida	X	X		
Inserción	X	X	X	
Secuencia incorrecta	X			
Datos corruptos				X
Retardos excesivos		X		
Mal direccionamiento			X	
Enmascaramiento		X	X	X
Fallas de memoria en switches	X			

Gráfico 3.6 - Mecanismos de seguridad de PROFIsafe

Tal como se muestra en el gráfico anterior, PROFIsafe adopta cuatro mecanismos de seguridad para evitar errores en la transmisión.

Con el numerado consecutivo de mensajes el nodo receptor puede determinar si ha recibido completamente todos los mensajes y en la secuencia correcta. Luego de recibido el mensaje, el receptor envía al emisor como señal de reconocimiento un mensaje conteniendo el número consecutivo del mensaje recibido, con lo cual el emisor se asegura que el mensaje llegó correctamente el emisor. Para este mecanismo de seguridad PROFIsafe ha elegido un contador de 24 bits.

Para determinar si el mensaje ha sido recibido dentro del tiempo establecido (time out) se utiliza un mecanismo de “watch dog” de tal forma que el tiempo del mismo es vuelto a cero cada vez que un mensaje consecutivo llega al nodo receptor.

La relación 1 a 1 entre el maestro y el esclavo facilita la detección de mensajes mal direccionados. El emisor y el receptor poseen una identificación que es única en la red y se utiliza para verificar la autenticidad del mensaje. PROFIsafe usa la dirección segura (F-Address) como código de nombre entre receptor y emisor.

Por último un código de redundancia cíclica permite detectar los bits corruptos de la comunicación. La probabilidad de falla impuesta por la IEC 61508 de 10^{-7}/h para sistemas SIL 3 y el porcentaje del 1% que se asume que debe ser como máximo provocado por sistema de comunicación, hace que la probabilidad de fallas peligrosas de PROFIsafe deba ser de 10^{-9}/h. Esto permite entonces calcular los polinomios de CRC adecuados que debe poseer PROFIsafe para cumplir con la probabilidad de máximo error residual de mensajes corruptos no detectados. De acuerdo al tipo de mensaje PROFIsafe usa polinomios CRC de 24 o 32 bits.

Los mecanismos utilizados por PROFIsafe hacen que su detección de errores sea independiente de aquellos procedimientos utilizados por el canal negro (subyacente a la comunicación PROFIsafe) para la detección de mensajes erróneos.

3.2.2 Marco PROFIsafe

Los mensajes PROFIsafe entre el nodo controlador seguro (F-Host) y el nodo de campo seguro (F-Device) viajan como carga útil (payload) dentro del mensaje PROFINET. En el caso de un dispositivo de campo modular que posee varios módulos seguros (F-modules) la carga útil consiste en varios mensajes PROFIsafe. El siguiente cuadro muestra la estructura del marco PROFIsafe.

Dato F-Input/output	Estado / Byte de Control	CRC
		Across Datos F-I/O Parámetros F Números consecutivos
Máximo de12 o 123 Bytes	1 Byte	3 o 4 Bytes

Gráfico 3.7 - Mensaje PROFIsafe

El mensaje PROFIsafe comienza con los datos seguros ya sea de entrada o de salida [19]. La estructura de estos datos depende del tipo de dispositivo particular de campo del que se trate y usualmente (al igual que PROFINET) están definidos en el archivo GSD (General Station Description) provisto por el fabricante.

En general las características de las señales manejadas en la automatización de fábricas y en las instalaciones de proceso difieren entre sí. Las primeras normalmente trabajan con señales cortas (bits) que debes ser procesadas rápidamente mientras que las segundas suelen usar señales más largas (por ej. punto flotante) que necesitan más tiempo de procesamiento. Para cubrir estas necesidades PROFIsafe cuenta con dos longitudes para la estructura de datos. Posee una longitud de datos máxima de 12 bytes que requieren un CRC de 3 Bytes para verificar la integridad de los mismos. Y posee otra longitud de datos máxima de 123 bytes que requiere un CRC de 4 Bytes.

Luego de los datos seguros de entrada o salida se encuentra un byte de control si el mensaje es del F-Host hacia el F-Device o de status si el mensaje va dirigido desde el F-Device al F-Host. Esta información se utiliza para sincronizar los mensajes PROFIsafe entre el emisor y el receptor.

El mensaje PROFIsafe finaliza con un Código de Redundancia Cíclica (CRC) cuya longitud depende el la longitud del mensaje enviado, como vimos anteriormente.

El número de mensaje consecutivo no es transmitido dentro del mensaje PROFIsafe. Tanto el nodo emisor del mensaje como el receptor poseen sus propios contadores y están sincronizados vía el byte de control y el byte de estado. La correcta sincronización es monitoreada vía

la inclusión de los valores de los contadores de mensajes en el cálculo del CRC. La dirección segura también es incluida dentro del CRC para verificar su validez.

3.2.3 Servicios de PROFIsafe

Los mensajes enviados por los transmisores y los receptores de mensajes se ubican en las capas superiores del canal negro. Usualmente estos servicios de PROFIsafe están desarrollados en software a través de los denominados “Drivers”. Su principal funcionalidad es la de controlar el flujo cíclico de datos para procesar los mensajes PROFINET y los estados de excepción como pueden ser el arranque o apagado del sistema, fallas, etc. La siguiente figura muestra cómo es la interacción entre la capa PROFIsafe el programa del usuario y el hardware utilizado [19].

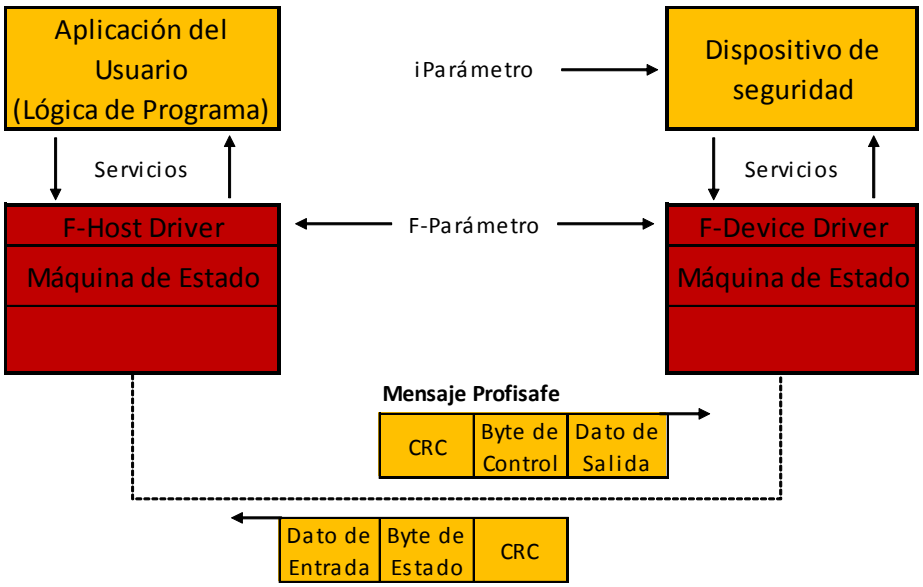

Gráfico 3.8 - Servicios de PROFIsafe

La principal función de los servicios PROFIsafe es el intercambio de mensajes de entrada y salida seguros. Durante el arranque o en caso

de errores los valores de proceso son reemplazados por valores de seguridad ante fallas que llevan al sistema a su estado seguro y que en la mayoría de las acciones es un estado de desenergizado (pasivado). Una vez que se ha producido un error el sistema no vuelve de su estado seguro a un estado normal sino después del reconocimiento de la falla por parte del operador, opcionalmente puede hacerse a través del programa del usuario. Todos estos servicios están incluidos dentro de PROFIsafe.

Los parámetros específicos relacionados con la tecnología de cada dispositivo seguro (F-devices) son denominados iParámetros y son diferentes de acuerdo a la clase de dispositivo que se trate. Diferentes servicios PROFIsafe permiten cargar estos iParámetros en los dispositivos y reasumir su operación normal. La tecnología de los dispositivos seguros permite reportar las fallas al controlador vía una bandera (flag) en el byte de estado.

A su vez los dispositivos seguros también poseen los llamados F-Parámetros que son los parámetros que contiene la información que le permiten a la capa PROFIsafe ajustar su comportamiento de acuerdo a las necesidades particulares del usuario. Los F-Parámetros más importantes son:

- F_S/D_ Address
- F_WD_Time
- F_SIL
- F_iPar_CRC
- F_Par_CRC

La dirección F_S/D_Address es una única dirección para el dispositivo seguro dentro de la isla PROFIsafe. La tecnología del dispositivo tiene que ser capaz de comparar esa dirección con la dirección propia (fijada localmente a través de micro switches u otra tecnología) para asegurar la autenticidad de la conexión.

El parámetro F_WD_Time especifica el número de milisegundos del temporizador de watchdog. Este temporizador monitorea la recepción del próximo mensaje PROFIsafe válido.

F_SIL especifica el valor de SIL esperado por el usuario para un dispositivo seguro determinado y es comparado con el valor indicado por el fabricante del dispositivo.

El parámetro F_iPar_CRC es una firma que involucra todos los iParámetros del dispositivo seguro.

Finalmente el parámetro F_Par_CRC es una firma que involucra a todos los F-Parámetros del dispositivo y sirve para asegurar el correcto envío de los F-Parámetros.

3.2.4 Implementación de PROFIsafe

El objetivo de la seguridad en la automatización es la de mantener los procesos productivos dentro de los parámetros normales para evitar daños a las personas, a las instalaciones o al medioambiente. La característica que mide la seguridad de una Función de Seguridad es el SIL que indica la probabilidad de que ocurra una falla peligrosa en el sistema. Esta probabilidad de falla es por ejemplo de 10^{-7}/h para SIL 3. En contraste a esto el objetivo de máxima disponibilidad, relacionado con la tolerancia a falla de un sistema, es el de mantener al sistema operando en caso de fallas. Una medida de la disponibilidad del sistema es la relación entre el tiempo en servicio real y el tiempo total de funcionamiento, por ejemplo de un 99,95%. El concepto de redundancia es muy útil a la hora de lograr los mayores valores de disponibilidad de un sistema. PROFIsafe puede trabajar sin o con redundancia para lograr sistemas tolerantes a fallas. La siguiente tabla muestra la relación entre PROFIsafe, Seguridad y Redundancia.

	PROFIsafe	Redundancia	PROFIsafe y Redundancia
Aplicación	Automatización de fábricas e industrias de proceso. Prensas, robots, control de quemadores. Válvulas de bloqueo, Interuptores, etc.	Industrias de proceso e infraestructura de transporte	Industrias de proceso e infraestructura de transporte. Industrias químicas o farmacéuticas, refinerías, explotación marina de petróleo
Alta disponibilidad	---	Deseable sin paradas (tolerancia a fallas)	Deseable sin paradas (tolerancia a fallas)
Seguridad	Sin fallas peligrosas	La redundancia por sí sola no provee seguridad	Sin fallas peligrosas

Gráfico 3.9 - PROFIsafe y Redundancia

Si bien la redundancia por sí sola no implica seguridad, un sistema altamente disponible es una precondición para la seguridad. Un sistema con poca disponibilidad, propenso a paradas indeseables, puede llevar al sector operativo a suprimir las funciones de seguridad haciendo el sistema altamente inseguro.

PROFIsafe puede ser transmitido vía cable, fibra óptica o también en forma inalámbrica. PROFIBUS Internacional establece los detalles de implementación para WLAN y Bluetooth. En estos casos además de la integridad de los datos hay que tener en cuenta estrictas medidas de seguridad en cuanto al ingreso de intrusos a la red.

Un punto a tener en cuenta es el tiempo de respuesta de las funciones de seguridad que debe ser lo suficientemente corto como para cumplir con su finalidad. Este tiempo depende de cada aplicación en particular y está relacionada a la industria en la que aplica el proyecto. El

criterio adoptado para establecer los tiempos de respuesta de una función de seguridad (SFRT - Safety Function Response Time) se calcula de la siguiente forma:

$$SRFT = TWCDT + \Delta T \text{ (del mayor tiempo de Watchdog)}$$

en donde TWCDT (Total Worst Case Delay Time) es el peor tiempo total de retardo del sistema y el ΔT (del mayor tiempo de Watchdog) es la diferencia entre el más largo tiempo de ejecución del integrante más lento del sistema y el tiempo de watchdog de dicho integrante.

3.2.5. Desafíos de la implementación

Una vez desarrollado el concepto de canal negro y habiendo analizado el estado del arte de uno de los buses seguros del mercado como es PROFIsafe, surge la inquietud del por qué no seguir extendiendo ese concepto a otras aplicaciones aún no desarrolladas.

- Si el concepto de canal negro se lo puede tomar como universal,
- si las características del las capas inferiores del stack no hacen a la confiabilidad del sistema siempre y cuando tengan disponibilidad,
- si se cuenta con un protocolo seguro certificado para SIL 3 como es PROFIsafe,
- si no es necesario contar con hardware especial para implementar el canal de comunicaciones,
- si ya hay desarrollos para blue-tooth y wi-fi,
- es dable pensar que sería posible aplicar estos conceptos a un enlace radioeléctrico y extender así a varios kilómetros el alcance de la comunicación.

Varias son las incógnitas que se plantean a la hora de la implementación utilizando los buses ya analizados. La primer duda que surge es la de si realmente los protocolos pueden ser transmitidos por las radios en forma transparente. Si bien mucho de los radiotransceptores no alteran el contenido de la información que transmiten, al ser cajas negras, no se conoce a ciencia cierta si serán compatibles o no con protocolos seguros.

Saber si la velocidad de transmisión radial (varias veces menor a la de una red Ethernet) será un escollo es otro de los puntos a tener en cuenta.

¿Cuál será el throughput de todo el sistema? Se podría realizar un cálculo previo teniendo en cuenta la información que brindan los fabricantes de cada dispositivo pero es difícil saber a priori si no habrá retardos o latencias no consideradas.

Una vez implementado el proyecto y verificado el rendimiento del sistema, ¿será lo suficientemente rápido para la aplicación deseada?

¿En la configuración del sistema de seguridad, se deben incluir las radios? ¿Cómo hacerlo?.

Dentro de la configuración del sistema con PROFIsafe cada dispositivo además de su dirección I/P tiene su propio nombre, ¿cuál es el manejo de los nombre de las radios?.

Las consultas realizadas al fabricante del equipamiento y del software a utilizar dejaron en claro que muchas de las preguntas no tenían respuestas ciertas. Las respuestas entonces hubo que buscarlas en el campo de la investigación y desarrollar un sistema, que de acuerdo a la teoría debería funcionar pero, que en la práctica tenía muchos puntos a dilucidar y dificultades que resolver.

CAPITULO IV

4 Implementación Práctica

4.1 Introducción

El objetivo del proyecto es comprobar que un protocolo seguro puede ser enviado a través de un enlace radial extendiendo el concepto de canal negro a este medio de comunicación.

Si bien la implementación práctica del proyecto se realizó con componentes marca Siemens y software del mismo proveedor la idea original fue la de implementar el proyecto con MODBUS TCP como protocolo base y openSAFETY, soportado por el Ethernet POWERLINK Standardization Group (EPSG), como protocolo de seguridad. El protocolo de Ethernet industrial utilizado por el ESPG es Powerlink y en la mayoría de los casos sobre éste se monta openSAFETY. Sin embargo este último protocolo, según los desarrolladores, puede ser adaptado para trabajar con cualquier otro protocolo industrial como MODBUS TCP. En el ambiente industrial este protocolo es ampliamente utilizado por lo que disponer de equipamiento no fue una tarea difícil. En primer lugar se configuraron los equipos maestros y remotos y posteriormente las radios para establecer el radioenlace. Con el equipamiento trabajando en MODBUS TCP se procedió a intentar adaptar el protocolo openSAFETY. Para ello se contactó a los especialistas del ESPG en Austria a fin de estudiar los cambios para la implementación con MODBUS TCP. Luego de algunas comunicaciones y solicitudes de información se comprobó que el ESPG estaba solamente detrás de intereses económicos por lo que se debió suspender la implementación del proyecto con estos protocolos y realizar un nuevo estudio para determinar qué protocolos utilizar.

Luego de la experiencia fallida con el ESPG se contactó a personal de Siemens para intentar ejecutar el proyecto con componentes de esta marca. Siemens posee todo su software licenciado y el equipamiento a utilizar está certificado por organismos internacionales por lo que su costo es elevado. Conseguir tanto el software como el hardware presenta complicaciones al no contar con presupuesto. Luego de varios encuentros Siemens decidió apoyar el proyecto a pesar de la incertidumbre en el resultado del mismo.

Cabe destacar que PROFIBUS y PROFINET Internacional ha especificado los detalles de la implementación para WLAN y Bluetooth sin embargo no ha avanzado sobre especificaciones en enlaces radiales. De ahí la duda de Siemens sobre la probabilidad de éxito del proyecto. En las primeras consultas hechas a la mesa internacional de ayuda de Siemens mostraron escepticismo ante la propuesta ya que el mercado existen enlaces inalámbricos para protocolos seguros pero no lo hacen vía radioenlace.

Es necesario remarcar que no se busca implementar un SIS sino utilizar todo el desarrollo y la potencialidad que las herramientas utilizadas en estos sistemas poseen para establecer una comunicación radial segura a través de la cual enviar señales de parada a distancia.

La arquitectura del proyecto implementado supone la existencia de una estación local la cual debe intercambiar información en forma segura con otra estación remota ubicada a una distancia accesible sólo vía enlace radial.

Sobre el canal de comunicaciones PROFINET se monta el protocolo PROFIsafe que asegura la confiabilidad de la comunicación. El

canal negro está formado por todos aquellos componentes que hacen posible el enlace radial.

Las condiciones de contorno del proyecto son:

- La distancia entre el PLC de seguridad (estación local) y la periferia distribuida (estación remota) puede ser cubierta a través de un enlace radial.
- El tiempo de respuesta de todo el sistema no es crítico pudiendo ser de algunos segundos.
- Puede asegurarse en todo momento la disponibilidad de la comunicación.
- Por ser proyecto aplicable a un sistema de parada de emergencia de accionamiento manual y no automática no se considera el mismo como un SIS, aunque se utiliza toda la potencialidad de estos sistemas. Al no ser considerado un SIS no se hace necesario cumplir con el ciclo de vida que indica la norma IEC 61511.

4.2 Listado de Componentes

El listado de componentes de hardware utilizados es:

a) Estación local

- CPU 315-2DP/PN F - 6ES7315-2FJ14-0AB0 (PLC de seguridad certificado SIL 2)
- SITOP 2A - 6ES7307-1BA01-0AA0 (Fuente de alimentación de estación local)
- Radio MDS iNet 900 – Acces Point

b) Estación remota

- ET200S F - 6ES7131-4BF00-0AA0 (Periferia distribuida High Feature)

- 6ES7138-4CA01-0AA0 (Módulo de Potencia 24 VDC)
- 6ES7138-4FA04-0AB0 (Módulo DI de seguridad)
- 6ES7138-4FB03-0AB0 (Módulo DO de seguridad)
- 208-0BA10-2AA3 (Switch Scalance X208)
- 6EP1331-1SL11 (Fuente de alimentación para Remote I/O en estación remota)
- Radio MDS iNet 900 – Remoto

c) Alimentación enlace radial (canal negro)

- 6EP1634-3BA00 (Fuente de alimentación de radiotransmisores y switch Scalance)

4.3 Software

Para la configuración del sistema se utilizó la suite “TIA Portal V12 SP1” los paquetes “SIMATIC STEP 7 Safety Advanced combo V12”, SIMATIC STEP 7 Professional Edition combo V12” [18] [21] todos desarrollados por la empresa Siemens.

4.4 Arquitectura Tradicional del Sistema

La arquitectura tradicional de un sistema de seguridad consta del PLC de seguridad y una periferia distribuida llamada Remote I/O [16]. Esta arquitectura es la mostrada en el gráfico 4.1. El PLC es el encargado de resolver la lógica, actuar en consecuencia y de verificar la integridad del sistema [11]. La periferia distribuida o Remote I/O es una electrónica separada del PLC que es la encargada de gestionar las entradas y salidas físicas del sistema. En una topología tradicional ambos se conectan a través de un cable Ethernet y se comunican utilizando los protocolos PROFINET y PROFIsafe.

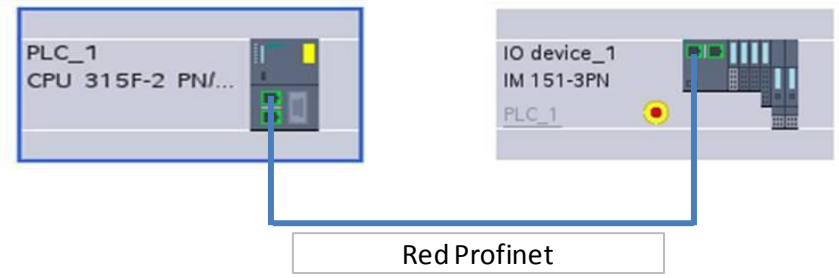

Gráfico 4.1 - Arquitectura original del sistema

La arquitectura presentada en el gráfico anterior muestra la topología tradicional de un sistema de control con periferia distribuida. En condiciones normales estos equipos están ubicados en la misma sala o en salas diferentes, separadas la distancia que la red PROFINET permita que dependiendo del medio físico usado será de 100 metros para cobre (cables categoría 5 ó 6), de 26 kilómetros para fibra óptica monomodo y de 100 metros para un enlace WLAN. Si queremos extender el alcance de la red, como en este proyecto, a una distancia mayor que la alcanzada por la fibra óptica, la solución más recomendable desde el punto de vista técnico-económico es establecer una comunicación radial que vincule ambos puntos del sistema de automatización.

Para ello hay que reemplazar el cable Ethernet por un enlace de comunicación y lograr que componentes que han sido diseñados para trabajar íntimamente conectados logren hacerlo en forma separada soportando elementos “extraños” entre ellos, para los cuales no han sido diseñados.

4.5 Arquitectura Real del Sistema

Como mencionamos, el sistema original está formado por el PLC y el Remote I/O mientras que en la arquitectura real del proyecto se suma el enlace radial conformado por dos radios y un switch junto con los cables de conexionado.

Al incluir el canal negro en el sistema, la arquitectura real del proyecto se ve modificada y pasa constar de varios integrantes: PLC, dos radios, dos antenas, el medio de transmisión, un switch y la periferia distribuida.

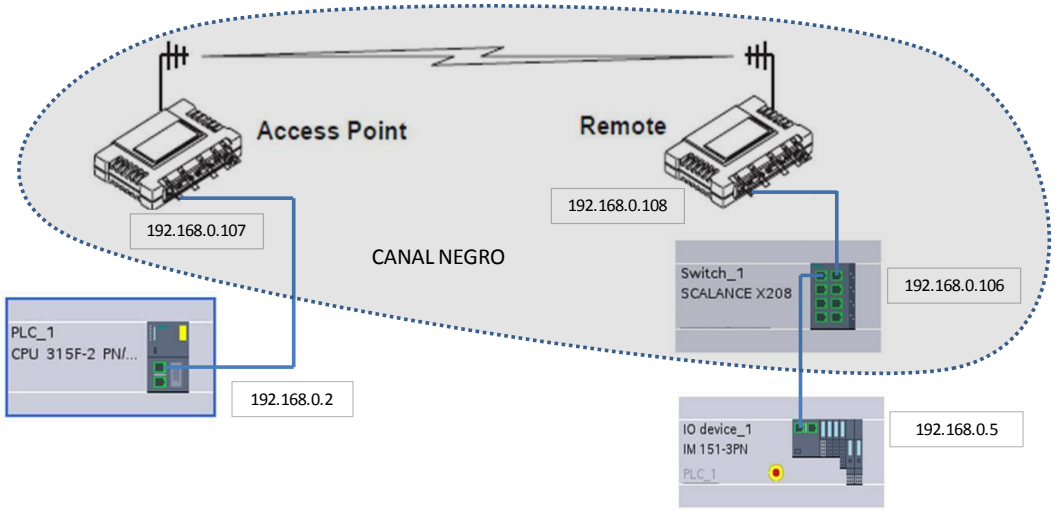

Gráfico 4.2 - Arquitectura real del sistema

En el Gráfico 4.2 se visualiza la topología completa del sistema experimental. Dentro de la nube se circunscribe el llamado canal negro. De acuerdo a la teoría el canal negro es transparente para el PLC y su Remote I/O y se busca demostrar que en la práctica también lo es.

En el mismo gráfico se indican las direcciones IP utilizadas para cada uno de los componentes. La máscara de red utilizada fue 255.255.255.0.

4.6 Demo de Laboratorio

Para la implementación práctica del proyecto se construyó un demo (a escala de laboratorio) sobre el cual se realizaron todos los ensayos. La imagen siguiente muestra la disposición física de los componentes.

La parte superior del demo consta de la CPU, del PLC y de su fuente de alimentación. En la parte media del demo se montaron las dos radios y

la fuente de alimentación (SITOP) de ambas. La radio de la izquierda es la radio maestra y la radio de la derecha la remota. La primera está conectada por un cable Ethernet a la CPU y la segunda a la periferia distribuida, también conectada por medio de un cable Ethernet. La única conexión entre las dos radios es a través del éter.

Imagen 4.1 – Demo de laboratorio

En la parte inferior de la imagen se visualiza la periferia distribuida propiamente dicha, el switch Scalance y la fuente de alimentación del switch.

4.7 Vista de Redes

El proyecto constó de dos fases. La primera contempló la implementación del sistema con la arquitectura tradicional. Para ello se configuraron los equipos, se desarrolló la lógica que posibilitara el

intercambio de información entre la CPU del PLC y el Remote I/O y se realizaron las pruebas de funcionamiento y detección de anomalías.

Una vez que se comprobó que el sistema estaba operativo y funcionando correctamente se pasó a la segunda fase. Esta segunda fase implicó reemplazar el cable Ethernet entre el PLC y el Remote I/O por el conjunto de dispositivos que conforman el enlace radioeléctrico.

Como ya vimos los dispositivos utilizados en los SIS tienen una gran capacidad de diagnóstico y cualquier error o problema en la comunicación será detectada y provocará que el sistema vaya a su estado seguro. Por lo que cualquier inconveniente al implantar el canal negro en el sistema original hará que la comunicación sea inviable y que el proyecto fracase.

La forma más confiable de determinar si el canal negro es realmente transparente para el sistema es verificar como se visualiza el mismo desde la consola de configuración de TIA Portal. La vista de redes de TIA Portal es un esquemático que muestra cómo están interconectados entre sí los distintos componentes de la red y su estado de funcionamiento.

En el gráfico 4.3 se puede apreciar como “ve” TIA Portal y el propio sistema Siemens el esquema de redes en la segunda fase del proyecto. Sólo se observan el PLC y el Remote I/O. Las radios y el switch Scalance son transparentes para el proyecto y para el sistema en sí. Tanto la CPU como el Remote I/O están operativos y sin fallas como indica el tilde en el costado superior izquierdo de cada bloque. En la parte inferior izquierda de la pantalla, en la solapa “Información de dispositivos” la leyenda “Ningún dispositivo con fallos” asegura que el sistema está 100% operativo y sin fallas. Para el sistema Siemens los dos nodos de la red están conectados por un cable, sin embargo hay un enlace radial comunicando ambas partes.

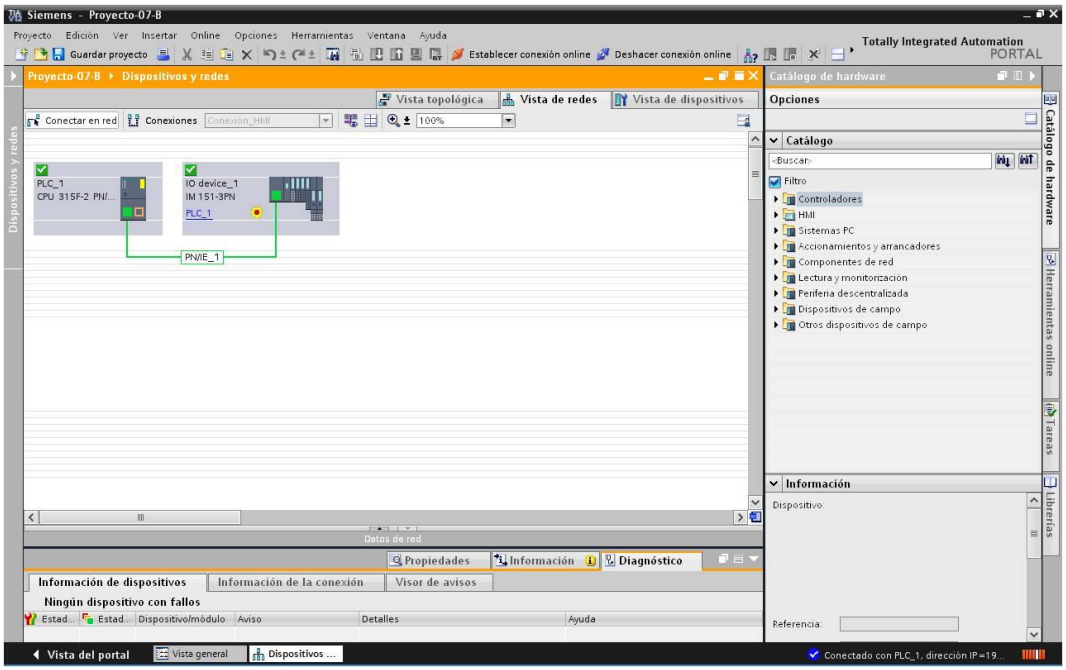

Gráfico 4.3 - Vista de redes del TIA Portal

Se puede acceder a información más detallada de cada uno de los componentes de la red seleccionando, en el árbol del proyecto, el dispositivo en cuestión y abriendo la ventana “Vista de dispositivos”. Así se logra visualizar el estado interno de cada componente dentro del nodo de red. El gráfico 4.4 muestra el estado del nodo PLC, en donde tanto la fuente de alimentación (PS 307) como la CPU del PLC (315F-2) se encuentran en condiciones operativas normales y sin fallos. En el gráfico 4.5 se observa el estado de los componentes del nodo de la periferia distribuida. El módulo de comunicaciones (ET 200S F), el módulo de potencia (fuente de alimentación) (PM-E), el módulo de entradas digitales (4/8 F-DI) y el módulo de salidas digitales (4 F-DO) también se encuentran operativos y sin fallas. En este mismo gráfico en el costado izquierdo se puede ver el árbol completo del proyecto con todos los componentes en estado normal de funcionamiento. Es válido recordar que estás pantallas fueron capturadas con el sistema trabajando a través del enlace radial.

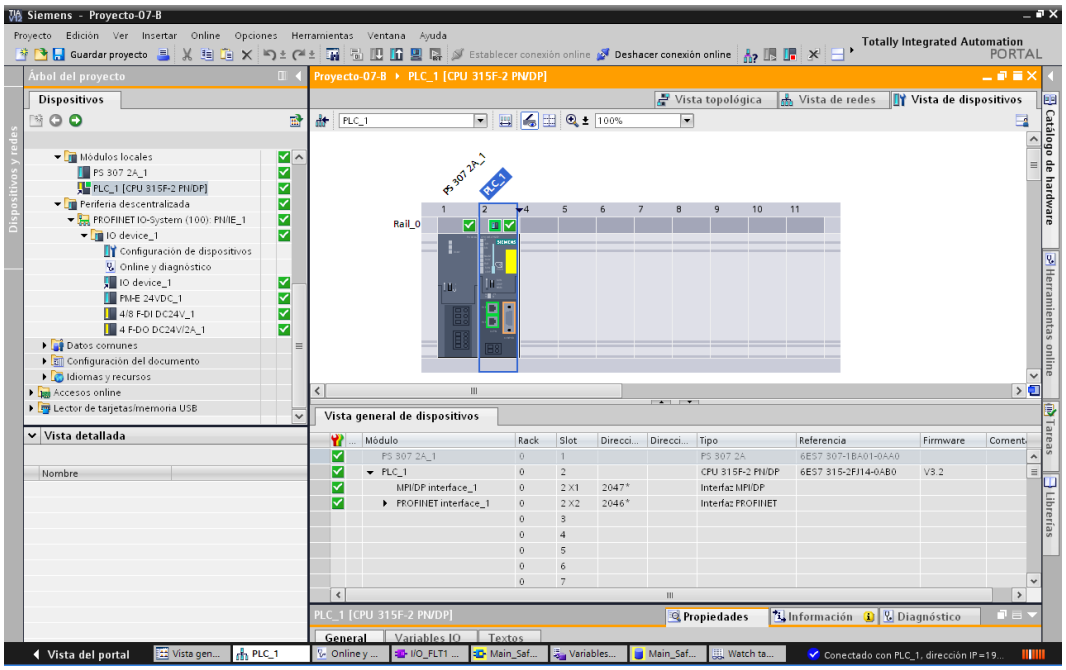

Gráfico 4.4 - Estado del PLC y sus componentes

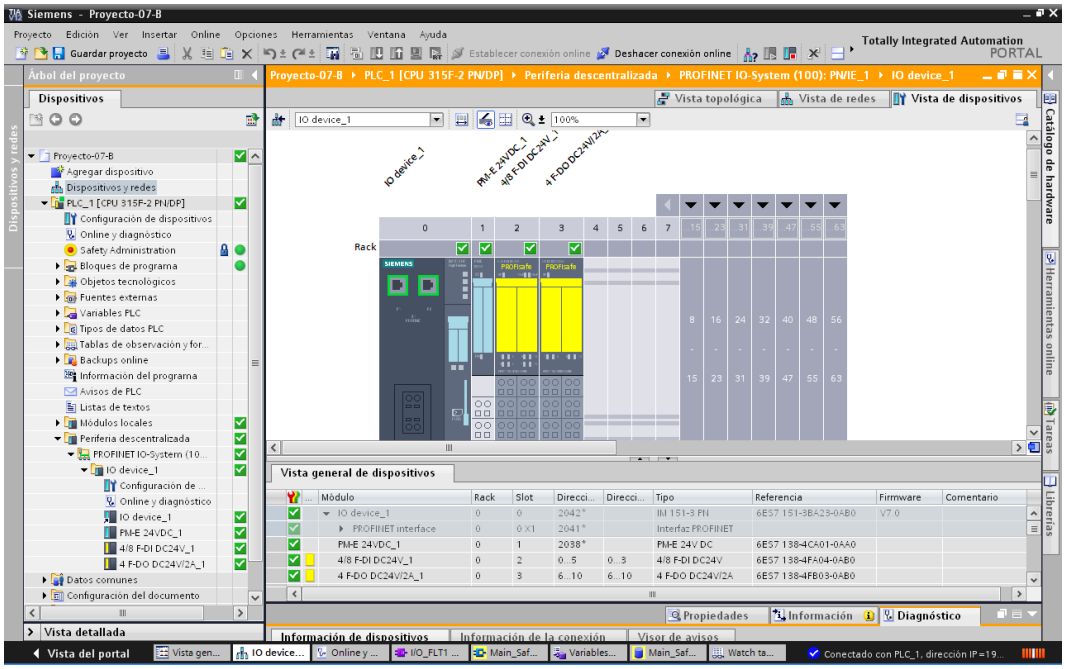

Gráfico 4.5 - Estado del Remote I/O (a través del enlace radial)

4.8 Configuración de Dispositivos

En este apartado se hace referencia a la configuración de los distintos dispositivos, tanto del enlace radioeléctrico como del sistema de automatización.

a) Radiotransceptores

Las radios se configuraron utilizando su puerto serial vía el Hyperterminal de Windows. Para la configuración de estas radios no fue necesario utilizar ningún otro software adicional [10].

Los parámetros de comunicación del puerto serie en ambas radios fueron de 19.200, 8, N, 1.

Las radios utilizadas pueden trabajar tanto como access point o como remotas, por lo cual la radio asociada al PLC (estación local) se configuró como access point y la radio de la estación remota como remoto.

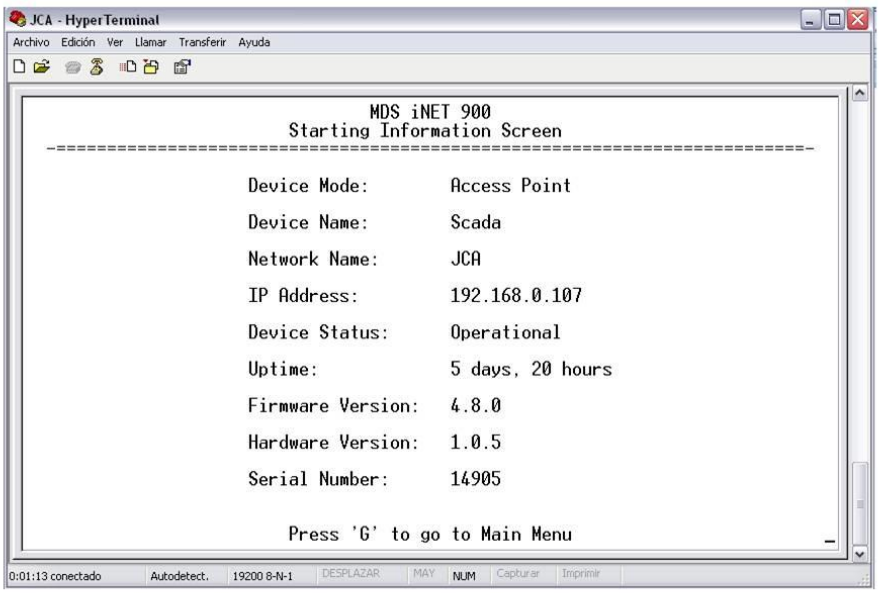

Gráfico 4.6 - Radiotransceptor Acces Point

En el gráfico 4.6 se visualiza la pantalla inicial de configuración que muestra los datos básicos de configuración del radiotransceptor que trabaja como access point. También se puede observar el access point operativo.

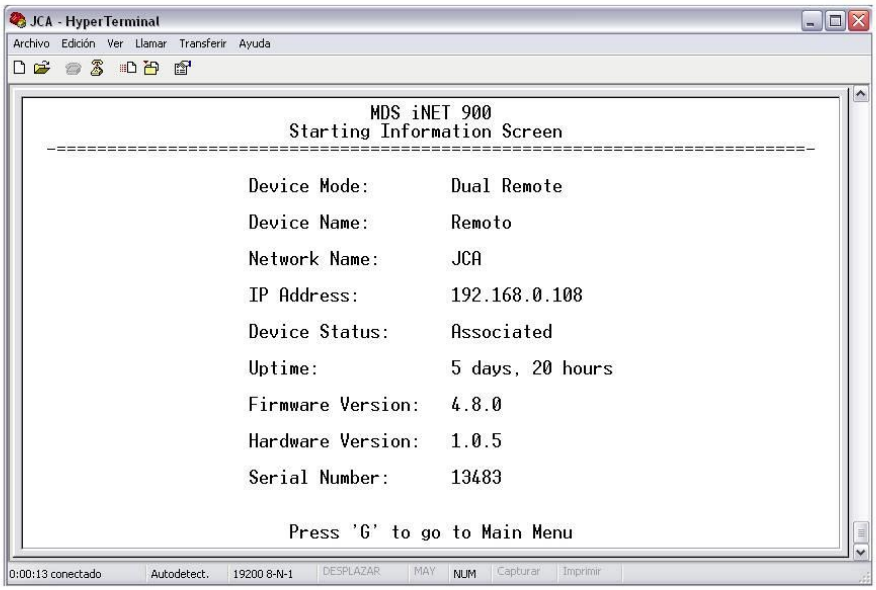

Gráfico 4.7 - Radiotransceptor Remoto

En el gráfico 4.7 se visualiza la pantalla inicial de configuración de la radio remota que muestra los datos básicos de configuración del radiotransceptor que trabaja como remoto. En esta pantalla se observa que la remota esta operativa y asociada al access point. Como dato adicional, en ambas pantallas se verifica que el sistema ha estado operativo por cinco días con veinte horas.

La velocidad de transmisión utilizada fue de 512 Kbps que es la máxima velocidad de transmisión disponible.

La tasa de transferencia Ethernet de estas radios es 10 base T y la frecuencia de transmisión de 900 MHz haciendo uso del estándar de seguridad FHSS (Frecuency Hopping Spread Spectrum).

El tipo de enlace utilizado fue el de Point-to-Point (Punto a Punto) que provee un medio de enlace simple entre dos puntos, como extensión de una red LAN, tal como lo muestra el gráfico 4.8.

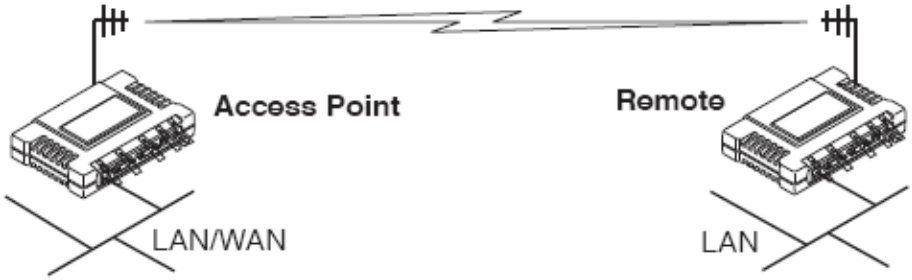

Gráfico 4.8 - Enlace Point-to-Point (Punto a Punto)

Los parámetros de comunicación se configuraron buscando maximizar la velocidad de transmisión. Para ello se optimizaron varios parámetros en las radios. Estos son:

- En el AP solamente. Ajustar el Dwell Time a su máximo de 262.1 ms. El Dwell Time es la duración (en milisegundos) del tiempo que se mantiene la radio utilizando una determinada frecuencia dentro del patrón de Frecuency Hopping. Esto disminuye el overhead debido a que la señal se transmitirá durante más tiempo por ese canal. La desventaja es que si un canal en particular sufre alguna interferencia se demorará más en saltar al próximo canal.
- En el AP solamente. Colocar el Beacon Period a su valor normal de 508 ms. Esto también reduce el overhead de los beacons enviados.

- Cambiar el umbral de fragmentación al máximo de 1600. Así serán enviados paquetes más largos reduciendo el overhead.
- Incrementar el umbral de RTS a un valor de 1600. El RTS fuerza a las remotas a requerir el permiso del AP antes de transmitir un paquete. El AP envía un paquete de control CTS para garantizar el permiso a la remota. Todas las demás remotas detienen su transmisión por una determinada cantidad de tiempo.
- Activar la compresión en el menú de configuración de la radio. Habilitar este parámetro es recomendado por el fabricante para comprimir la información (por ej. archivos de texto) de acuerdo a un algoritmo de compresión antes de enviarla. En el caso del presente proyecto este parámetro no tiene incidencia en la perfomance de la transmisión.

Los parámetros de perfomance de sistema radial durante los días de ensayo (debido a la estabilidad del enlace) se mantuvieron constantes durante el mismo siendo:

- Potencia de salida: Ajustada a 20 dBm
- Relación Señal ruido: 25 dB
- Indicador de fuerza de señal de recepción (RSSI): - 71dBm
- Velocidad de transmisión: 512 kbps

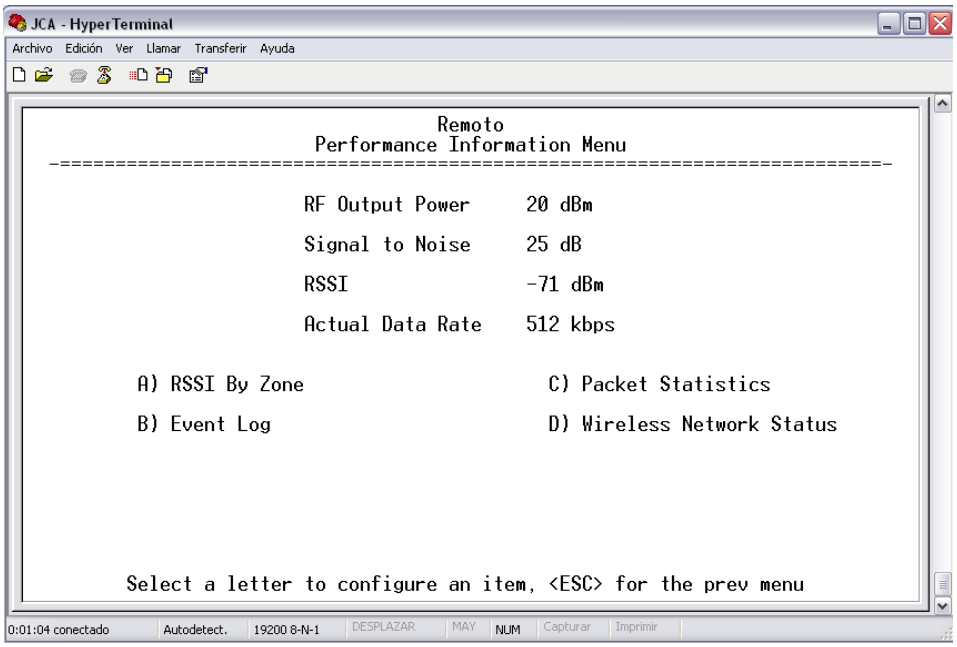

Gráfico 4.9 - Perfomance del enlace radial

b) PLC y Remote I/O

El sistema de automatización Siemens se configuró con la suite TIA Portal V12 SP1 y el paquete SIMATIC STEP 7 Safety Advanced combo V12.

Se tuvo especial cuidado en el ajuste de los parámetros de comunicación para trabajar con PROFIsafe en el modo RT (Real Time).

Los parámetros que se ajustaron fueron:

- Tiempo de ciclo de emisión.
- Ancho de banda calculado para datos I/O cíclicos.
- En todos los puertos se activó la autonegociación.
- La velocidad de transferencia en el puerto Ethernet del PLC se dejó configurada en automático. En el Remote I/O la velocidad de transferencia es fija a 100 Mbs.

  Esto fue una complicación al proyecto debido a que el PLC puede autonegociar con el AP la velocidad de transferencia fijándola en

10 Mbs. Pero el Remote I/O acusó error de comunicación al no poder establecer una comunicación con una velocidad de transferencia de 100 Mbs con la radio remota. Para solucionar este problema se colocó el switch Scalance X208 entre la radio remota y el Remote I/O. Dicho switch se comunica entonces en 10 Mbs con la radio y el 100 Mbs con el Remote I/O. Si las radios tuviesen una velocidad de transferencia de 100 base T no sería necesario el uso de este switch.

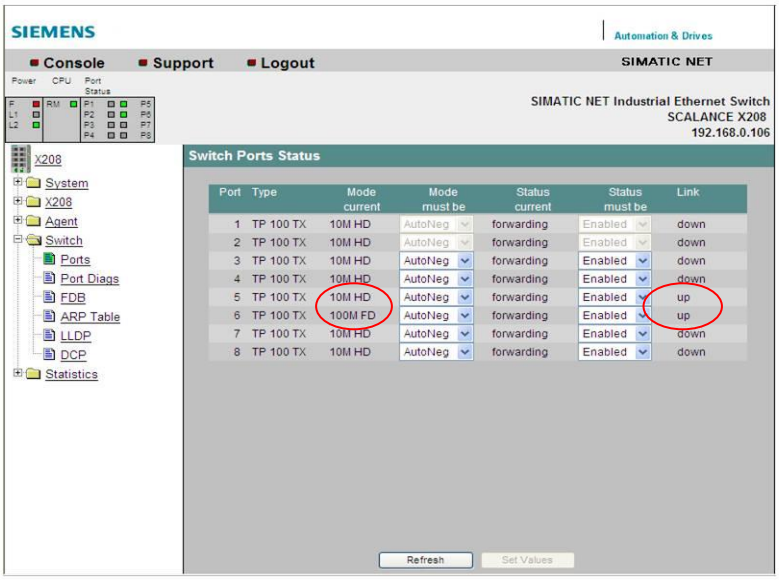

Gráfico 4.10 - Velocidad de transferencia en puertos del switch Scalance X208

En el gráfico 4.10 se visualiza el estado de los puertos del switch Scalance X208. Los puertos activos (up) del switch son el puerto número cinco y número seis. El puerto número cinco está conectado físicamente al PLC y está trabajando en 10 Mbs en half duplex. Mientras que puerto seis del switch, conectado al Remote I/O, está trabajando a 100 Mbs en full duplex.

- Las direcciones IP utilizadas en el proyecto fueron:

PC: 192.168.0.1

PLC : 192.168.0.2

Remote I/O: 192.168.0.5

Switch X208: 192.168.0.106

AP: 192.168.0.107

Remoto: 192.168.0.108

La máscara de red utilizada fue: 255.255.255.0

Dentro del TIA Portal se puede configurar y visualizar el modo de transferencia de datos entre la CPU y el remote I/O. Se ajustó el sistema para que trabajase en RT (Real Time) tomando al PLC como maestro de sincronismo. Esto se puede observar en el gráfico 4.11 que muestra dentro de las propiedades de la CPU, en la configuración en tiempo real, en el campo “Clase RT” que se está trabajando en RT.IRT.

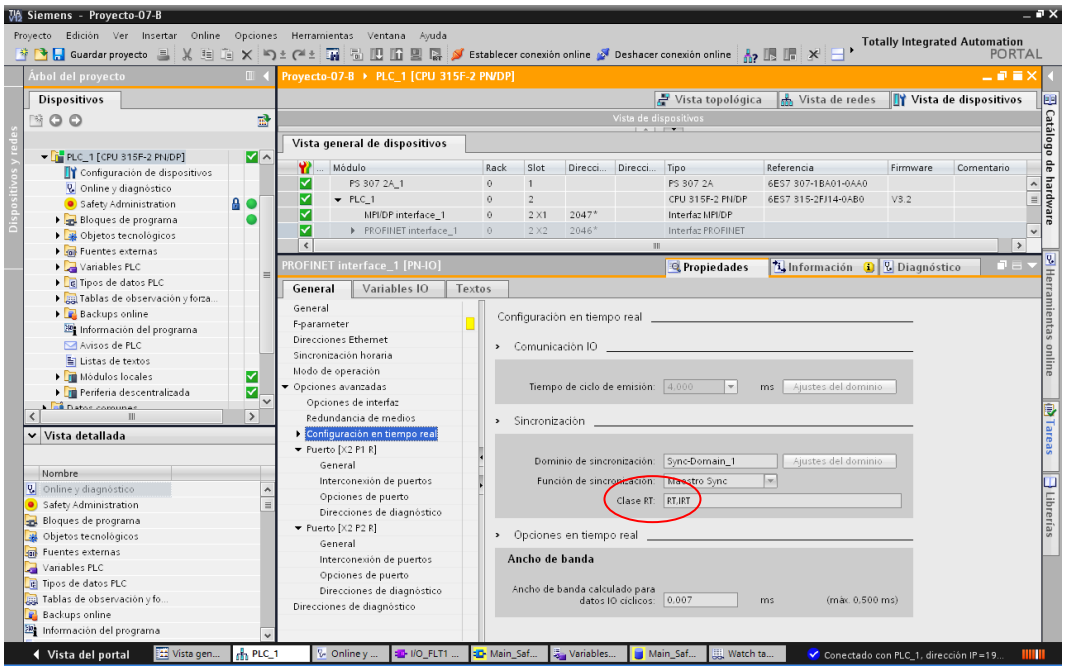

Gráfico 4.11 - Modo de comunicación en RT (Real Time)

En el gráfico 4.12 se visualiza al Remote I/O trabajando también en el modo RT. Esto se puede comprobar observando que está seleccionada en el campo “Clase RT” la opción RT (círculo rojo).

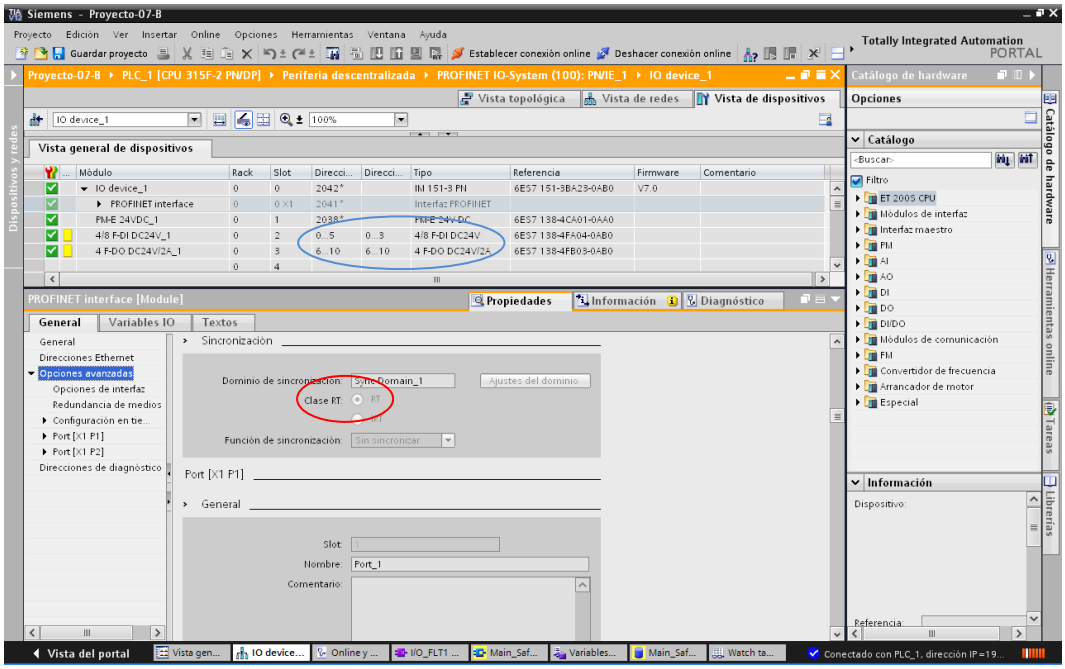

Gráfico 4.12 - Remote I/O trabajando en RT (Real Time)

4.9 Programación del PLC

La programación del PLC en este proyecto es sencilla debido que el objetivo del mismo no es desarrollar alguna estrategia de control o automatización sino lograr establecer una comunicación confiable, vía radio, entre los elementos componentes del sistema seguro.

La programación de la lógica se desarrolló en el bloque **FB**1 [Function Block 1] [Main Safety] que es el bloque en donde se configuran las funciones de seguridad y consta sólo de tres redes. La primera de las redes consta de una entrada digital (denominada **Entrada**) y una salida digital (denominada **Salida 01**). El sentido de esta red es la de probar la comunicación desde y hacia el Remote I/O. Al activar la entrada digital **I0.0** (**Entrada**), en el módulo DI (Entradas Digitales) del Remote I/O, la

señal debe viajar hasta la CPU del PLC la cual resuelve la lógica y ordena activar la salida **Q6.0** (**Salida 01**) del módulo DO (Salidas Digitales) enviando la señal nuevamente al Remote I/O. Así queda probada la comunicación en ambos sentidos.

La dirección **I0.0** apunta a la primer entrada física del módulo de entradas digitales (DI) y la salida **Q6.0** hace referencia a la primer salida física del módulo de salidas digitales (DO).

En el gráfico 4.12, están señaladas con el círculo azul, las direcciones de los módulos y de las entradas y salidas físicas de los módulos. En la cuarta columna de la pantalla presentada por TIA Portal se observa que la primera dirección lógica para el módulo de entradas digitales es la “0” de un rango de “0” a “5”. También se puede ver que la primer dirección lógica posible para un módulo de salidas digitales es la “6”, de un rango de “6” a “10”. En la quinta columna de la misma pantalla se puede visualizar que las primeras direcciones lógicas para las entradas y salidas físicas de los módulos de entrada y salida digital son “0” en ambos casos. El programa hace uso entonces de la primer entrada digital y de la primer salida digital disponibles.

Una segunda red consta de una marca (denominada **Marca**) y una salida digital (**Salida 02**) cuya dirección lógica es **Q6.1**. Una marca es una variable lógica dentro del programa que no tiene asociada una salida física en el PLC y que puede ser forzada (colocarle un valor “0” o “1” lógico) para simular una señal generada por la lógica del PLC. La intención de esta red es la de simular una señal que parte del PLC para alcanzar el Remote I/O. Esto emula, por ejemplo, la acción de un sistema de parada de emergencia en donde se genera en la estación local una señal de paro que debe ser recibida en la estación remota para activar la salida digital de shutdown (paro).

Por último la tercera red está conformada por una marca (denominada **Reset**) y un bloque de reconocimiento global (**ACK_GL_DB**) que permite restablecer el sistema cuando se ha producido una falla. El bloque de reconocimiento global es propio del software de programación y su funcionalidades la de resetear en forma general las fallas del PLC.

En condiciones normales PROFIsafe está monitoreando permanentemente el estado de las comunicaciones, cuando se produce algún error que compromete la confiabilidad del sistema, éste pasa a estado seguro. Este estado seguro es también llamado de pasivación. En la mayoría de los casos el estado seguro del sistema significa provocar el paro de una máquina, o proceso y activar válvulas de blowdown o shutdown que evitan alcanzar escenarios peligrosos. Una vez que el sistema ha sido pasivado y se han restablecido las condiciones normales de operación, se puede entonces volver a normalizarlo (o “despasivarlo”) lo que se logra ejecutando el bloque ACK_GL_DB.

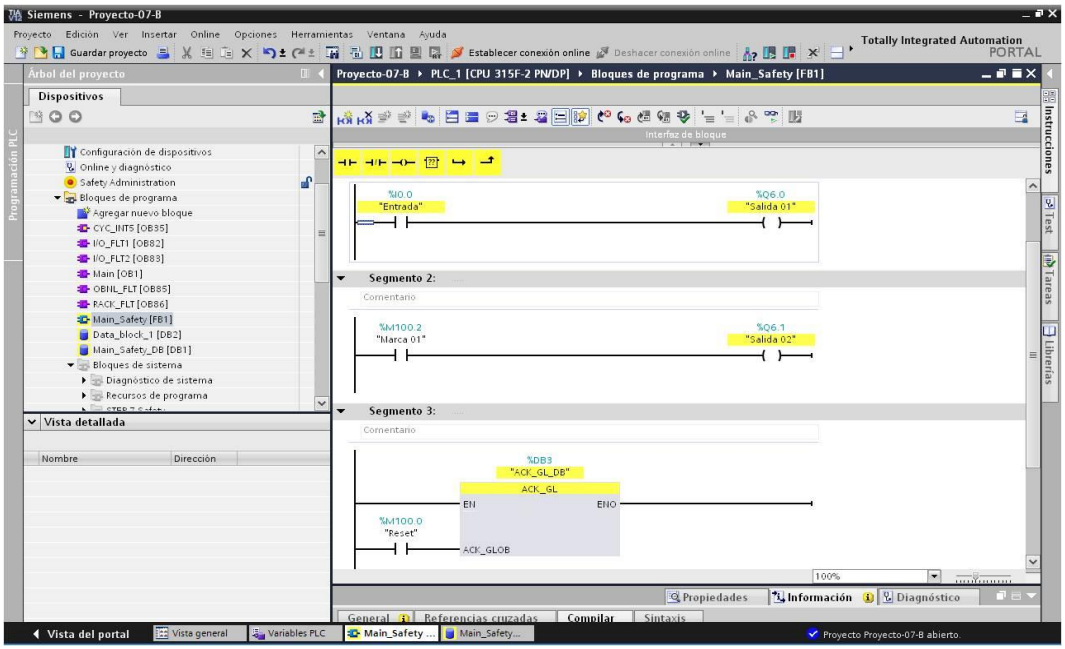

Gráfico 4.13 - Lógica programada en el S7-315 F

4.10 Ensayos de Confiabilidad

Con el conjunto Estación Local–Estación Remota funcionando correctamente se simularon diversas fallas de hardware en los distintos componentes del sistema para verificar la confiabilidad del mismo:

- Se provocaron pérdidas de comunicación debidas a falla de alimentación tanto del access point como del remoto. Para ello se desconectó la alimentación de la estación local y se verificó que el sistema fuese a su estado de pasivación. Luego de restablecido el sistema y las comunicaciones se desconectó la alimentación de la estación remota provocando nuevamente la caída de las comunicaciones y el paso de los módulos de I/O al estado seguro.
- Se indujo el deterioro en la calidad de señal del enlace entre el access point y el remoto. Para ello se desacoplaron las antenas, primero en el remoto y luego en la estación local. Ante ambos eventos los módulos del PLC procedieron a evolucionar hacia su estado de “pasivación”
- Se apagó la fuente de alimentación del Remote I/O lo que fue acusado inmediatamente por el PLC maestro. Apagar la alimentación a los módulos I/O provoca que se desenergizen las salidas digitales lo que lleva al (supuesto) proceso que se está controlando a su estado de reposo. Si bien esto sucede con cualquier tipo de PLC la diferencia en este caso es que, cuando se restablece la energía al remoto, el PLC maestro mantiene a los módulos de I/O en su estado de “pasivación” hasta que se ejecute el bloque de reconocimiento global. Es decir que el proceso no vuelve a la normalidad sino es realizada esta operación.
- Se desconectaron los distintos cables que vinculan el access point con el PLC, el remoto con el switch, el switch con el remote I/O y las

demás combinaciones posibles. En todos los casos, al ser interrumpido el normal flujo de información, los módulos I/O pasaron a su estado seguro y se debió restablecer el sistema mediante el ya descripto proceso de normalización.

- Se cambió on-line la configuración de las radios, con lo que se provocó la pérdida de la comunicación. En este caso también el sistema reaccionó evolucionado hacia su estado seguro y necesitando luego del proceso de reseteo para volver a estar operable.

Se comprobó en todos los casos que los módulos del Remote I/O pasaron a su modo “pasivado” desactivando en este caso las salidas. Para retornar al estado normal, una vez solucionado el problema de hardware, se activó el bloque ACK_GL_DB a través de la variable Marca.

En el gráfico 4.14 se muestra una imagen del buffer de diagnóstico (on–line) del PLC luego de una falla en la comunicación radial. Primero es detectado un fallo en el Remote I/O y los dos módulos de seguridad (“F” de failsafe) pasan al modo “pasivado”, indicado por el círculo rojo. Una vez restablecida la comunicación se recupera la comunicación con el equipo (Remote I/O) para luego colocarse, los módulos, en estado “ok”, indicado dentro del círculo azul.

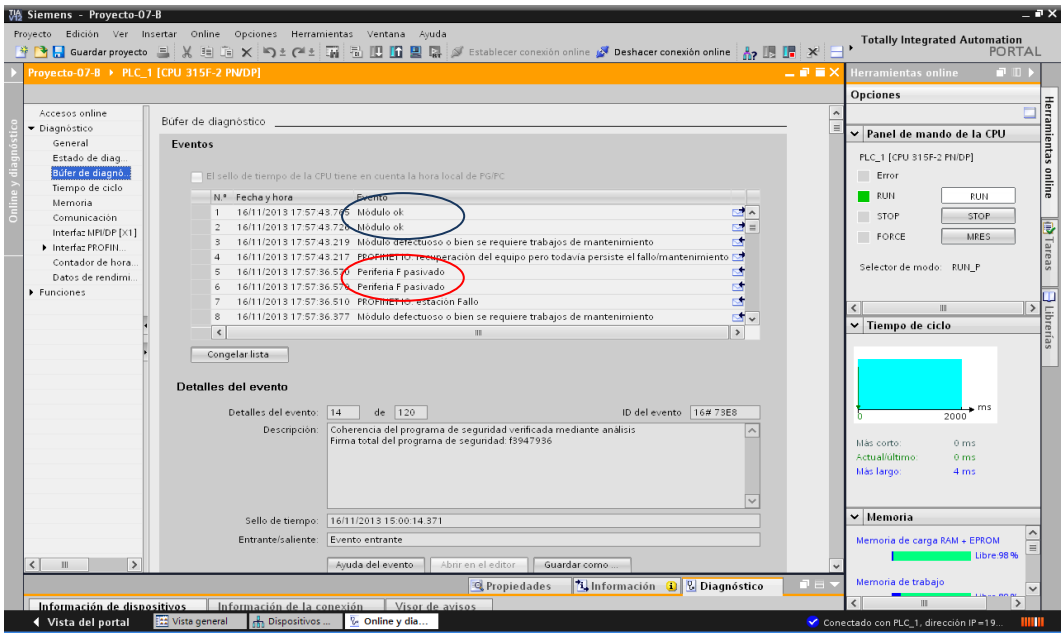

Gráfico 4.14 - Módulos de Remote I/O en estado “pasivado”

Sin embargo los módulos continuarán en estado pasivado hasta que se restablezcan de la falla (reseteo). En esta condición los leds de SF (System Fault) de los módulos parpadean con un período de 1 seg. En este estado se siguen recibiendo y procesando las señales de entrada pero las salidas se encuentran en estado seguro.

Una vez reconocida la falla, se restablecen los módulos los que pasan al estado normal de “no pasivado” como se visualiza en el gráfico 4.15.

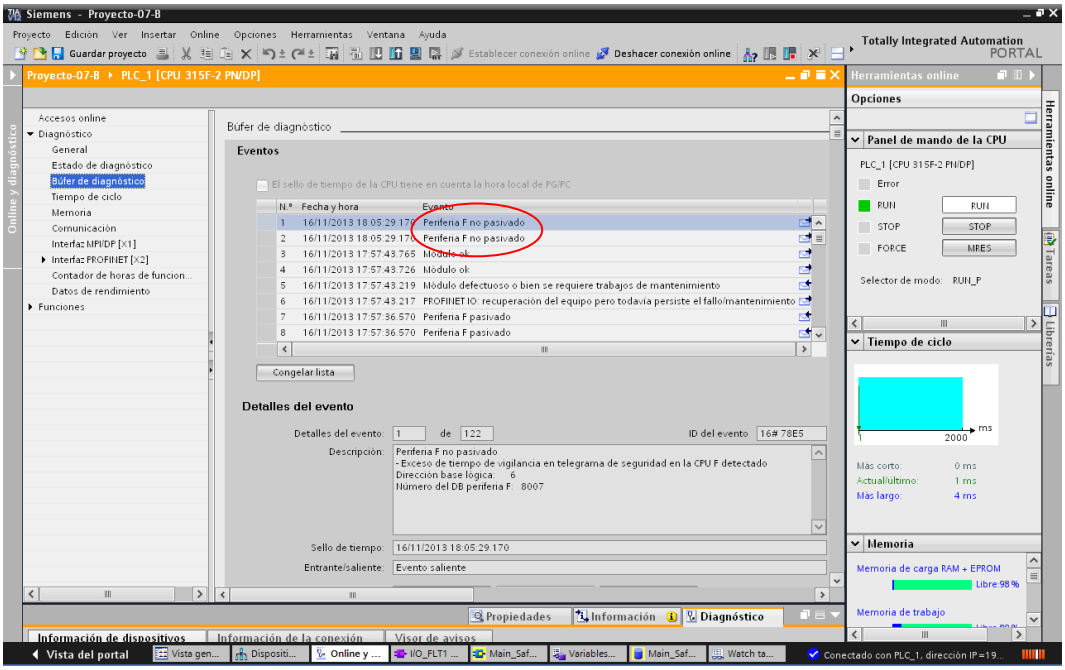

Gráfico 4.15 - Módulos del Remote I/O en estado normal (no “pasivados”)

Es necesario resaltar que es totalmente esperable que el sistema se comportara como lo hizo en absolutamente todos los casos en que se interrumpió de alguna u otra forma la comunicación entre las partes. Esto es así ya que el comportamiento determinístico y en tiempo real del sistema está garantizado por PROFIsafe que posee todos los requisitos para trabajar en sistemas confiables hasta SIL 3.

Por lo que realmente el éxito del proyecto no está en la verificación de la confiabilidad del sistema, visto esto como su respuesta ante fallos, sino en el haber logrado establecer la comunicación “sin fallas y con una respuesta acorde a las exigencias planteadas” utilizando un enlace radioeléctrico como canal negro.

CAPITULO V

5. Conclusiones

Sin lugar a dudas Ethernet ha conquistado no solamente el espacio de oficinas y la comunicación mundial, a través de internet, sino que también se ha posicionado definitivamente como bus industrial.

Todos los grandes desarrolladores de protocolos y de hardware para sistemas de control industrial lo han adoptado y adaptado a sus necesidades dando origen a diversos protocolos, a los cuales han dado diferentes nombres, pero que en el fondo son, en esencia, Ethernet. La compatibilidad es tal que cualquier hardware hogareño puede trabajar con estos nuevos protocolos industriales basados en este estándar. Durante el desarrollo de este proyecto, y ante la falta temporaria de un switch de tipo industrial, se utilizó un switch hogareño siendo totalmente transparente para los protocolos utilizados, PROFINET y PROFIsafe, que permitió seguir desarrollando el trabajo.

La versatilidad que presenta Ethernet lleva a que sea utilizado también como base para la transmisión de protocolos seguros en los sistemas instrumentados de seguridad (SIS). Este es el caso de PROFIsafe que se monta sobre PROFINET, utilizando el concepto de canal negro.

Este concepto, que es aplicado por los fabricantes de equipamiento certificado para SIS, implica un cambio de paradigma en el manejo de la información en los buses de campo industriales. Antes de la aparición de esta nueva concepción todo el sistema debía ser completamente seguro. Tanto hardware como software debían cumplir con todos los requisitos para ser considerados como seguros. Con la aplicación de este nuevo concepto se pone énfasis en el protocolo seguro, en este caso

PROFIsafe, como “reaseguro” de que si la información llega al destinatario es “seguro” que lo hace en forma correcta. Esto es, lo que es llamado por todos, confiabilidad del sistema.

Sin embargo no hay que olvidarse que debajo de este protocolo seguro hay todo un sistema (hardware y software) que debe hacer su trabajo y que lo debe hacer bien. Es decir el sistema debe tener disponibilidad, que es otro de los requisitos básicos a cumplir en la implementación de sistemas de control industrial.

Este proyecto hace uso del canal negro y lo aplica en un enlace radioeléctrico, extendiendo el campo de aplicación de este concepto. El sistema de comunicación, en este caso radial, debe ser desarrollado e implementado de forma tal de asegurar la disponibilidad requerida a fin de cumplir con su objetivo.

Es decir que si logramos tener un enlace radial disponible, la utilización de un protocolo de seguridad (PROFIsafe en este caso) transforma a ese enlace disponible también en confiable, asegurando que la información que llegue a la estación remota lo hará sin errores. Por otra parte, y que no es menos importante, si se produce algún error el sistema evolucionará hacia un estado seguro.

El sistema disponible se logró utilizando radiotransceptores de larga trayectoria en la industria y de reconocida calidad. Se respetaron los parámetros de perfomance del enlace, recomendados por el fabricante y se optimizaron las comunicaciones de acuerdo a lo indicado en los manuales. Durante los días de ensayo de los equipos no se sufrió ningún problema en las comunicaciones logrando un sistema 100% disponible. Sobre este esquema se montó PROFINET y PROFIsafe logrando además un sistema confiable

De los ensayos realizados se concluye que la extensión del concepto de canal negro a un enlace radial es totalmente posible y puede ser aplicado a un sistema de parada de emergencia manual a distancia.

CAPITULO VI

6. Trabajos Futuros

Varios son los frentes que aún se pueden seguir desarrollando una vez comprobada la posibilidad de tener un enlace confiable, con la seguridad que da transmitir y recibir un protocolo certificado para SIS como lo es PROFIsafe.

Uno de ellos es el de extender la distancia de cobertura de los enlaces y lograr la disponibilidad que el proyecto en cuestión necesite. Esto podría lograrse a través de diferentes topologías de comunicaciones y equipos, enlaces redundantes a través del uso de protocolos tales como RSTP (Rapid Spanning Tree Protocol) u otros mecanismos que aseguren una buena perfomance en la comunicación.

Otro de los desafíos es enviar señales analógicas a través del enlace radial como, por ejemplo, para manejar variadores de velocidad con la posibilidad de llevarlos a su estado seguro (velocidad segura) ante problemas en el proceso.

Un proyecto a futuro puede ser el de incrementar el número de Remote I/Os utilizados en el sistema y comprobar que con un solo PLC y una red de comunicación radial se puede montar, un sistema de parada de emergencia distribuido en el campo.

Reemplazar el Remote I/O por otro PLC de seguridad ubicado en otro lugar de tal forma de aumentar la disponibilidad (redundancia) del sistema. Esto permitiría seguir trabajando en forma segura ante un incendio en el lugar en donde estuviese instalado uno de los PLCs.

Otra de las posibilidades es la de desarrollar este proyecto con otras marcas y modelos de radiotransceptores y/o con otras marcas y modelos de hardware así también con software de otros fabricantes.

Varios son los escenarios que se pueden plantear y resolver con la viabilidad de enviar protocolos seguros a través de un enlace radial pero en todos ellos y por varios años más va a estar como telón de fondo Ethernet.

BIBLIOGRAFÍA

- **[1] Bernhard, Heitzer**. (07/2012). *Real-time behaviour of Ethernet on the example of PROFINET.*
- **[2] Exida**. (01/2006). *IEC 61508 Overview Report A Summary of the IEC 61508 Standard for Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems*.
- **[3] Felser, Max**. (05/2005). *Real-Time Ethernet—Industry Prospective*.
- **[4] Felser, Max**. (07/2002). *The Fieldbus Standards: History and Structures*.
- **[5] Felser, Max y Sauter, Thilo**. (07/2002). *The Fieldbus War: History or Short Break Between Battles?*.
- **[6] IAONA Handbook.** (04/2005). *Industrial Ethernet.* Second Edition.
- **[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC)**. (04/2010). *61508-3 Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 3: Software requirements*. Edition 2.0.
- **[8] Ladkin, Peter B**. (2008). *An Overview of IEC 61508 on E/E/PE Functional Safety.*
- **[9] Luis Manuel Garcia**. (07/2010). *El futuro de los buses de campo en aplicaciones de seguridad de procesos continuos*.
- **[10] Microwave Data Systems Inc**. (12/2005). *MDS iNET 900™ Series Users Guide Wireless IP/Ethernet Transceiver Firmware Release 4* MDS 05-2806A01, Rev. E.1.
- **[11] PI PROFIBUS & PROFINET International.** (03/2007). *PROFINET Cabling and Interconnection Technology Guideline for PROFINET.* Version 2.00 Order No: 2.252.
- **[12] PI PROFIBUS & PROFINET International**. (2009). *PROFINET System Description*.
- **[13] PROFIBUS Working Group 6**. **Electromechanics in the Technical Committee 2 Communication Profiles**. (02/2004).

PROFINET Guideline, Order No: 2.252 p2 *Installation Guideline PROFINET Part 2: Network Components.* Version 1.01.

- **[14] Rofár, J. & Franeková, M**. (11/2010). *Functional Safety Specification of Communication Profile - PROFISAFE.*
- **[15] Ron, Bell**. (08/2005). *Introduction to IEC 61508*.
- **[16] Smith, Davis J & Simpson Kenneth GL**. (2004). *Funtional Safety A Straightforward Guide to applying IEC 61508 and Related Standards*. Second edition. Ed. El Sevier.
- **[17] SIEMENS**. (09/2006). *Comunicación con SIMATIC. Manual de sistema*.
- **[18] SIEMENS**. (03/2006). *Programar con Step 7. Manual*. Edición 03/2006.
- **[19] SIEMENS**. (11/2010). PROFIsafe System Description Technology and Application
- **[20] SIEMENS**. (04/2007) *Seguridad funcional en la instrumentación de procesos con clasificación SIL. Preguntas, ejemplos, antecedentes.*
- **[21] SIEMENS**. (10/2011). *SIMATIC STEP 7 Professional /WinCC Advanced V11 for Sample project Filling Station. Getting Started.*

LISTADO DE GRAFICOS